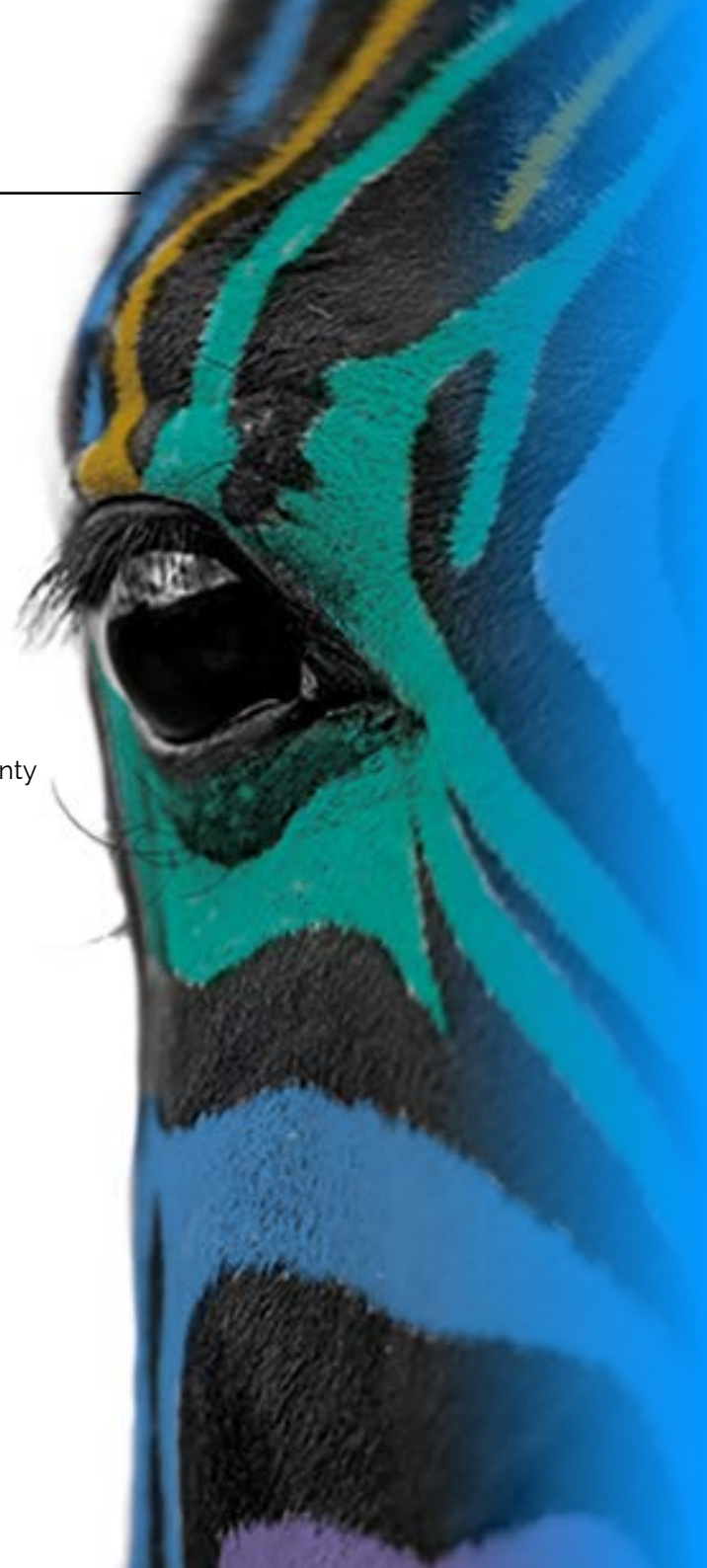

Digital Vision: Cybersecurity 3

Opinion paper

Atos

Contents

3	Foreword
6	Trends in cybersecurity
8	Industry focus: Public Sector & Defense
10	Digital transformation
11	Safety first? Delivering digital transformation
16	Re-imagine: a world without boundaries
18	Delivering diversity and inclusion within cybersecurity
20	Industry focus: Health & Life Sciences
22	Digital sovereignty
23	Preparing organizations for a sovereign digital future
27	Why people are at the heart of mastering data sovereignty
30	The CISO perspective on digital sovereignty
33	Managing the risks around 5G
36	Industry focus: Financial Services & Insurance
38	Zero trust
39	Risk in a zero trust world
42	The power and potential of context-aware security
44	IAM at the heart of the zero trust approach
46	Five tips for a successful zero trust journey
50	Industry focus: Telecom, Media & Technology
52	Cloud security
53	Securing the journey to the cloud
56	Deciphering the sovereign cloud
60	How AI can simplify cloud security management
62	Lexicon
64	Acknowledgements
65	Production team





Atos Digital Vision: Cybersecurity 3



Kulveer Ranger

SVP, Head of Strategy, Marketing, Communications & Public Affairs,
Atos Northern Europe & APAC and techUK board member

Introducing the latest Atos cybersecurity opinion paper, Kulveer Ranger urges organizations' to consider their approach to cybersecurity in a volatile world.

More than two and a half thousand years ago, the philosopher Heraclitus famously observed that *"there is nothing permanent except change"*.

While the pace of this change has increased exponentially over the last few years in no small part due to the pandemic, much of it in the digital sector has been welcomed by businesses, governments and citizens.

The pandemic turbo-charged the transformation of how we live and work – a two-year period of intense change that would have otherwise taken about five years, forcing organizations to rapidly accelerate their digital transformation journeys. As a result, the expectations and demands of citizens and customers of goods and services has only increased.

There is much to appreciate about rapid change but the need to keep pace with technological change can mean adopting new technologies, often before their vulnerabilities are fully understood.

Discovering flaws and security vulnerabilities can take time. However, the imperative to meet demands for an increasingly

digital-first approach to the delivery of products and services, increasing cyberattacks from both criminal and state actors, alongside a digital skills deficit in both businesses and consumers, means that the exposure to cyber risks is greater than ever. The tension between the drive to innovate and the need to keep data secure is something that can only be resolved if governments, businesses and citizens work together.

To add to the complexity, different regions, countries and cultures have differing legislation and regulations governing the management and movement of data, and this landscape is subject to constant change.

The increased reliance on connected, online systems has made businesses more vulnerable to cyberattacks as well as cybercrime. Businesses and organizations of all shapes and sizes need be more strategic, innovative and engaged in the way they approach cybersecurity if they are to stay ahead of these challenges and ensure their success in our increasingly digital future.

It's a challenge, but a crucial one — as Heraclitus also said: *"big results require big ambitions"*.

In this latest Atos Digital Vision: Cybersecurity 3, we explore some of the most pressing issues in cybersecurity and provide organizations with insights into how they can define or adapt their cyber strategies. Examining four core themes – digital transformation, digital sovereignty, zero trust and cloud – this paper provides ideas and guidance from experts in the cybersecurity field that can be directly applied within individual organizations.

Securing digital transformation

The pre-pandemic cybersecurity landscape was one, for the most part, where cyber risks were still perceived as an issue for individual organizations to grapple with alone.

COVID-19 upended the cybersecurity landscape. The rapid increase to remote working meant IT departments found it increasingly difficult to control the connectivity path of employees. As organizations adapted to the 'new normal' of the pandemic, many embarked on digital transformation programs despite some not having effective security mechanisms in place. This was despite becoming more reliant on public cloud and SaaS applications.

Even as security risks multiplied, in-house cybersecurity leads were operating with new systems, often with limited visibility of what employees were doing. As workers became remote, so too did customers, meaning that maintaining a secure online environment became doubly important for business.

These security challenges have been further compounded by the fact that organizations increasingly found themselves part of ecosystems of interdependent service providers, further reducing their control.

To address these issues my colleagues Vasco Gomes and Dan Schaupner highlight why companies should place cybersecurity at the centre of every digital transformation project they undertake.

Microsoft's Sarah Armstrong-Smith looks at how global instability has impacted risk appetite for companies and what that could mean for the future of cybersecurity. Also, Katarzyna Gołńska, looks at the culture of cyber and the importance of creating an inclusive work environment to identify and address cyber risks.

Understanding digital sovereignty

As organizations have come to terms with a wider array of digital risks spread across an increasingly diverse business ecosystem, policy makers and regulators have begun to raise concerns around data, technological and digital sovereignty.

The concept of digital sovereignty itself is critical yet poorly defined. In their article, Zeina Zakhour and Vasco Gomes seek to untangle the different aspects of sovereignty and explain why increased understanding is increasingly crucial to effective long-term decision making.

We should consider data sovereignty and technological sovereignty as the two pillars of digital sovereignty, reflecting the degree of control an organization has over its digital environment, including data, applications, software, systems, and hardware. Consequently, if organizations are to successfully achieve data sovereignty there is an urgent need for employees to take an active part in delivering this.

For many organizations this will require a radical cultural shift and a renewed emphasis on training. Effective navigation of these issues could be the difference between an organization's future success or failure.

Marianna Peycheva explores this in her article, addressing why it is important to put people at the heart of strategies to deliver data sovereignty. Barbara Couée writes about managing 5G risks and how collaboration is needed between national and regional institutions across the technology value chain.



The tension between the drive to innovate and the need to keep data secure is something that can only be resolved if governments, businesses and citizens work together on common solutions.



Reducing risk through zero trust

With so many organizations grappling with the need to defend an ever-expanding attack surface from cyber threats, one option is the so-called 'zero trust' approach to cybersecurity. A zero trust security model is deployed to ensure end to end cyber and cloud security, based around the principal that "trust is never granted implicitly and must be continually evaluated." In this environment, all users of a network must be authenticated, authorized and validated before being granted or retaining access to applications and data.

Zero trust has far-reaching implications for the way in which organizations protect against and detect cyber risks and Farah Rigal examines what this means in practice for those seeking to reboot their cybersecurity approach.

However, the full potential of a zero trust approach to cybersecurity has yet to be fully recognized. Aaron Chu's article examines how context-aware security can enable organizations to balance strengthening cyber defenses with a smooth, secure access experience. Meanwhile, Yann Morvan notes how a zero trust approach can best be calibrated and Panos Zarkadakis provides some tips on introducing zero trust and the benefits it can bring.

Securing the cloud

Many organizations have realized the cost and efficiency gains alongside the potential to quickly innovate offered by cloud computing. Whether organizations are moving to private cloud, hybrid cloud or public cloud, cybersecurity should be a central consideration in the migration process. Wolfgang Baumgartner looks at why it's vital to consider cloud security at the earliest possible stage in the migration strategy. Picking up the digital sovereignty theme, Pierre Brun-Murol and Vincent Dupuis take a look at the concept of Sovereign Cloud, while Harshvardhan Parmar examines how AI can help simplify cloud security.

There is a vast, evolving landscape with ever increasing and adaptable bad actors willing to exploit the positive and innovative ambitions of those who seek to deliver better, exciting services and opportunities from digital. Our collective role is to ensure that the digital society that is becoming omnipresent and essential to our lives is one that can be enjoyed safely and with confidence, for that we must stay ahead and keep innovating.

Trends in cybersecurity

The appetite for effective cybersecurity solutions as more organizations move to cloud-based services is growing significantly. Here are some key facts showing the growth in demand for cybersecurity products and the skills shortage that is affecting every part of the industry.



2.72 million

the number of additional cybersecurity professionals need to adequately defend their critical assets.¹



48%

of women say COVID-19 affected their career in cybersecurity in a positive way.²



1.3 trillion

the amount invested into Digital Transformation in 2018.³



526

cyberattacks against retail businesses per week.⁵



30%

of healthcare organizations considered zero trust to be a top priority in 2020.⁶



81%

the number of organizations that use at least two cloud service providers.⁷

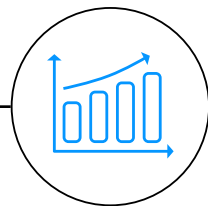


10 terabytes

of data stolen each month by ransomware threat actors between May 2021 and June 2022.⁸

Footnotes:

1. (ISC)² Cybersecurity Workforce Study (2021) <https://www.isc2.org/Research/Workforce-Study>
2. Tessian research (2021) <https://www.tessian.com/research/opportunity-in-cybersecurity-2021/>
3. <https://hbr.org/2019/03/digital-transformation-is-not-about-technology>
4. ISACA State of Cybersecurity 2022 <https://www.isaca.org/go/state-of-cybersecurity-2022>
5. Check Point Research (2021) <https://blog.checkpoint.com/2022/01/10/check-point-research-cyberattacks-increased-50-year-over-year/>
6. Orkta Inc. The State of Zero Trust Security 2021 <https://www.okta.com/sites/default/files/2021-07/WPR-2021-Zero-Trust-070821.pdf>
7. <https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy>
8. ENISA <https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg>
9. DCMS, Cyber Security Breaches Survey 2022 <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022>



60%

the number of enterprises
experienced difficulties retaining
qualified cybersecurity professionals
in 2021..⁴



39%

percentage of UK businesses
identifying a cyber attack in 2022..⁹

Industry focus:

Public Sector & Defense

The digital delivery of government services, which has been accelerated by the pandemic, has transformed how citizens interact with government and, in many cases, changed how those services are designed and delivered.

With ever increasing demands from citizens, particularly in developed countries with ageing populations who require more government assistance, digital transformation programs have helped deliver more for less.

While the delivery of digital services achieve efficiencies and value for money for the taxpayer, there is also an increased pressure on government budgets.

In the UK, for example, the government is looking to reduce the civil service by around 20% to save taxpayers money, while maintaining service and customer satisfaction levels. This can only be achieved by replacing legacy services, by delivering more digital services, building and running well constructed systems and doing it all at scale, efficiently, safely and securely.

