Digital Vision for Cybersecurity

Global opinion paper - March 2019

Trusted partner for your **Digital Journey**

Atos

Atos Digital Vision series aims to provide a thoughtful and informed view of the opportunities brought about by digital services. It demonstrates how these opportunities are being harnessed by governments, markets and businesses to help deliver innovative solutions that benefit their customers and citizens, today and into the future.

This opinion paper features contributions from Atos global experts and from leading thinkers from other major industry organizations and leadership bodies.

Contents

Foreword

Thierry Breton
Atos Chairman & CEO

Cybersecurity must manage the ever-increasing external threat landscape but, in the age of digital transformation, it must evolve to protect the developments within the internal business also.
It must be able to move, flex and change with your business and keep up with emerging technologies as well as ever-shifting regulations.

We believe that cybersecurity is a journey of constant adaptation and automation, which requires a mix of products, services and consulting. Being prepared for the unexpected both outside and within your organization.

Over the next few years, as the prevalence of data shifts business models, we predict that cybersecurity will be a key function of your organization in ensuring trust is maintained with your customers. This