However, while digital services are delivering efficiencies and value for money for the taxpayer, they continue to increase the attack surface that can be leveraged by bad actors, making the securing services even more challenging for government.

At the same time, all governments are facing an extremely competitive cybersecurity jobs and skills market. With limited budgets, it is increasingly difficult for them to hold on and secure



Governments across the world are seeking to do more for less. Technologies like AI, machine learning, digital IDs and biometric authentication can provide value for the taxpayer, improve services for citizens and also help make sure data is protected and trust is maintained in government services.

Adrian Gregory

CEO Northern Europe & APAC, Atos



the right talent and skills. As headcounts reduce and with a high turnover of people, providing essential continuous training and development in cybersecurity is often impossible, leaving governments playing catch up as they attempt to stay one step ahead of changing attack landscape.

Securing systems, while delivering more for less requires a new approach from governments to innovation. Standardization of systems and increased use of robotics process automation, artificial intelligence and machine learning along with process re-engineering can eliminate waste and improve services.

These must all be designed using the right cybersecurity and compliance frameworks which, when implemented, can deliver digital services safely and securely.

This can only be achieved by those with the skills and knowledge to maintain systems, detect and respond to the increase in cyber threats along with designing robust strategies to protect systems from both internal and external threats.

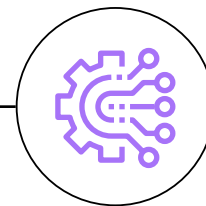
It is critical for governments to continue to partner with cybersecurity experts like Atos to ensure that systems are secure to maintain trust with the public and protect sensitive information. Only then can we deliver the services citizens expect at a reduced cost for taxpayers.



Digital transformation

How organizations can enhance customer journeys while keeping data, sensitive information and transactions safe.





Safety first? Delivering digital transformation

Adopting a new technology is challenging, but if organizations want to remain competitive and relevant, they need to continually adapt to demands from customers. Vasco Gomes and Dan Schaupner explore how and why organizations need to place cybersecurity at the heart of their strategy before embarking on any digital transformation.

Why you should consider cybersecurity risks and their mitigations before adopting new technologies or undertaking any new digital transformations.

Often, this requires adopting new technologies early on, long before we know everything about them. Specifically, before knowing the vulnerabilities or the best practices for designing, deploying, configuring and maintaining those new technologies.

This creates risk, yet is absolutely vital for the business.

Cybersecurity firefighters

The Chief Information Security Officer (CISO) and their team are expected to solve problems, quickly assessing how to mitigate a new technology's risks without impacting its value.

Sounds difficult? Yes, but business leaders naturally expect them to deliver. After all, that's what they are employed to do.

However, we often underestimate the complexity facing these teams.

Technologies are piling up because digital transformation adds to — but does not always replace — enterprise legacy applications. 5G is deployed in parallel with Wi-Fi, IoT and cabled networks. Mobile devices function alongside workstations. Even as business application teams implement DevOps, redesign applications into microservices and deploy infrastructure as code, other enterprise applications are still monolithic, deployed manually on virtual machines or physical servers. Legacy doesn't disappear — it shrinks.

For a CISO, the legacy vulnerabilities and misconfigurations remain a concern as important as new technologies. Because cybersecurity is only as strong as its weakest link, we cannot overlook one application, one scope, or one technology. It could be used as the entry point for an attack.

Addressing the cybersecurity skills gap

So say you are a CISO facing a multi-technology risk landscape. Surely, the answer must be to recruit more specialists to build up your teams through a technology focus. Unfortunately, it's not that simple, because this area is facing a shortage of skilled resources.

In its 2021 cybersecurity workforce study, (ISC)² estimated the cybersecurity workforce gap at 2.72 million professionals worldwide. These estimates seem to be confirmed by a jobs report by Cybersecurity Ventures, which also pointed out the nearly non-existent unemployment rate in the cybersecurity sector.

The demand for cybersecurity professionals is indeed outstripping the supply, despite the efforts of governments and businesses. According to (ISC)², "the global cybersecurity workforce needs to grow 89% to effectively defend organizations' critical assets."

2.72 million the global cybersecurity workforce gap in 2021*

* (ISC)² Cybersecurity Workforce Study <https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021ashx>

Cybersecurity is siloed and manual

Perhaps the solution to the skill shortage is to employ a common set of simple, effective tools that will help cybersecurity professionals do more with less. Here again, I'm sorry to be the bearer of bad news. According to Dr. Sridhar Muppidi, IBM Fellow and CTO for IBM Security Systems, "cybersecurity is among the most siloed disciplines in all of IT... The average enterprise uses 80 different products from 40 vendors."

In the cybersecurity field, critical tasks like identifying the risk exposure of an environment, implementing preventive protections and recovering normal operations after a security incident are still largely performed manually. Making matters worse, cybersecurity suffers from a lack of available standards. This is obviously an issue for automation, as most cybersecurity solutions require their own proprietary implementation.

Finally, although there has been progress using artificial intelligence (AI) to improve incident detection and response, AI for cybersecurity is still in its infancy. Here too, cybersecurity finds itself on the back foot, as hackers and other adversaries employ AI in their attacks.

Are all new technologies good technologies?

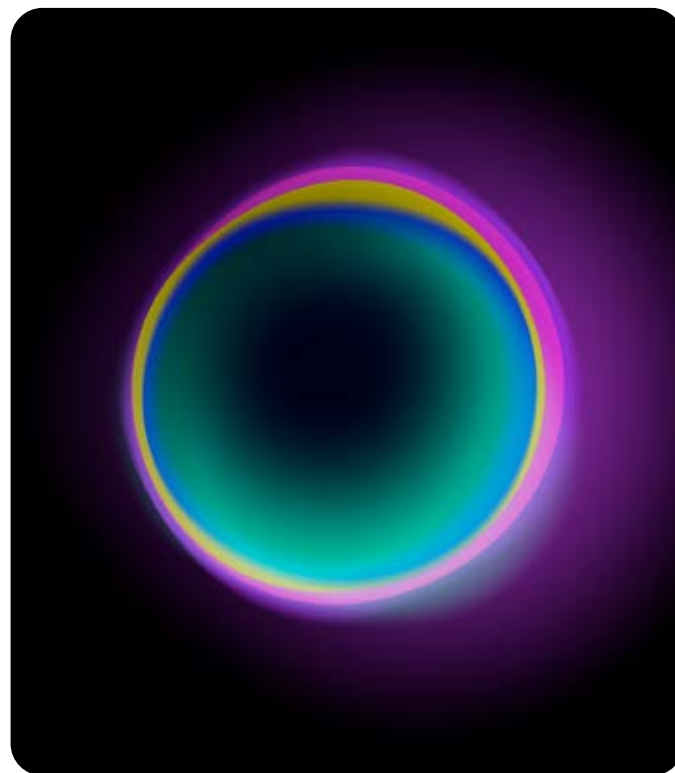
Given the situation, it's fair to wonder if we are adopting technologies too fast, if the technology is mature enough, and if we're trying to run before we can walk. These questions obviously need to be asked and considered carefully.

Ultimately, new, immature technologies will always need to be adopted — they are what makes a transformation possible.

With that fact in mind, how can we put CISOs in a better position?

Half the solution is understanding the problem, so the more closely you examine the conundrum we have outlined above, the closer you are to solving it.

Here are some of the key reasons why you should consider cybersecurity risks and their mitigations before adopting new technologies or undertaking any new digital transformations. They will go a long way to solving this conundrum.



1. Lower the cybersecurity landscape complexity

Recognize that a large number of cybersecurity tools creates a risk, and accept that one solution covering 10 controls could, in some situations, be better than 10 specialized tools covering one control each — even if they are individually stronger.

Adopt global standards rather than vendor-specific implementations. Although the cybersecurity domain has improved in the last decade, there is still a lack of globally defined and adopted standards. The Organization for the Advancement of Structured Information Standards (OASIS) is doing incredible work in this regard, and enforcing standards such as SAML, KMIP, PKCS#11, STIX, TAXII and many others.

2. Enforce cybersecurity automation

Use AI to alleviate cybersecurity analysts from lower-level tasks. This must be driven from different angles:

- Cybersecurity vendors can adopt AI to improve tool efficiency and management overload, which includes reporting, configuration and alerting
- Cybersecurity services can use AI to automate their service and orchestrate interaction between solutions
- Customer CISO teams can effectively manage the entire enterprise cybersecurity posture through an AI-powered global enterprise security dashboard

Use infrastructure-as-code (IaC) to your advantage, ensuring cybersecurity is also implemented as code. We've seen enterprises shrink production integration and deployment cycles down to a few minutes, but cybersecurity is an afterthought — still requiring several days to allow new communication flows or deploy cybersecurity agents on workloads.

Cybersecurity changes should be embedded in the IaC approach, with cybersecurity agents and communication flows embedded in the deployment templates. This could be extended to compliance reporting, encryption activation, provisioning of access rights and many other controls.

Accordingly, the cybersecurity team can focus on the deployment templates to verify cybersecurity compliance and ensure that production workloads have not deviated from it.

3. Increase available cybersecurity skills and improve work organization effectiveness

Train new cybersecurity analysts. At the same time, remember to upgrade and enhance the skills of cybersecurity experts to keep pace with the dynamic market. Train non-cybersecurity teams on the cybersecurity domains closest to their responsibilities. Most enterprise cybersecurity efforts are too heavily concentrated in the CISO office — responsible for watching the environment, but often called into sitting on design meetings and included very late in the secure software development lifecycle (SDLC). The digital transformation environment should have security engineering and design functions woven into the SDLC. It securely reduces the time-to-operate, mitigates risks and costs of rework, and ensures proper separation of duties among the stakeholders.

Embrace the power of collaboration, acknowledging that we cannot cover everything alone. The Charter of Trust initiative, of which Atos is a founding member, includes more than a dozen large corporations such as IBM, Siemens, NEC and others, who confidentially share information on cyberattacks with each other. This is a unique representation of this new age of cybersecurity, fostering dynamic protection and cooperation.

4. Do not hesitate to kill or zap a legacy technology

Question the continuation of legacy technologies. If it is confined to just a few small applications, consider that the cost of a complex migration or evolution might be worth the reduction of the above-mentioned negative impacts.

Don't believe the hype. At least, not blindly. Calculate the risks that any new technology may create and weigh them against the rewards it will bring to your business. Identify possible risk mitigations before adopting any buzzy new technology.

Cybersecurity and digital business risk management: Two sides of the same coin

Organizations are investing significantly in digital transformation. This is a prudent decision, considering the business value implications and the benefits to stakeholders.

As they transform, these organizations have the option of integrating security prior to implementation, or to fail to do so and repeat the mistakes of the past. The effectiveness of transformation is limited by how resilient its structure is against the threat environment. From the board and C-suite to line managers, all business leaders are responsible for managing risks and protecting next-generation information systems. While they may not need to know how to configure a secure cloud, they do need to know how to keep the enterprise accountable for expectations, and that includes all the considerations discussed here. The question is, who and what will be ready to help them navigate through these complexities?

Ultimately, cybersecurity should be a strategic consideration, discussed at the board level prior to considering a digital transformation.





*This is about all of us — we need to be aware of the ways we can be attacked.**

Tom Tugendhat MP
UK Minister for Security

Re-imagine: a world without boundaries

Microsoft's Chief Security Advisor, Sarah Armstrong-Smith, examines the impact of recent global instability on changing appetite for risk and what this could mean for how we approach cybersecurity in the future. Sarah goes on to look at the prospects for building frictionless, trusted and integrated networks, where organizations can successfully re-imagine themselves as digital-first ventures.

Did we become risk-tolerant during the lockdown? Many organizations have re-imagined themselves to be fully digital, but achieving this needs to be done in safe and secure manner.

If I could sum up the last few years with one word, it would be resilience. Whilst pandemics are nothing new, the world was not prepared for an event of the magnitude of COVID-19, and it forced many organizations to operate in ways that may have seemed incomprehensible just a few years ago.

As organizations contended with waves of lockdown, there was a rush to ensure services remained available and accessible. Despite the closure of many physical locations, digital services had to remain open as demand soared. As the weeks turned into months, apprehension eased, and stories of defiance started to appear. The rhetoric of "we can't do this" gave way to "we must do this." The risk-averse became the risk-tolerant.

If there is one thing we know about humans — when faced with major global events and extreme adversity, we bounce back stronger and rebuild. To do so requires us to continuously innovate. But despite every opportunity that presented itself for organizations, they also presented opportunities for attackers.

Attackers don't respect boundaries

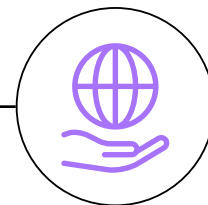
As many organizations revised their policies, such as enabling personal devices or collaboration tools to keep people online, cybercriminals took advantage of the situation. We witnessed a level of recklessness by the attackers and a willingness to test the boundaries of the defenses, to push further than they had dared before.

Changes to working practices, technology and infrastructure opened a variety of new and evolving attack vectors. These are no longer just focused on disruption but also destruction. It's a reality that we can't ignore, as we consider the effect of deliberate and sustained sabotage on an already weakened supply chain.

A world without boundaries should not mean a world that is not secure. It means our evaluation and perception of risk must continue to evolve. It requires a shift in mindset, from "it may happen" to "it will happen." Rather than fear the change, let's embrace it.

Crossing the boundary of technology and cybersecurity

We often talk about hybrid, as the divergence of legacy and cloud infrastructure. But to go beyond boundaries, we need to consider hybrid more holistically. No longer can CIOs and CISOs just consider the security of IT infrastructure. With opportunities for digital innovation extending further into the physical and biological worlds, they should also secure IoT/OT/ICS and robotics, combined with augmented and mixed reality and AI. This fusion, known as the internet of everything, is an ever-expanding ecosystem of digital connectivity and smart technologies that enables enhanced consumer and employee experiences and engagement. In parallel, it introduces additional risk and attack vectors that can be exploited. This intersection requires us to consider the interplay between digital security and safety, where the traditional need for confidentiality, integrity and availability also requires us to build for quality, endurance and reliability.



To be safe and secure in this digital world, you must start from a position which assumes you are neither safe nor secure. We must therefore design for and assume failure, by thinking of the myriad ways in which it could be physically and logically accessed by exploiting vulnerabilities. Having an assumed compromise/failure mentality requires that safety and security controls be deployed to counteract this. This is an evolution for chaos engineering, which is designed to test against these severe (but plausible) and turbulent conditions — pushing it beyond its boundaries.

Modernize with longevity and sustainability

We know that no system is infallible, and that risk is relative. Hence, it needs to be dynamic and constantly evaluate and react to the changing landscape. Speed and agility are of the essence, along with built-in digital protections that reduce complexity and provide longevity for our investment — especially considered against the backdrop of an economic downturn.

“
*A world without
boundaries
should not mean
a world that is
not secure.*
”

It sounds scary to re-imagine a world without boundaries, but what we're really building is a frictionless, trusted and integrated network, where siloes are removed and complexity is reduced by having end-to-end visibility of each interconnected touchpoint. Many organizations are already re-imaging themselves to be digital organizations, opening new lines of business, supply chains and experiences for employees and consumers. To do this in a safe and secure manner requires a network of trust. This means adopting an identity of everything mindset to explicitly verify and validate each entry and data point.

Forging new links between the physical and digital worlds dramatically increases the scope of enterprise security and safety. This is perhaps the next step in the evolution of zero trust, where we re-imagine a trusted network without boundaries that enables us to operate end-to-end to explore the art of the possible.

Delivering diversity and inclusion within cybersecurity

Although cyber is changing and there is increasing diversity, public perceptions change slowly and many women perceive the field as a “boys club.” Katarzyna Gołuńska reflects on her experience as HR professional in the field and the role of Diversity, Equality and Inclusion (DEI) in creating a truly inclusive work environment.

Do we need to encourage women to step in the cybersecurity field or should we shift our thinking so that we can achieve diversity of experiences on many levels?

Some time ago, during the International Women Day celebrations at Atos, I hosted a special event dedicated to female colleagues. The idea was to conduct an interview and create a space for meaningful debate between an experienced, successful woman — seen by others as a role model — and the audience. The special guest, a talented senior cybersecurity manager, inspired participants with their potential to tap into their strengths and the courage to “sit at the table.”

The resonance was amazing. Many days after the meeting, my guest and I received messages of appreciation and words of gratitude. Many women expressed that they finally felt it's time to swing into action.

That was an uplifting day for me and many other women, giving each of us the chance to observe someone just like you in a place where you aspire to be. Where — in a professional sense — you dream to be.

Rethinking the roots of the gender gap

It's worth noting that not every voice was so enthusiastic. Often, people have told me that they see no need for special engagement of women. Usually, they ask: “Do we really need to encourage women to step into cybersecurity? Come on! They are independent, adult people, they can make it on their own.”

To me, this is debatable. For some of my female colleagues, there was no need to follow a role model or support from a female mentor. They didn't feel compelled to find out how many women work here before joining the company. Such individuals entered the cyber field with courage, with a sense of mission, and with excitement to battle against cybercrime. Unfortunately, one size does not necessarily fit all.

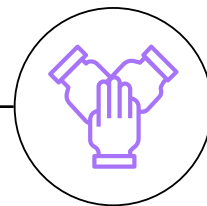
Many women perceive the field as a “boys club,” but this doesn't paint an accurate picture of the workplace we know. Although cyber is changing and there is increasing diversity, public perceptions change slowly.

Why not be a part of it?

We cannot overlook the fact that according to the (ISC)², in 2021, there are over 3 million unfilled positions in cybersecurity, with a workforce that is twice as likely to be male.

Somehow, for reasons discussed time and again, women stay away from cybersecurity. Authors of *The Future is Cyber – Opportunity in Cybersecurity Report (2021)* surveyed 200 female cybersecurity professionals to better understand why after years of debate, we are still struggling with the gender gap. The women interviewed highlighted three main emphasis points — equal pay, role models and a gender-balanced workforce — that would encourage other women to consider entering the field. So, do we really need to address these?

The answer is obviously yes.



The report provided some other thought-provoking revelations. They also surveyed 1,000 18 to 25-year-old adults to gauge interest in cybersecurity. Even in the young generation, men are still almost twice as likely to consider working in cybersecurity as women (42% vs 26%). We cannot underestimate the power of role models, as there is nothing more inspiring than seeing other women at the helm. For young women, it is important to see strong female representation in the organization. Let's face it: breaking stereotypes about the industry will take time.

The next shift: Diversity, Equality and Inclusion

I can imagine a time when we shift our thinking and debate from gender balance to diversity of experiences on many levels. That is to say, tapping peoples' identity-related knowledge and experience as a source of learning for the whole organization. All employees are total participants: seen, heard, developed, engaged and rewarded.

This approach is called Diversity, Equality and Inclusion (DEI). In a nutshell, if we create a truly inclusive work environment, there is no need to specify the type of diversity we want to see. We can then effectively build an inclusive, welcoming feeling in any department — including cybersecurity. Adopting this sustained change leads to higher-quality work, better decision-making, greater team satisfaction, and more equality (Ely, Thomas, 2020).

Increasing diversity, including gender balance, is only the first step. The time has come, and the ultimate goal should be to create a truly inclusive culture.



Industry focus:

Health & Life Sciences

Today's healthcare organizations face a daunting and ever-increasing level of cyber risk. Healthcare providers must protect sensitive customer data, while enabling appropriate sharing at the right time to improve customer care. The pharma and biotech industries are driven by the collection, analysis and sharing of valuable information between researchers. New technologies, like connected medical devices, must ensure the data they collect stays confidential.

The varied range of security needs means that the Health & Life Sciences sector has unique vulnerabilities and requirements. Coping with such a wide array of demands is made no easier by the perceived absence of a single partner to whom healthcare organizations can turn.

It is also vital for organizations in the sector to respond to long-term changes to the healthcare system. Rapidly rising costs, the difficulties of delivering healthcare in remote areas and a shortage of skilled and experienced health professionals are issues felt worldwide. As the population of industrialized countries continues to age and the number of people suffering from chronic conditions increases, the need for long-term care is growing.

Technologies including augmented reality (AR) and virtual reality (VR) will help leverage scarce expertise in the future. This can help in emergencies, where dedicated expertise might not be found in a

\$636.38 billion
the projected global
market for telehealth
in 2028*

hospital but could be accessed by liaising with an expert in a different location providing support during surgery. They can help researchers across the world collaborate more easily, but these in themselves create new cyber security challenges and vulnerabilities.

Healthcare organizations often rely on a series of vendors to help them manage

security, typically with non-integrated point solutions requiring additional onsite staff and expertise. This results in higher costs, an increased risk profile, and promotes "technology sprawl," a problem that can severely compromise their capacity to identify and address potential incidents. For healthcare organizations, strategic planning and consulting can be a valuable first step in reducing these risks.

In this challenging environment, how we secure and share data, sometimes across regulatory boundaries, will be key to an organization's success.

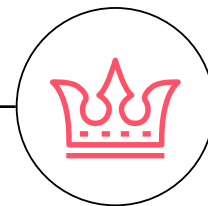
* <https://www.fortunebusinessinsights.com/industry-reports/telehealth-market101065>



Digital sovereignty

Where data is stored and processed matters to citizens and governments. Organizations must respond to the emerging regulatory environment.





Preparing organizations for a sovereign digital future

In a world where most data is processed and stored across geographical borders, often using foreign technologies, many governments are raising valid concerns around data, technological and digital sovereignty. In this article Zeina Zakhour and Vasco Gomes seek to untangle the different aspects of sovereignty and explain why understanding these is increasingly central to organizations' long-term decision making.

In a world where most data is processed and stored across geographical borders, often using foreign technologies, many governments are raising valid concerns around data, technological and digital sovereignty.

Before tackling this issue further it is crucial to agree on the definition of sovereignty. Data sovereignty refers to the degree of control an individual, organization or government has over the data they produce and work with (whether local or online). In contrast, technological sovereignty is the degree of the control the organization has over the technology it uses.

Data sovereignty and technological sovereignty are the two pillars of digital sovereignty, which can be defined as the degree of control an organization has over its entire digital environment, including data, applications, software, systems, and hardware. Which is aligned to the World Economic Forum definition of "the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create."

“

Atos defines data sovereignty as the degree of control an individual, organization, or government has over the data it produces and works with.

”

Taking a closer look

A closer examination reveals that cybersecurity is at the heart of data sovereignty and helps enhance technological sovereignty.

It is important that organizations understand that digital sovereignty is not an "all or nothing" proposition. Digital sovereignty exists in varying degrees on a scale which is constantly in flux.

Governments and organizations advocating for digital sovereignty need to adopt a risk-based approach. They must carefully assess their level of control over data and technology and take great care to ensure that sovereignty does not come at the cost of agility – a key factor to thriving in the Digital Age.

As many organizations make the massive move to the public cloud and embrace mobile/remote working (which has greatly accelerated during the COVID-19 crisis), they must measure the risks to their digital sovereignty. When they delegate technological choices data hosting and data processing to a provider, they put themselves at the mercy of that provider and its respective regulatory authority.

As a result, a hybrid cloud approach is gaining significant traction. Hybrid cloud leverages several different cloud solutions in parallel: from the least trusted to the most trusted, or even a disconnected, on-premises deployment. Data can be processed and hosted in different environments, depending on its business sensitivity.



Unlocking potential

This modular approach helps organizations leverage the potential of large providers to enhance the competitiveness of their less sensitive business processes. At the same time, they can protect their most sensitive business processes by keeping them under their own control or the control of more trusted providers.

Most importantly, organizations should not overlook the fact that digital sovereignty can become a competitive advantage by putting data sovereignty — and consequently, trust and transparency — at the core of their digital transformation.

Digital sovereignty is a growing concern in our increasingly digitalized world. Yet, policy makers, governments and enterprises must master the art of balancing digital agility with digital sovereignty, as this will be key to competitiveness.

Maximizing data sovereignty

Atos defines data sovereignty as the degree of control an individual, organization, or government has over the data it produces and works with. Accepting this definition leads to a big question: "How can an organization find the right degree of control?" Let's tackle it in four steps.

1

What is control?

Data has become the main support of our digital economy. For most companies, the digital strategy relies on a few critical pillars:

- Their data
- The way data are processed (algorithms, apps, compute)
- Who can access data and run operations and reports on them

If you don't have a clear view of these pillars, you don't have a clear picture of your business — which means you will soon be out of business. It's that simple.

You must ensure that access rights and identities are compliant with your digital strategy and based on the sensitivity of your data. That's the definition of control. Controlling your data is to specify and enforce who can do what with them at any point in time.

2

How can you increase control?

To control who can do what with your data, you have to start with identity and access management (IAM) and extend it beyond your employees to all kinds of IT, OT and IoT objects. However, IAM and encryption are often entangled in layers of applications, infrastructures and networks to run business applications and facilitate user experience. There is no such thing as perfect cybersecurity controls, so you must constantly monitor them for compliance and incidents and be able to respond and recover from them in a timely manner.

3

How much should you increase it?

Strengthening a security control can come at the expense of agility. So, for every security control, you should find the proper balance between excess and restraint. The best way to find that sweet spot is at the core of cybersecurity: What kind of risk am I addressing and in which form could it happen? You won't apply the same level of control to mitigate an espionage risk, external influence, usage/operation prevention, or data loss, whether accidental or malicious.

4

Is all data born equal?

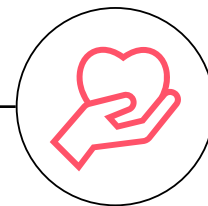
Protecting all assets the same way often results in protecting none of them correctly. Indeed, security controls tend to be attracted by the weakest link. Data classification is a huge program that should never be underestimated. But, to give you a sense of scale, we have observed through many projects that, in average 80% of customers' data are not sensitive, and that the remaining 20% can further be split into 80% "just sensitive" and 20% highly sensitive. It is not unusual that the split is close to that double 80/20 rule: 80% non-sensitive, 16% sensitive and 4% highly sensitive (maybe even classified).



Atos is actively responding to the growing concerns around digital sovereignty, responding to new requirements at EU and national level with certified cybersecurity products and solutions.

Peter t' Jong
CEO, Atos Netherlands





Why people are at the heart of mastering data sovereignty

Data sovereignty is one of the biggest challenges businesses face today, with many organizations recognizing it as a strategic operation rather than simply a tactical issue. In this article, Mariana Peycheva notes the extent to which employees are at the cutting edge of digital transformation and explains the crucial role of data privacy professionals in supporting their colleagues and organizations to successfully transform their data governance and achieve data sovereignty.

With technology evolving faster, providing more sophisticated products and services for protecting sensitive data, we should not ignore the role of people in achieving data sovereignty.

Data sovereignty is one of the biggest challenges businesses face today. It can be considered the new currency of the business world and a well understood norm for senior management, who already recognize data sovereignty as a strategic operation. They don't see it as a tactical issue any longer.

Technology is evolving faster, providing more sophisticated products and services for protecting sensitive data. However, we cannot address the data sovereignty challenge without considering its main cornerstone: people.

Are people the primary barrier to achieving data sovereignty?

When reading about major incidents concerning data leaks, we almost automatically suspect the leak to be caused by cybercriminals based outside of the organization. However, the sad truth is that most of them are caused by human errors — as many as 66%, according to the Dutch Data Protection Authority.

Recently, the Australian government admitted that they are more fearful of human errors than cybercriminals. Mistakes were the primary cause for 74% of the data breaches reported by government agencies in 2021, while the percentage was just over 30% for other sectors.



According to the European Union Council, non-malicious threats are a significant part of the list of top cyberthreats in the EU, most of which result from human errors. If these numbers are not alarming enough, consider the GDPR fines issued in 2021: Amazon – €746 million, WhatsApp – €225 million, Notebooksbilliger.de – €10.4 million.

There are certain patterns of human errors which lead to these situations.

Many employees use public Wi-Fi networks for sensitive business operations or use their personal smartphones for work-related activities — often with minimal security on their devices. Other real-life examples include sharing their corporate device with family and friends, having weak passwords and even using the same password after a breach. In its 2020 Data Breach Investigations Report, Verizon asserted that misconfiguration is among the top causes of data breaches. There are many more examples and the gravity of the situation is clear.

Growing awareness

Rather than merely blaming employees, it is essential to start improving the overall culture of data protection and develop better processes to secure business data. Data sovereignty is largely dependent on the organization's culture. Recognizing the challenge from the highest management level and understanding that data protection is part of the organizational vision and responsibilities will help create a strong culture among employees — who remain the first and weakest level of defense.

Logically, the policies and process that will follow are the second step, but how do we ensure that they are the right ones? Strong processes and more advanced technology for user authentication, locking devices, and security configuration guidelines could avoid many of the issues mentioned above.

Building data sovereignty consciousness at every level

Compliance with local data privacy laws is not the only reason for doing this. The nature of the business must also be taken into consideration. Effective data classification is a must. Knowing where the critical data is stored and who has access to it

provides good visibility so processes and controls can be applied according to the different data classifications. Companies can focus investments and effort to mitigate the risk for the sensitive data, rather than wasting resources on low-risk areas.

Data privacy training for employees should be a natural process, but not every employee needs to be trained in the same way. Employees who process and access sensitive data should be approached differently.

At the same time, there should be mandatory training focused on best practices and requirements for all employees, to ensure that they understand the concept and consequences of data leakage.

Different departments often handle their data without any clear guidance on how it should be done, so simple and understandable guidelines should be made available to employees.

Managers should be included in the process and should take responsibility to ensure that their teams understand and comply with standard processes. Open discussions with the employees impacted by the processes and gathering their feedback is important for subsequent optimizations.

Adapting training to each department's needs

Because the processes can make or break an initiative, the organization should employ trained professionals to create them and understand data sovereignty within the department. The skills of an organization's data privacy and security specialists will differ based on the organization's scope, but there are well recognized trainings and certifications available on the market.

Investing in the continuous education of your professionals will provide a return on the investment in the future. Some examples include the DPO Certification from the EU GDPR institute, the Data Protection Certification Course from the European Institute of Public Administration, and ISACA certifications like Certified Information Systems Control, Certified Information Security Manager, Certified Data Privacy Solutions Engineer and others. These can be complemented by technical training from vendors and cloud providers. Working with legal experts who specialize in local and global data privacy regulations is a non-negotiable requirement.

“

China is taking a leadership role in digital innovation, with Chinese technologies transforming global businesses. This also comes with a strong data sovereignty requirement and strict Cyber Security Laws that local businesses need to comply to. Atos helps companies (whether subsidiaries of foreign MNCs or local enterprises) combine innovation with regulation, by using Cybersecurity as an enabler. For instance, we introduced global Detect and Response strategy within the local cyber security context to identify, monitor and respond to current and future cyber threats..

Tan Chee Wooi

Director, Presales & Solution Management BDS Cybersecurity, APAC; Member of Atos Scientific Community

”

Working together to create inclusive digital sovereignty

In the 21st century, employees are constantly facing digital transformation, so the organization should take all necessary steps to make these processes easier for them. We must avoid at all costs a situation where the organization's data privacy and security function is perceived to be pointing a finger at other departments and accusing them of mistakes. In fact, it should be quite the opposite. The data privacy professionals are there to support the other business units and having the right professionals guiding the data governance is a key factor.

Closing the human gap in data sovereignty is undeniably a challenge — but not an impossible task. In doing so, the organization will address one of the biggest challenges for data sovereignty.



The CISO perspective on digital sovereignty

The battle for digital sovereignty is well underway, with organizations both large and small now working to adapt their technologies and strategies accordingly — especially for those processes that rely on data processing. In this article, EDF Group's Chief Information Security Officer, Olivier Ligneul provides his perspective on what this has meant for his organization and how organizations can collaborate effectively to expand digital autonomy in the future.

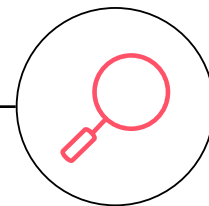
EDF Group's Chief Information Security Officer, Olivier Ligneul offers his perspective on how organizations are responding to the "battle for digital sovereignty" and adapting their technologies and strategies to ensure sovereignty and trust are maintained.

As far as our company (Électricité de France) is concerned, the battle for our digital sovereignty is well underway and campaigns are being conducted internally. We have taken digital sovereignty into account and adapted our technologies and strategies accordingly — especially for our business processes that rely on data processing. These are the cornerstone upon which the concepts of sovereignty and trust are built.

Our goals, as an energy producer, are to secure electricity production and to develop new production sites. In addition, we are also committed to keeping our high service levels to customers, contributing to energy savings, protecting the rights of citizens and the confidentiality of consumer information, and securing our end-to-end supply chain in order to protect our strategic company assets.

Digital independence is essential for us to stay in control of our destiny. We must maintain our ability to choose our technologies, and independently evolve our sovereignty activities over the long term to protect our company, our customers' interests, and our future.





Cybersecurity itself must be protected to develop a self-defense capability

To reach an adequate protection level, we must be free to choose our strategies for countering attackers and therefore to choose the best protection for our critical assets and any trade secrets.

We must preserve and control our freedom of choice as well as guaranteeing that our infrastructures are shielded from outside threats. Technological independence can also be a challenge for companies, which is why reversibility processes are necessary, even mandatory, to guarantee the continuity of our services.

To further illustrate, here are some examples of sovereignty issues:



Digital twins (like a digital copy of a site plan, an event simulator, or modeling tools for nuclear power plants) use sensors to provide a link between the real world and the digital world. The integrity of the data generated by those assets is essential, as they contribute to the business's decision-making processes and strategies.



Artificial intelligence (AI) can mimic the problem solving and decision making capabilities of the human mind, but how can you guarantee the integrity of algorithms and their outcomes? Can you secure the decision cycle based on the intent of the designer? In short, we must be able to verify that algorithms serve the original intent of the designer and haven't been compromised.



Similar questions exist about blockchain, which ensures the integrity, traceability and enforceability of transactions by using a shared, immutable ledger to provide a secure, immediate exchange of data or documents between multiple parties.

How can we guarantee the integrity of the ledgers and thus the validity of the data or document? Protecting them against intrusion is key, as compromised data or falsified documents can have real strategic and business impacts and lead to a financial loss for the organization. However, sovereignty and autonomy are not just about security, technology, or the economy. They also encompass human factors.

There is a growing need for skills in the cybersecurity fields, which is why our organization has implemented training pathways to create career opportunities in cybersecurity. Furthermore, we also conduct cyberthreat awareness campaigns for everyone from end users to decision makers.

Cybersecurity initiatives to expand digital autonomy

To expand our digital autonomy strategy in the EU cybersecurity market, our Group is one of the founders and key partners of Gaia-X. Gaia-X is a European initiative that is developing a software control and governance framework and implementing a common set of policies and rules that can be applied to any existing cloud or technology stack. The Gaia-X framework is meant to be deployed on top of any existing cloud platform that chooses to adopt the Gaia-X standard. The main objectives are to enable transparency, controllability, portability and interoperability across data and services — along with protecting European sovereignty.

The objective of Gaia-X is to define what sovereignty means and how it will be applied in our data market by ensuring controllable services and verifiable independence from legislation or influence by non-European actors. This initiative has been publicly and supported by many public institutions as an important evolution in supporting the advancement of European sovereignty. European users will require Gaia-X compliant services, and non-European players will be free to adopt this sovereignty framework in order to operate in Europe.

Martine Gouriet, EDF's Director of Digital Uses, is leading the work related to Gaia-X labeling, and we recently launched a survey of all Gaia-X members to establish the rules and criteria for three different types of labels.

The Gaia-X framework will define common service descriptors, compliance verifiers and registers — which will be accessible to all for inspection. Gaia-X labels will be assigned only to services (not operators) verified to be compliant with the labeling framework. Non-European players will be able to offer services labeled as level 1 and level 2. However, the criteria require that non-European players cannot be the main providers of level 3 services, although they can cooperate with the main service provider.

In the spirit of autonomy and independence, other initiatives are also underway, such as our active participation in ECSO, the European Cybersecurity Organization. The main goal of ECSO is to coordinate the development of the European cybersecurity ecosystem and support the protection of the European Digital Single Market, ultimately contributing to the advancement of Europe's digital sovereignty and strategic autonomy. ESCO also contributes to the establishment and development of a network with our peers.

Our participation in the Brienne fund and our internal discussions on trusted cloud also contribute to our digital autonomy.

Finally, as a global organization, digital sovereignty contributes in a positive way to the implementation of remote working. Along with other initiatives, it also helps our global organization share business and technical expertise across the Group and within our extended enterprise.



Managing the risks around 5G

Security and sovereignty issues cannot be addressed alone. As 5G technology matures, organizations will require collaboration between national and regional institutions across the technology value chain. In this article Barbara Couée examines how organizations are working together to unlock the huge infrastructure and platform capabilities of cloud providers and offer their customers an interoperable platform ecosystem.

"In three to four years, cutting 5G will mean cutting power in terms of impact... The impact [of an attack] would be terrible for our economy."

These are the words from Guillaume Poupard, Director of the French security agency ANSSI (Agence nationale de la sécurité des systèmes d'information), referring to the risks of eavesdropping on communications — which led major Dutch providers to block Huawei from their core networks, and resulted in connectivity outages in 5G.

In the US, this strategic importance of 5G has already led to restriction on Huawei and ZTE equipment.

In some non-EU countries like the UK, Huawei was banned and regulations have been enacted to limit its use. The Telecom Act in the UK prohibited mobile network operators from purchasing Huawei equipment after December 2020; they are now asked to remove Huawei from UK's 5G network by 2027.

In Europe "faced with the risks of 'third-party state interference,' Europeans want to guarantee their 'technological sovereignty' over 5G networks and the data that will circulate there." The European Union is therefore considering amending cybersecurity laws to apply extra security measures for critical infrastructures, including 5G mobile networks. This could lead to limited usage or even a ban on equipment from providers suspected of espionage.

In parallel, with network virtualization and cloudification, the significance of hyperscalers is growing (AWS for edge, Google Anthos, Azure Stack). This raises questions about the level of control on all planes of sovereignty — data, technology, operations — and the risk of dependency on US capabilities.

In view of the high stakes, countries have now no choice but to get involved in the deployment of future networks in order to guarantee security & resilience.



How is the EU pushing for technologically sovereign 5G solutions?

If Europe already benefits from patents owned by Nokia and Ericsson, disaggregating the network into microservices also opened the door to alternative choices to this duopoly in terms of infrastructure equipment. Deutsche Telekom, Orange, Telecom Italia (TIM), Telefónica and Vodafone are participating in Open RAN demonstration projects and campaigning to build an Open RAN ecosystem for Europe, with the goal to ensure that Europe continues to play a leading role in 5G (and in future 6G networks), despite an ecosystem (Airspan, AltioStar, Casa Systems, Parallel Wireless, Radisys, Asocs, Intel, etc.) that is mainly non-European. Among the hot topics: the European alliance in cloud, semiconductor issues, and interoperability standards and openness.

There is a push to move from a heterogeneous approach to federated European 5G, overcoming a lack of coordination between EU members. Accordingly, institutions are attempting to re-gain sovereignty and develop ecosystems over the next five years, through European and national funding programs.

Examples of European projects to foster 5G and 6G EU sovereignty include the IPCEI[1] on Microelectronics and Communication Technologies, the IPCEI on Next-Generation Cloud Infrastructure and Services (IPCEI-CIS), and The Smart Network and Services Joint Undertaking (SNS JU) for 5G/6G.

In the SNS JU alone, this is more than €900 million over the next seven years that EU plans to allocate to help European players build the research and innovation capacities for 6G systems and develop lead markets for 5G infrastructure. This includes communication components, systems and networks, and "radical technology advancement" with a strong vertical approach. Cybersecurity is part of this plan, with focus areas like connectivity resilience, trust, threats, AI, and secure privacy preserving methods in a multi-stakeholder, or multi-tenant world.

Sovereignty is about the level of control. Who has control over the 5G cloud to edge, network and data?


5G networks are evolving to cloud-native architectures, pushing communication services providers (CSPs) to fundamentally transform their infrastructure and operating model – and avoid being squeezed to the connectivity between antennas and cloud.

To benefit from the huge infrastructure and platform capabilities of cloud providers and/or offer their customers an interoperable platform ecosystem (mixing connectivity infrastructures, cloud-to-edge infrastructures and software), CSPs have built partnerships with network equipment providers and hyperscalers. These include, among others: Google with Telefonica, AWS with Orange and Vodafone, and also Microsoft with Vodafone and Telefonica.

Understanding and assigning responsibility

Operators are responsible for the security of customer data, and for the confidentiality of data exchanged on the network from user endpoint to 5G Core. But when networks are managed by foreign companies, how trustworthy can they be — especially when it's impossible to know if and how data can be used?

In order to be agile to offer service creation and monetization, deployment automation and orchestration are required in both central and local clouds for network capabilities and applications. In this context, security enablers can help counter-balance the challenge of untrusted environments. Key strategies include encryption and advanced access management, deployment of AI to identify misconfigurations and suspicious patterns within networks, and technologies ensuring privacy-enhanced services (e.g. with a focus on preserving confidentiality and ensuring traceability).



Governments and citizens around the world are concerned about where and how their personal data is being used and stored. Understanding the emerging digital sovereignty landscape is vital for governments and businesses, so they can adapt to fast changing regulatory environments and to the demands from customers.

Mike Green

Managing Director, Atos Australia

Industry focus:

Financial Services & Insurance

Digital services have transformed the Financial Services and Insurance sector. The shift online has reduced costs, improved efficiency and competitiveness, and improved customer journeys. However, it has also created new opportunities for both criminal and state actors to exploit vulnerabilities.

The sector has responded by becoming a leader in cybersecurity. The costs, both financially and reputationally, are too great to get things wrong. But a rigorous approach to securing every single transaction must be balanced with usability and accessibility for customers. Adding complexity discourages use, while too many false positive rates on transactions can harm customer relationships.

The move to cloud has also increased risks. While cloud has brought a range of benefits for both consumers and the sector, it has also opened up new vulnerabilities. Cloud providers can ensure the security of cloud services, but if an organization doesn't know who is accessing its network or sharing data, or if endpoints aren't secure, cyber criminals can strike and move through networks at speed.

Digital ID will be a significant tool in helping to maintain security. Technologies like biometrics, can help increase trust in the process. With the addition of artificial intelligence and machine learning, red flags can be processed in near real-time to avoid the costs of retrospective fraud mitigation.

**2,527 incidents/
data breaches**

in the FS&I sector of which
690 included confirmed
data disclosure.*

But for many in the sector, the regulatory environment has still not caught up with the needs of consumers or the industry. The responsibility for security has to be shared between the sector, their digital service providers and customers. Institutions must be able to understand their obligations. The right evolution of the regulatory landscape will combine incentives to share best practice with mandatory requirements, but much of this is yet to be decided.

In a world where fraud, risk and compliance dynamics are constantly changing, our role is to help organizations identify issues and manage this landscape as well as responding to threats as they appear, to ensure organisations remain operationally resilient. At Atos, we are the trusted partner to some of the world's biggest banks and insurers, because we understand that trust in security systems, once lost, can have catastrophic impacts on confidence. This doesn't just impact an individual brand but has knock on effects to the whole industry.

With new technologies and changing regulatory environments, the Financial Services and Insurance Sector must constantly update and refine its approach to cybersecurity to remain resilient and best in class.

* Verizon Data Breach Investigation Report 2022 <https://www.verizon.com/business/resources/reports/2022/>



Zero trust

How a zero trust approach to cybersecurity can protect against external and internal threats.





Risk in a zero trust world

The zero trust principle envisions cyberspace as a hostile environment where no trust can ever be established and where all parties are assumed to be constantly involved in hostile activity. The implications of this for how we approach cyber risks are far reaching and in this article, Farah Rigal discusses some of the ways it is already transforming approaches to detecting and protecting against cyber risks.

How the zero trust approach is transforming the way organizations seek to detect and protect against cyber risks.

Cyberspace is a wide-open arena, not a closed circle where you need to be prudent only until trust is established with the parties involved. The zero trust principle takes this statement to its extreme — portraying cyberspace as a hostile environment where no trust can ever be established, and where all parties are assumed to be constantly involved in hostile activity.

The protect/detect dilemma

Imagine that you have handed your house keys to your teenager for the weekend. Ideally, you get to enjoy a romantic weekend away while your kid can have a few friends over without a bothersome adult presence.

Trust occurs when you simply assume things will go well. Zero trust requires you to constantly assume that you are being fooled by your teenager — for instance that he or she intends to throw a big party that you have strictly forbidden.

It is natural to consider how to protect before you detect, simply because protect comes first in every cybersecurity framework and checklist I can think of. However, you must assume that the protect controls will fail in the face of a motivated adversary or a compromised insider. In our example, your kid may distribute the entrance code to your building (if there is one) and would also be in the position to lock up your family's trusty guard dog so it cannot sound an alarm.

Eliminate the blind spots

Continuing with the party example (although I'm not that kind of

parent at all), let's conclude that a security camera is the best way to verify your assumptions that a wild party is taking place without your permission.

One option is to make the camera clearly visible, thereby acting as a deterrent against misbehavior. However, the more paranoid you are (i.e. exhibiting zero trust), the better you should hide it. The reasoning is simple: If the camera is visible, it is possible for bad actors to hide in its blind spots, or even feed it wrong or understated data.

In a cyber environment, threat detection measures and security event analytics act in a continuous untrustful paranoid process loop. The less that adversaries know about them (where they are placed, what exact tactics, techniques and procedures they can detect, etc.) the more work it is for adversaries to evade control. However, it's important to note that security simply by obscurity is not the fundamental principle here.

Keep your friends close, and your adversaries closer

All activity needs to be collected and analyzed, even if it doesn't raise any alerts. Successful authentication events, calls to selected authorized system libraries, opening connections to other systems, and other similar activity need to be monitored to detect any anomaly in volume, timing or other meaningful attributes. This means that in addition to the security camera, the video needs to be analyzed by computer vision software for anomalies and suspicious patterns.

The rights to turn off the camera (i.e. event monitoring or reporting) need to be segregated from other administrative rights as much as possible. When a system fails to report its events to the monitoring solution, it should be treated as a separate security event and investigated as such.

From cyberspace into the real world

The latest cyber breaches have confirmed that motivated adversaries can circumvent the strictest security controls, no matter how sophisticated they are. In targeted attacks, the offenders conduct detailed reconnaissance to find the path to evade all controls.

Non-targeted attacks can also make use of the latest attack techniques, including evasion capabilities. Some attacks are even named after their ability to fool security controls. To qualify as a Highly Evasive Adaptive Threat (HEAT), a threat needs to successfully bypass at least one of several traditional security defenses. As they proliferate, it is increasingly important to deploy multi-vector threat monitoring to reduce dwell time and response time in the event of a compromise.

Exploiting trust

Ironically, some breaches have also demonstrated how offenders can use trust adversely. In the high-profile SolarWinds Sunburst backdoor attack, the hackers exploited the established trust in federated (hence trusted) authentication environments to extend their access rights and establish long-term access. The famous watering hole attack falls in this category as well, because it relies on poisoning or compromising a site that the victim commonly visits and trusts.

Taking advantage of a trust relationship to gain or extend malicious access is a documented known attack technique. In the Mitre Att&ck® framework, this technique is known as Trusted Relationships, and seeks to gain access through a less scrutinized path. This may be that of the supply chain or the system administration team. It is unfortunate when high trust and elevated rights are associated, despite the well-known principles of segregation of duties and least privileges.

Many controls can mitigate the risk of compromised trust relationships, such as the good practices of identity and access management, and secure-by-design network and system architecture. Yet zero trust loyalists will prefer to back these with multifactor authenticated access, through bastion systems with session monitoring, event correlation and content inspection.



Zero trust: A continuous work in progress

Cyber defenders need to look at continuously improving their security systems. In collaboration with the testing and red-teaming function, they need to adopt a zero trust mindset and continuously investigate where it could possibly fail.

As long as you can think of any way that your teenager can circumvent your controls, you need to strengthen your plan and build a truly watertight response. Don't stop until you see yourself losing all the possible benefits of this hypothetical weekend getaway!

“

The APAC region is a hub for innovation, but with new technologies come new cyber threats. Understanding and responding to vulnerabilities in new technologies and adapting cybersecurity strategies to emerging risks is a key demand from organizations across the region.

Daniele Principato
CEO, Atos Asia Pacific

”

The power and potential of context-aware security

Aaron Chu examines how context-aware security uses situational information to determine the nature and risks of individual access requests to effectively protect information and resources within organizations.

How context-aware security enables organizations to balance strengthening cyber defenses with a smooth, secure access experience.

Security is a major concern in the digital age. The proliferation of mobile devices and cloud computing has made it simpler and more rewarding for hackers to steal information. At the same time, users are being targeted by cybercriminals who employ malicious software and social engineering techniques to gain access to personal or organizational data.

Context-aware security is an access control design strategy that uses situational information to determine the nature and risks of an access request before granting appropriate access permission to the protected information or resources within an organization.

How does context-aware security work?

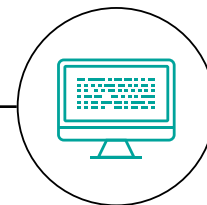
Let's look at an example that illustrates how to apply context-aware security:

1. When I want to withdraw money from my bank, they need to know who I am. Once authorized, they look in my account to see how much money I have. If I have enough funds for the request, they give me the amount I asked for. Simple enough, right?

Context-aware security enables organizations to strengthen security without hindering what users want to do.

2. What if I make my withdrawal request over the phone without any formal identification? Does the bank still allow me to withdraw cash? If I had lost my wallet and passport during an overseas trip, I could be stuck if the bank refused access to my money!
3. With context-aware security, the bank could still give me all or part of the money I requested by considering the circumstantial information about my request.
4. My bank can examine the time and location (environmental factor) when the request was made, request a personal interview with a bank manager at a nearby branch (additional authentication), and confirm the reason (context) for my withdrawal request.
5. While evaluating all these additional details about my request, the bank can quickly build a risk profile for my withdrawal request, then make a comparison against other known risk factors such as my past withdrawal patterns, local crime statistics, and the current probability of malicious withdrawal requests (threat intelligence). More importantly, the bank must determine how much money it is willing to lose if this is not a genuine emergency cash withdrawal request from me (risk tolerance).
6. In this scenario, my bank agrees to give me enough money to pay my hotel bill and fly home the following day.

Context-aware security enables organizations to strengthen security without hindering what users want to do. It allows users to have a smooth, secure access experience without going through an onerous series of multiple authentication mechanisms.



A smart analytics engine is often used to evaluate the risk factors from multiple sources and produce appropriate decisions for the security controls to enforce prescribed access in real time.

Zero trust and context-aware security

Zero trust security assumes the network perimeter-based protection is no longer effective, because your data assets and resources now reside in an open and interconnected world. No longer should any request to your network, environment, application or data be trusted.

Instead of granting access to everything upon login, regular identity verification for requesters and devices is required before minimum access is granted — along with a prescribed network route to the requested environment and a defined set of data to be made available. The access granted is time-limited and the use of this access privilege is under constant monitoring. Any deviation will trigger changes in the granted access or elevated authentication.

Context-aware security is a key component of implementing zero trust security. We can set up many smaller protected zones in an open environment by using identity as the protection perimeter and deploying context-aware security control as the gatekeeper.

This type of zero trust security implementation offers strong protection for your data and resources within the secured zone. The frequent examination of their intentions and behavior makes it extremely difficult for an internal or external intruder to move across the guarded zone without being detected.

Apart from reducing the chances of security breaches, context-aware security also reduces the amount of constant authentication challenges demanded by the zero trust principle of “never trust, always verify.”

Regular evaluation of how the least privilege access is granted and used provides real-time feedback to the context-aware security control as an additional factor, enabling access to be fine-tuned without bothering the user with extra authentications. Accordingly, it is a great way to implement a frictionless security service without impacting user productivity and experience.

The journey towards a trusted business

There are many cybersecurity products and services that offering context-aware security capabilities today. However, both zero trust and context-aware security are based on cybersecurity design philosophies and simply not about a product implementation.

Zero trust and context-aware security are means to create a highly trusted environment for your customers to confidently interact and do business with you. Such an environment requires transparency and traceability of all transactions carried out within it.

The business will need visibility into who has access to what information, and what transactions took place and when. Most enterprises are unlikely to implement this kind of capability with only a single technology.

The best approach is to create a vision of what your trusted environment should look like based on your business objectives, what risks you want to mitigate, and what data you need to protect.

1. Understand the goals and requirements
2. Where to deploy controls
3. How many controls
4. Make them all work together

Once the cybersecurity goals and requirements are understood, you can decide where the context-aware security controls can be deployed, how many controls are needed, and — more importantly — how they will work together seamlessly. The guiding principles of zero trust can be used as a compass to map out your transformation journey, positioning your business as a trusted brand in your industry.

IAM at the heart of the zero trust approach

As more companies respond to the rapid rise of cyberattacks of all kinds, particularly ransomware, many are being pushed to expand their defense perimeters by applying a zero trust approach. In this article Yann Morvan provides an explanation for how this approach can work and how best to calibrate its effectiveness.

As more companies respond to the rapid rise of cyberattacks, many are expanding their defense measures by applying a zero trust approach, but how can this work and how can the effectiveness of this best be calibrated?

The rapid rise of cyberattacks of all kinds, particularly ransomware, is pushing companies to expand their defense perimeter by applying a zero trust approach. But how does it work? And more importantly, how can its effectiveness be calibrated?

Often, an organization's first instinct is to implement zero trust at the network level by reinforcing access to company resources, particularly via VPN for remote workers. However, in the event of an intrusion on the company network, access to information depends entirely on user access rights. It is therefore necessary to manage these access rights to ensure minimal user privileges. This is where the role of identity and access management (IAM) takes center stage.

IAM: The cornerstone of zero trust

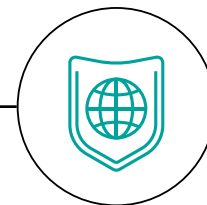
The constantly increasing number of applications in use, especially SaaS (Software as a Service) applications in the cloud, leads to an increase in the number of identities for the company and for each user.

This translates into the at many more access doors for hackers. All these identities, regardless of their location, must follow the same security policy and the same constraints as the main identity of the user in the company. Here again, IAM plays a key role in the zero trust policy being implemented — helping maintain control over user identities and guaranteeing the minimum access rights for each resource accessed, whether internal or external.



On the other hand, a large proportion of intrusions employ user identifiers, often taking advantage of weak passwords. Tightening an organization's password policy may lead to a less-than-optimal user experience and can become counterproductive. The answer to that is to move to stronger authentication methods that are more acceptable to users. Because users now log-in from various locations and devices, these authentication methods must adapt to the criticality of applications and data — as well as to the user's login context. This calls for an integrated IAM solution, where identity governance and access (IGA) functions are connected to authentication and access control functions, possibly in a dynamic way.

Depending on an organization's business and need, information systems are now available to the outside world, enabling partners and even customers to access certain applications. Inevitably, this widens the attack surface for hackers, making it extremely important to extend the zero trust approach to this new set of users and integrate them into the IAM solution. You need to be able to manage and control their access rights, even if you delegate the administration of these identities to third parties or to the users themselves.



Managing identity as the new benchmark in zero trust

Identity federation forms an integral part of IAM, making it possible to limit the proliferation of user identities, especially in SaaS applications. In doing so, the company retains sovereignty over user authentications, as well as control of access rights to applications. It is an application of the zero trust approach by limiting the trust given to applications and the functionalities they provide, without entrusting them with the primary functions of authentication and authorization.

User lifecycle management, enforcement of a comprehensive security policy, approval of rights by key individuals, and automatic provisioning of accounts and access rights ensure that only authorized individuals have access to applications and data with minimal rights. This shows how central IAM is to a zero trust approach. Adding identity federation and multi-factor authentication (MFA) greatly reduces attack surfaces while providing a better user experience.

For applications outside of identity federation, adding a single sign-on (SSO) brick (either desktop or web-based) strengthens security by increasing the complexity of passwords that are no longer known to users. Of course, it is necessary to use MFA for the primary authentication. This is another way to decrease the attack surface and extend the zero trust approach while making life easier for users.

Numbers matter: The role of governance and analytics

Just like in any security strategy, governance is an integral element in the zero trust approach, as is IAM. Dashboards and alerts from

both identity management and authentication and access control bricks enable proper execution of the policy and the detection of deviant behavior — like multiple requests for specific application rights not allocated by the role-based access control (RBAC) model. Processes such as the re-certification of rights, roles

and accounts also contribute to governance, thereby reinforcing the zero trust approach by regularly questioning and verifying the rights acquired by users.

All IAM components generate audit information that can be processed for risk analysis purposes or to identify the cause of an intrusion — such as a fraudulent assignment of a right to a user.

Going further, IAM can participate in the dynamic side of the zero trust approach by using artificial intelligence to analyze events coming from IAM, and taking decisions such as deactivating an account, disconnecting a user, or increasing the level of user authentication required in response to an anomaly. This is exactly the prescriptive approach employed by our Evidian IAM software suite.

IAM: An integral lever in an enriched zero trust policy

Making information systems accessible to the outside world

and the extensive (and necessary) use of cloud can expose organizations to different types of threats. Identities, application accounts and the associated rights are at the heart of hacker attacks, so they must be managed and fiercely protected as key elements of a zero trust approach. Complemented by strong authentication and reinforced access control for all types of internal or external users, IAM enriches the zero trust policy by applying it right down to the application level.

“With a thriving tech sector, Singapore has become a hub for innovation in the APAC region. Atos introduced both Security by Design and Zero Trust approach by leveraging its wide portfolio of cybersecurity products like IAM, Encryption technologies coupled with our AI/ML Managed Detect and Respond services. This is very crucial as data is shared more widely across the world while cyber threats and attacks increase.”

Olivier Castaignede
Head of APAC, Big Data & Security

Five tips for a successful zero trust journey

Swisscom's Head of Security Architecture, Panos Zarkadakis, explains why the company chose a zero trust approach for the future of its security. To help others assessing the merits of adopting a similar approach, he outlines five tips for ensuring that the adoption of a zero trust network delivers for an organization in the long term.

Swisscom's Head of Security Architecture, Panos Zarkadakis, explains why the company chose a zero trust approach for the future of its security.

In our ecosystem, we sometimes hear that security is a journey, not a destination. Sooner or later, we realize that perfect cybersecurity can never be achieved. However, it's still important to aim for it, as the true way to enhance security is through experiences. As the head of security architecture at Swisscom, I am not only responsible for today's security architecture, but also for what it will look like in 5 to 10 years. That's why this journey towards a long-term security strategy is very important to me.

Four years ago, we came to the conclusion that tomorrow's risks could not be managed by today's technology, so we needed to build a new architecture. As the largest telecommunications company in Switzerland, Swisscom falls into the category of critical infrastructures and must take the required measures to prevent disruptions that could be caused by cyberattacks. Considering our complex technological infrastructure, security needs, customer requirements and policies, we decided that zero trust was the future.

We knew that it would be a very bumpy road with a lot of time, money and resources invested, but this is the kind of long-term project that I love because they change things fundamentally. I would like to share a few tips from what I learned during this journey.





Tip #1: You must have a highly motivated core team

The first element to consider when starting your zero trust journey is building a highly motivated team. Changing the way your organization approaches security is a long and difficult process. It is therefore essential to have the right sponsors to implement this transition. But how to identify the right people? The team needs to believe in the approach, constantly learn about zero trust and be able to convince others that it is the right path for the organization.

At Swisscom, we started the journey with five people who were convinced that zero trust was the way to go. One of the biggest challenges is to explain and mobilize everyone involved in this transition — such as product owners, project managers and executives, since everyone must be involved for a successful transition.

Educating the core team was key to having a deep understanding of what zero trust is all about and, through conferences and discussions with vendors, being able to demonstrate the benefits of such a transition to all relevant stakeholders.

Tip #2: Understand what zero trust really means

There is a lot of hype around zero trust, a buzzword that many software vendors are promoting. However, not everyone has the same definition of the concept. Educating yourself what zero trust network access (ZTNA), identity-based segmentation and service mesh will help you understand what to expect. There are many books out there worth reading. This will definitely help you once you start working with vendors to pursue your zero trust journey. While collaborating with them, it is important to understand their approach to zero trust. Not all vendors define zero trust the same way. Finding a vendor that really has implemented zero trust capabilities is the first step of the collaboration.

At Swisscom, zero trust has been part of our mindset for a very long time. We have been through several different phases and our implementation throughout the organization is still ongoing.

1. First steps towards zero trust: We started our zero trust journey on a small scale. In 2018, we started by implementing one service on a network layer, followed by zero trust network access (ZTNA) components in our workplace (BYOD, workplace for customers, managed workplace, etc.). Some applications already had zero trust access methodology embedded, which made the implementation and education easier.
2. Embracing zero trust more broadly: More than a year ago, we launched educational sessions in Swisscom to enhance and deepen the know-how of our employees focusing on both zero trust network access and service mesh. This program has helped our employees better understand our definition and views on the concept and talk about zero trust in the same manner.
3. Continuing the zero trust journey: To vendors, zero trust may be a product, but for cybersecurity professionals, it is a mindset. At Swisscom, the implementation is not yet complete and it will still take us three to five more years to reach a satisfactory level of maturity. We are working in a very large environment with complex IT and cloud infrastructure, access to public clouds, but also legacy systems in the IT and telecommunication infrastructure.

Tip #3: Incorporate zero trust into your processes from the start

Zero trust is not just security products that you can easily install in your infrastructure. To implement it successfully, you will have to redesign application access and completely rethink how you implement security policies across all your business and technology units. The most important element is to get a deep understanding of your structure, which is critical when it comes to complex environments like our networks. This way, you can determine how to better secure them and how to add zero trust by design in upcoming developments.

In every development process, we now have a “built-in security” initiative. Whenever we build something, security requirements must be considered by design. The scope is highly scrutinized and security requirements are defined by the team. For instance, we ask ourselves and our customers if there are any special regulations that we should take into account, or if the data we are handling is sensitive. Then, each product and development team has at least one security professional (a “security champion”) who is responsible to keep security top-of-mind for the project.

All developers and engineers are being trained to build secure products, which leads me to my next tip.

Tip #4: Education is key

One of the most important steps in the zero trust journey is to have a clear view on what it is and what it means for the future of your company and its security. To accomplish that, education must be the foundation. It is not just about understanding the technical and technological units, but also about redesigning enforcement points, communication between application components, application access, and changing the mindset — for example, in terms of access allowance management. The zero trust path is very long and requires many resources. Therefore, it is crucial to be educated on this topic to motivate everyone to become a part of this journey.

By educating, we learn to be aligned as a team and move together on this long journey, so that everyone is equally involved, interested and willing to share all the resources that are needed.

Tip #5: Start small and take time

In a big company like Swisscom, the process of zero trust implementation requires changing more than 1,000 application deployments, including access control policies and security architecture. All changes need to be approved by the application managers, so they must be on-board. We see this as a combination of awareness and financial challenges. Although the zero trust journey takes a lot of resources, one of the most important ones is time. Be ready for any such project to take years to be fully implemented.

This is why we started the implementation by setting up small pilot groups to run and test how zero trust works for us. We learned a lot from user feedback and were able to fine-tune our processes progressively. Besides that, these pilots also helped us create training sessions craft FAQs and develop chatbots to help answer user questions. Although they are only based on a narrow working environment, our pilots have shown that zero trust does not have a negative impact on the user experience or vulnerability management.

The result? We are saving time in most of our development processes and are able to rationalize them. Developers that previously viewed security as a burden now understand its importance in their job. With service mesh we are transitioning towards “security as code”, completely automating security enforcement. A huge leap forward compared to asking operational teams to configure dozens of firewalls with hundreds of rules for each developer request in the past. This makes the overall process much faster and more efficient as human interventions and errors are avoided.

My key takeaways

While the adoption of zero trust network access did pay off immediately, the complete overhaul of our security architecture towards a perimeter-less zero trust approach will take much longer. We are confident that adopting zero trust will have tremendous positive impact on the long run. We know that the process will still take a lot of time, but we are very satisfied with having implemented this new approach. Zero trust is becoming an important differentiator, both internally and for our customers.

Finally, remember, that the most important step in a zero trust transformation has nothing to do with technology. Rather, it's about understanding, learning and taking the right decisions for each organization's needs.

“

Digital transformation doesn't stop, and we believe – thanks to strong, stable politics and societies – that the Nordic region can trail innovations for the better of society and become a global leader. Cybersecurity has to be built in from the beginning so there is security for government, the private sector and citizens.

Harri Saikkonen
Managing Director, Atos Nordics

”

Industry focus:

Telecom, Media & Technology

The Telecom, Media and Technology (TMT) sector is at the heart of major technological advances and convergence, heralding a new era for operators and their customers.

As ubiquitous digital connectivity and services becoming like the 2nd oxygen for consumers and businesses, Telcos aspire to become platform providers to move up the value chain and drive revenue growth. Significant investment is being made across *5G, fibre, edge, hybrid multi-cloud, data-driven operations and customer engagement platforms*.

Media companies are transforming to become Digital Media Enterprises to remain relevant to consumers and optimise cost. The key investment priorities for the sector being *digital transformation, IP broadcast, cloud migration, content digitisation & monetisation, automation and audience experience and engagement*.

Cloud adoption continues to grow with new use cases and serverless computing in the high-tech sector. Technologies such as AI, High Performance Computing, Industry 4.0, IoT, 5G private networks, edge and cloud-native applications are playing a crucial role in this journey.

Alongside this, strong competition to attract and retain talent is driving investment in modern digital workplace solutions enabling proactive employee experience and engagement.

The rollout of new digital capabilities is helping revolutionize the experiences and services that the companies can offer their people and customers. But with new opportunities come new regulations around data control and privacy. Cybersecurity must be built in by

48% IT and telecom
had the largest revenue
share of the zero trust
market in 2020*

design to ensure regulatory compliance and to foster trust in customers.

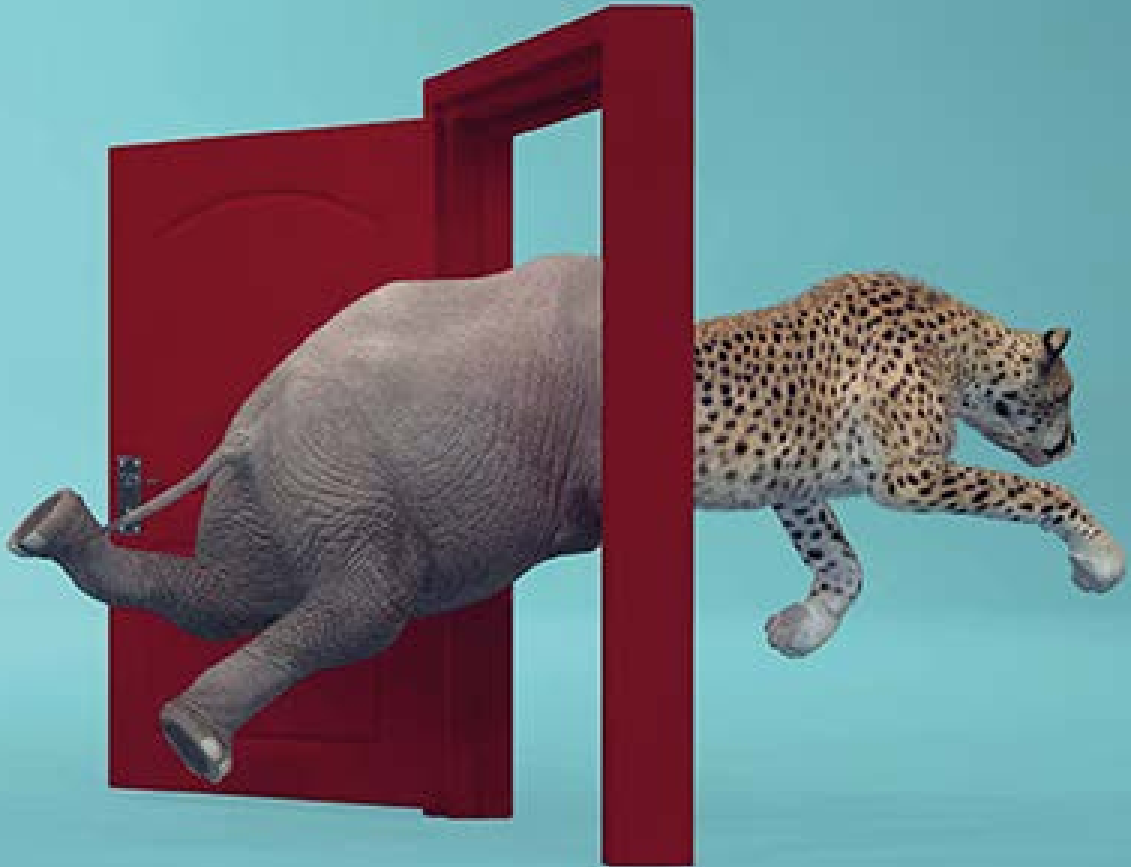
Securing systems and networks requires visibility on the performance of security services end to end, from user device to the cloud. By automating infrastructure configuration there can be instant patching in the event of a breach.

As the organisations aspire to become very agile and achieve faster time-to-market, high feature release velocity (100-1000 features/releases per day) becomes a critical factor. The security policies of the organisations can become a barrier to achieve this degree of agility. But, security can become an enabler, not a barrier for agility by implementing security-policies-as-code across the DeSecOps pipeline.

Advances in technology can significantly improve an organization's response to risks and attacks. As the TMT industry comes to grips with new technologies, so must their response to cyber-attacks, whether these originate from criminals or from state actors.

New digital landscapes and the speed of digital transformation are changing the way we do business. As the surface attack area is expanding, so the threats are evolving. As world#1 in managed security services, Atos brings a unique combination of experience, capabilities and solutions to help the TMT sector predictively detect and respond to advanced and emerging security threats.

* Grand View Research (2021) <https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report>



Cloud security

Cloud provides benefits to consumers and businesses. But organizations must understand and respond to the vulnerabilities of cloud services.





Securing the journey to the cloud

Cloud computing brings immense benefits but cybersecurity can sometimes be an afterthought. In this article, Wolfgang Baumgartner examines how organizations can implement cloud security, and where responsibility ultimately lies for securing the cloud.

Cloud computing brings immense benefits but cybersecurity can sometimes be an afterthought. How do we secure the cloud and who is responsible?

Cloud computing offers a wide range of benefits for organizations of all sizes. It can deliver significant cost and efficiency gains, help them remain flexible, offer near endless scalability and enable companies to quickly adopt innovations to stay ahead of the competition. Those who adapt first will become technical innovators and position themselves as leaders in an ever-changing market.

Cloud security matters right from the start

Many organizations that migrate to the cloud treat cybersecurity (and cloud security in particular) as an afterthought — something that is only considered after the migration process is finished. This leaves the system vulnerable and causes organizations to miss an opportunity to deeply integrate security into the architecture.

Integrating security after migration has another drawback as well, as it can be particularly challenging. Incorporating the cloud into an organization's existing security program is not as straightforward as adding a few more controls and dashboards. Instead, a thorough assessment of the business requirements and solutions in use is needed to develop an appropriate security strategy.

The complexity of implementing cloud security

At Atos, when we perform a proactive cloud security assessment, we move through different environments to identify vulnerabilities and elevate our privileges. A common observation from these assessments is that many of our clients are unsure of their own set-ups. In order to successfully move to the cloud, they need to understand how the process works.

There are some stumbling blocks on the road — like the question of who will be responsible for the migration. Whoever is nominated as the responsible person is not necessarily trained for this action. Quick training from the provider will often solve the problem, but they build what they know (namely networks) and include only network security. Unfortunately, that covers just one part of the necessary measures.

The duality of the data layer (old school with packets, services running on virtual machines and data being transferred and stored) and the control layer (which orchestrates resources, permissions and security) must also be considered — a very complex situation.

Responsibilities and permissions

One key aspect to consider is that security in the cloud is always a shared responsibility between the public cloud provider and the user. Organizations often believe that the cloud is secure since *"the big providers know what they are doing."* However, they may overlook that the provider is only responsible for physical protection in a data center and the virtual separation of the data for different customers. The user is ultimately responsible for everything that is stored within the cloud. Companies should not underestimate their own role in the security approach, because it is sometimes unclear where the responsibility stops — and it's possible to build highly insecure applications on highly secure offerings.

Another important topic is permission management. It is common to use the deny approach, where existing permissions and options are restricted. Very often, the system's cloud set-up is comparable to what our teams see in onsite security: everything is running as root and everyone has access to everything. The better approach is to decide beforehand who should be allowed to use a specific service.

A glimpse into the future

Organizations need a private, secure solution which is easy to deploy and manage without restricting functionality. Cloud security offers significant advantages such as more flexibility to react to ever-changing threats and a reduction of administrative efforts through intelligent tools. An adequate cloud security strategy also ensures not only the security of the organization's core asset (its data), but also safeguards data in compliance with all legal requirements. It protects companies from the reputational, financial and legal consequences arising from security or data breaches.

Our experience shows that clients greatly appreciate a well designed and implemented security strategy — once they recognize its value. Securing systems with a state-of-the-art security will deliver organizations a major competitive advantage.



“

As a digital partner to a wide range of public and private organizations, Atos Belux is delivering secure, decarbonized digital transformation solutions that help organizations monitor, manage and respond to cyber threats.

Punit Sehgal
CEO, Atos Belux

”

Deciphering the sovereign cloud

What is the sovereign cloud and how can it contribute to cybersecurity? In this article Pierre Brun-Murol and Vincent Dupuis provide an explanation of the concept, how it can be implemented and the challenges ahead.

What is the sovereign cloud and how can it contribute to cybersecurity?

We have defined digital sovereignty as the degree of control an organization has over its entire digital environment.

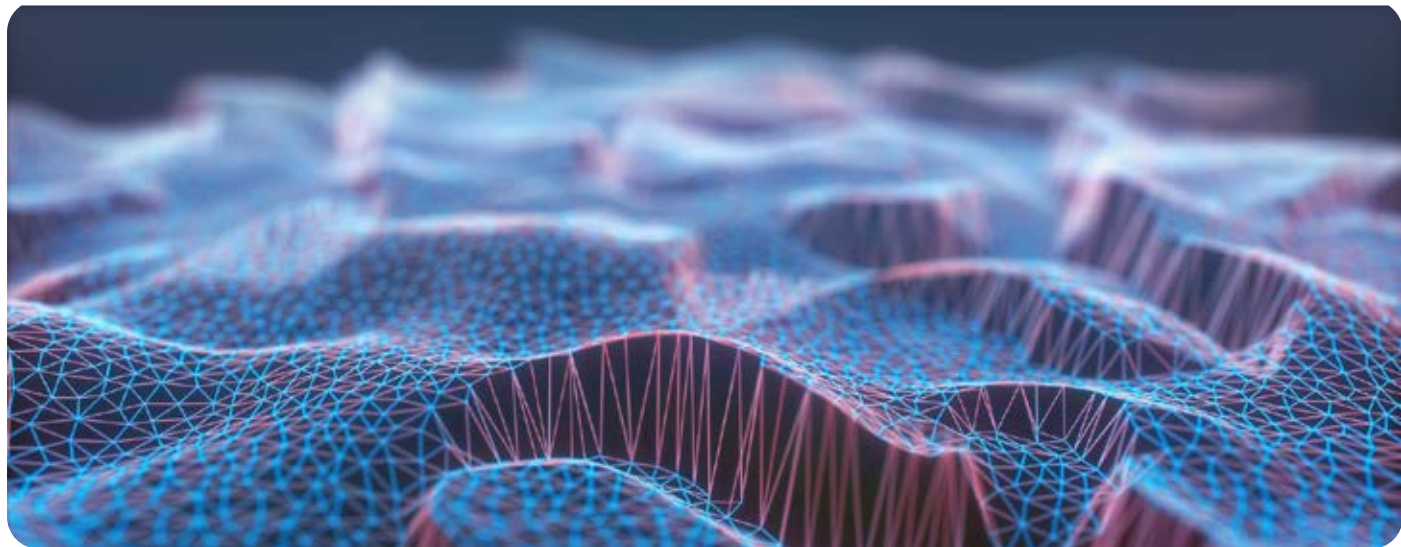
When applied to a cloud environment, sovereignty differs from security by considering the sovereign risks induced directly or indirectly by cloud providers. The primary indirect risk is foreign interference using an extra-territorial law or government pressure on the cloud provider. Hence, a sovereign cloud is a local concept with a different answer from one country to another.

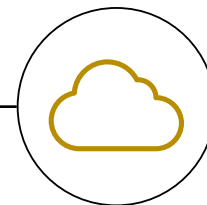
We could define sovereign cloud with a risk-based approach, saying it's a cloud environment that covers at least part of the sovereign risks. However, in some countries (especially in

Europe), it is mainly defined by a certification issued by a national agency such as SecNumCloud in France, C5 in Germany and ENS in Spain.

We would also like to emphasize that sovereign cloud is too often reduced to data confidentiality, but availability is just as important. What if your most business sensitive service goes down with no way for you to restart it or recover your data?

Now that we have defined the key features of a sovereign cloud, let's take a look at what it requires for cloud providers and customers.





A cloud provider's journey to sovereign cloud

Outside of the USA, there are two cloud service provider profiles that emerge from DC operators.

Current situation	Future path
<p>These providers host and operate their services in-house, using a mix of off-the-shelf products and their own technologies to build a solution that they host and operate by themselves.</p> <p>With their local footprint and clear role, even when depending on foreign technologies, they are the first to achieve sovereign qualifications such as a certification by the French SecNumCloud, on a limited subset of services (mostly IaaS) covering a small to mid-size capacity.</p>	<p>While their current concern is to expand their services portfolio, this may create staffing challenges for building services and running activities. Should they create technologies from scratch or buy them from another tried and tested manufacturer?</p> <p>Additionally, they want to be able to operate at scale, inducing more automation needs and triggering some local footprint questions when settling in new geographic areas.</p>
Hyperscalers current situation	Hyperscalers future path
<ul style="list-style-type: none">• These providers have the largest portfolio of services to offer, armed with an understanding of customer requirements, faster innovation and time-to-market.• They ensure a very high level of confidentiality versus third party disclosure.• However, their global hosting and operations make them appear not to be sovereign — except from their home country.	<ul style="list-style-type: none">• With high levels of industrialization and a least privilege approach deployed across their systems, hyperscalers score high on customer data confidentiality. They will continuously release new services to give customers more control for critical security elements.• They invest a lot to demonstrate that confidentiality of customer data is preserved against the hyperscaler tools and personnel as well, and particularly on promising Privacy Enhancing Technologies".• However, for availability governed by the strictest certification schemes, their main challenge is to guarantee the localization of the whole stack hosting and operations. Even for locally hosted data centers sold in the region, they must clarify boundaries and dependencies between services to co-locate them. Most hyperscalers either rely on creating local entities for operations, or partner with local players.

Moreover, service providers that do not operate data centers (like SaaS) face sovereign challenges as well. Consuming services from certified sovereign cloud providers is not enough for them, they must implement additional security controls for their SaaS operations, and may optionally apply for a sovereign qualification as well.

A customer's journey to sovereign cloud

Even if sovereign cloud is a hot topic in Europe, not every customer may need it. Customers need to first assess their requirements with a formal risk analysis. This risk analysis must consider the different sensitivity levels existing in their information system, which may not require the same level of sovereignty. Once this assessment is complete, a sovereign cloud may be their answer to the sovereign needs identified.

These needs can be broadly categorized as follows:

- **Compliance with regulations and laws**

Some standard public cloud offerings, especially from foreign cloud providers, may be incompatible with regional laws and regulations. In that case, the easiest way may be to use a certified sovereign cloud whose certification scheme ensures compliance with specific requirements. Alternatively, a risk-based approach must be taken.

In the future, especially in Europe, we foresee laws that will require certified sovereign cloud for some activities such as for Critical National Infrastructure.

- **Protection of business strategic data**

Most customers have highly critical data like industrial secrets, innovations or even customer databases that need a high level of sovereignty. To maintain control over this data while leveraging cloud, they need to select a sovereign cloud with a risk-based approach.

Once the required level of sovereignty is established, an important criterion for choosing the target sovereign cloud solution is the customer's expectations about the cloud features they need. As described above, cloud providers' sovereign services catalogs are not equivalent, and won't match the same functional needs, depending on the customer's cloud maturity level.

There are at least two different types of customers here:

- **Cloud customers focused on IaaS**

For these customers, the focus is to migrate to the cloud for the agility, capacity and/or cost reduction it brings, but without transforming their applications. For them, all sovereign cloud service providers will fit their functional needs if they offer IaaS services.

“

Most customers have highly critical data like industrial secrets, innovations or even customer databases that need a high level of sovereignty. To maintain control over this data while leveraging cloud, they need to select a sovereign cloud with a risk-based approach.

”

- **Cloud native users**

These customers want to benefit from cloud SaaS and PaaS services even in their sovereign cloud, because they are already using them for less sensitive perimeters. For them, it is currently very difficult to find a good compromise. Most SaaS providers fall into this category.

Sovereign cloud: navigating the challenges ahead

In conclusion, the sovereign cloud market is still being shaped by three key dimensions that influence each other:

- Emerging certification schemes and regulations
- A constantly evolving landscape of sovereign services by cloud providers that lacks variety
- Customers' uncertainty about business and compliance requirements and timelines, and hesitation to zero in on the need for sovereign cloud.

Finalizing a business strategy that incorporates a sovereign cloud demands time and an organization-wide commitment. While this article has outlined the different types of players in the sovereign cloud environment, both service providers and customers need to map their internal business goals and chart their own journey towards sovereign cloud.

Learn more about
Atos's cloud offerings



How AI can simplify cloud security management

Organizations are increasingly migrating their infrastructure to the cloud. This risks new security vulnerabilities — but how can AI help? Harshvardhan Parmar explores in this article how migration to cloud services can create security gaps and how AI can assist organizations detect and respond to attacks quickly.

How can AI simplify cloud security management so organizations detect and respond to attacks quickly?

Organizations are increasingly migrating their infrastructure to the cloud, with COVID-19 accelerating cloud adoption across various industries. Gartner predicts that by 2025, enterprises will spend more on cloud computing than on traditional IT.

Migrating to a cloud ecosystem has many benefits for organizations. However, this migration also increases security risks that cannot be addressed by traditional security mechanisms.

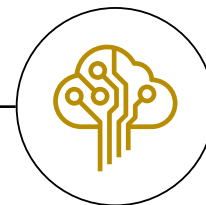
Let's take a look at why security risks are increasing and how AI can help us overcome them.

1. Hasty migration leads to unintentional security gaps during deployment

Cloud adoption has accelerated across almost every industry since the pandemic. One of the key requirements that arose was the need to quickly support remote working options. Moving to cloud seemed like the natural choice for a requirement like this. However, the rush to get things operational resulted in weak configurations and insufficient security controls.

Traditional IT infrastructure has tested and proven security configurations. Cloud controls on the other hand are evolving as the technology evolves, and there is limited guidance on robust security controls.

AI can be leveraged to perform dynamic checks across the various moving parts to identify misconfigurations. It can also be used for vulnerability management and access management..



2. Cloud technologies increase the attack surface for threat actors

Although moving to the cloud gives organizations more flexibility as compared to traditional data centers, very few organizations use it for their entire infrastructure. Many organizations use a hybrid approach, distributing their workloads between cloud and on-premises or a multi-cloud approach that distributes workloads between multiple cloud service providers.

The vast majority of organizations use at least two cloud service providers. This means that multiple technologies work together to create a unified ecosystem. However, this very aspect also increases the attack surface available to threat actors. Additionally, extensive use of application programming interfaces (APIs) — a critical component of cloud services — contributes to the increased attack surface.

This larger attack surface directly increases the workload for cybersecurity professionals¹, despite the global shortage of skilled cybersecurity professionals. AI is capable of processing large volumes of data in a short period of time and can therefore be leveraged to augment the analysis performed by cybersecurity professionals. The result is not only comprehensive coverage for an increased attack surface, but also an overall increase in the efficiency of security processes.

3. Cloud technologies are evolving rapidly, resulting in unknown security threats

Cloud computing has introduced new technologies, such as serverless, containers and microservices, which are not seen in traditional IT technologies. These technologies provide an advantage in terms of scalability, flexibility and cost. Like any new technology, however, they can also inadvertently introduce new vulnerabilities and/or weaknesses. Due to a lack of knowledge about these technologies and their vulnerabilities, it is difficult to protect against these threats through traditional security mechanisms.

AI is already being used to varying degrees for anomaly detection. However, it can truly display its potential in a cloud scenario. While supervised learning can be used to detect known threats, unsupervised learning can enable the detection of unknown threats, including potential zero-day attacks. It can also be used to learn the normal behavior of users and systems in order to create a baseline, which can be used to detect any deviations.

AI not only helps you detect threats faster and more efficiently, but can also help you respond to threats more quickly. AI can be used to determine potential remedial actions and present them to a human analyst. The actions performed by the human analyst can then be used as a training dataset to enable a machine to mimic human decision making and perform remedial actions when threats are identified.

1. <https://fortune.com/education/business/articles/2022/06/30/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/>

Lexicon

Application programming interface (API): A set of routines, protocols, and tools for building software applications. Put simply, an API specifies how software components should interact.¹

Behavioral analytics: Tools that identify aberrant behaviour by an individual or a computer that may suggest there is a risk that needs to be addressed (e.g. that a user has become an insider threat or a computer may have been compromised).

Cloud computing: Utilization of remote servers in the data-center of a cloud provider to store, manage, and process data instead of using local computer systems.

Data fusion: The process of integrating multiple data sources to produce more consistent, accurate, and useful information than that provided by any individual data source.²

Denial of service attack: An attack that stops authorised access to systems or data, or delays technology operations. If more than one source is used to mount the attack, it becomes a distributed denial of service (DDoS) attack.

Digital sovereignty: The concept that an individual or organisations should have sovereignty over their own digital data.³

Domain name service (DNS): The way that internet domain names are located and translated into internet protocol addresses. A domain name is a meaningful and easy-to-remember 'handle' for an internet address.

Edge & swarm computing: Edge computing describes compute resources beyond the boundaries of data centers. Swarms are formed when these edge devices are able to interact and co-operate as self-organizing intelligent groups.

Endpoint: An endpoint is a remote computing device that communicates back and forth with a network to which it is connected.⁴

Firewall: A security system that prevents unauthorized access to systems or data on a private network. Fourth industrial revolution: the current and developing environment in which disruptive technologies and trends such as the Internet of Things, robotics, virtual reality and artificial intelligence are changing the way we live and work.

General Data Protection Regulation (GDPR): An EU regulation that places obligations on organizations in relation to the protection of personal data and requirements to report data breaches.

Identity and access management (IAM): A framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources.⁵

Incident management: The process that manages the lifecycle of all incidents (unplanned interruptions or reductions in quality of IT services). The primary objective of this Information Technology Infrastructure Library (ITIL) process is to return access to the IT service to users as quickly as possible.⁶

Inter-cloud: A single common functionality combining many different individual clouds into one seamless mass in terms of on-demand operations.⁷

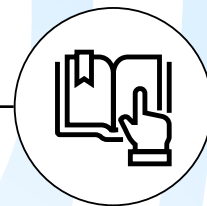
Infrastructure as code (IAC): Infrastructure as code (IaC) uses a high-level descriptive coding language to automate the provisioning of IT infrastructure. This automation eliminates the need for developers to manually provision and manage servers, operating systems, database connections, storage, and other infrastructure elements every time they want to develop, test, or deploy a software application.⁸

Malware: A generic term for malicious software that is developed with a hostile intent, for example to damage or gain unauthorized access to a device or network (e.g. worms, viruses, Trojan horses).

Multi-factor authentication (MFA): When a conventional password is used for authentication, there will always be a chance that users and administrators will choose machine-guessable passwords and be susceptible to seeing their security compromised. MFA introduces a second factor, either through phone, a card reader or passcode, to authenticate a user.⁹

National Cybersecurity Centre (NCSC): The UK's independent authority on cybersecurity.

Patch: A discrete update released by a software vendor to fix vulnerabilities and bugs in existing programs.



Phishing: A cyber crime in which individuals or companies are contacted by email, text or phone by someone posing as a trustworthy source in order to trick the recipient to disclose personal or financial details. This can also be an automated process. It is called spear phishing if specifically targeted or whale phishing if targeted at senior people.¹⁰

Playbook: A self-contained set of processes on how to deal with the most common incident types; they include procedures, advice, further enrichment tools and rapid access to the relevant toolsets for remediation.

Privilege access management (PAM): A class of solutions that help secure, control, manage and monitor users' privileged access to critical assets.¹⁰

Quantum encryption: An encryption technology that allows cryptographic (encryption) keys to be exchanged between two parties with guaranteed privacy — typically using photons transmitted through fibre-optic cable. Data transferred in this manner can't be intercepted or manipulated without leaving clear evidence.

Ransomware: A type of malware that is a form of extortion. It works by encrypting a victim's hard drive, denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again.

Security incident event management (SIEM): A tool that collates and analyses log data coming from a variety of sources to help manage security threats.

Security operations centre (SOC): A facility where analysts work with security tools and threat intelligence to monitor what is happening in the network and take remedial action if issues arise.

Software as a service (SaaS): Software as a service (SaaS) is a software distribution model in which a cloud provider hosts applications and makes them available to end users over the cloud.¹¹

Sovereign cloud: A sovereign cloud is a cloud computing architecture that's designed and built to provide data access in compliance with local laws and regulations. A sovereign cloud service provider will ensure that each subscriber's data — including their metadata — is protected from foreign access and stored in compliance with the originating country's privacy mandates.¹²

Terabyte (TB): A unit of information where a single terabyte is equal to one thousand gigabytes.

User and entity behavior analytics (UEBA): A type of cybersecurity process that takes note of the normal conduct of users. In turn, they detect any anomalous behavior or instances when there are deviations from these "normal" patterns.¹³

Virus: A type of hidden malware that self-replicates (by copying its own source code) and infects other computer programs by modifying them. A virus cannot run by itself; it requires a host in order to spread. Once infected, computer programs and machines are compromised.

'Zero-day' attack: A 'zero-day' (or zero-hour or 0-day) attack or threat is a computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability.

Zero trust approach: A zero trust approach is a cybersecurity paradigm focused on resource protection (e.g. services and data) and the premise that trust is never granted implicitly but must be continually evaluated.¹⁴

Footnotes:

In association with SANS (unless otherwise stated as footnotes): <https://uksans.org/security-resources/glossary-of-terms>

1. <https://www.webopedia.com/TERM/A/API.html>

2. https://en.wikipedia.org/wiki/Data_fusion

3. <https://www.techopedia.com/definition/33887/digital-sovereignty>

4. <https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint>

5. <https://www.webopedia.com/TERM/I/iam-identity-and-access-management.html>

6. https://wiki.enit-processmaps.com/index.php/Incident_Management

7. <https://www.techopedia.com/definition/7756/intercloud>

8. <https://www.ibm.com/cloud/learn/infrastructure-as-code>

9. <https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services>

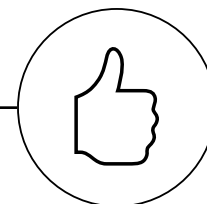
10. <https://doubleoctopus.com/security-wiki/authentication/privileged-access-management/>

11. <https://www.techtarget.com/searchcloudcomputing/definition/Software-as-a-Service>

12. <https://www.techopedia.com/definition/34628/sovereign-cloud>

13. <https://techterms.com/definition/terabyte>

14. <https://www.ncsc.gov.uk/collection/zero-trust-architecture>



Acknowledgements

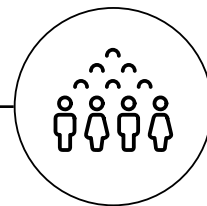
We would like to thank the following contributors.

If you wish to send feedback, please use the hashtag **#DVfCS** or email us at **digitalsociety@atos.net**.

In order of appearance

Name	Title
Kulveer Ranger	SVP, Head of Strategy, Marketing, Communications & Public Affairs, Atos Northern Europe & APAC
Vasco Gomes	Global CTO for Cybersecurity Products, Atos
Dan Schaupner	Head of Digital Security Consulting, Atos North America
Sarah Armstrong-Smith	Microsoft Chief Security Advisor
Katarzyna Gołusńska	Global Workforce Manager for Cybersecurity Services, Atos
Zeina Zakhour	Global CTO Digital Security, Atos
Mariana Peycheva	Global Cybersecurity Business Development Manager, Atos
Olivier Ligneul	Chief Information Security Officer, EDF Group
Barbara Couée	Portfolio Manager, Atos Digital Security
Farah Rigal	Deputy Head of Global Cyber Security Services, Atos
Aaron Chu	Advisory Practice Director, Enterprise Architecture and Identity, Atos Northern Europe
Yann Morvan	International Presales Manager, Atos
Panos Zarkadakis	Head of Security Architecture, Swisscom
Wolfgang Baumgartner	Head of Digital Security Consulting, Atos
Pierre Brun-Murol	Cybersecurity Global Business Development, Atos Senior Expert
Vincent Dupuis	Cloud Solutions Architect, Atos
Harshvardhan Parmar	Global Head of Data Science, Managed Detection and Response, Atos

Production team



Editor: Kulveer Ranger, Martin Pietersen

Production team: Nush Balapaskaran, Mark Barnett, Laurence Bégou, Anna Cantin, Sebastian Hanley, Felipe Copetti Hickmann, Victoria Pearson, Elizabeth Sauma, Benedict Surtees, Ed Thomas and Anastazija Zivkovic

Design: Jennifer McGhee

About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The [purpose of Atos](#) is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us

atos.net

atos.net/dvfcs-3

Let's start a discussion together



For more information: digitalsociety@atos.net

Atos is a registered trademark of Atos SE. October 2022.
© Copyright 2022, Atos SE. Confidential Information owned by Atos group, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval of Atos.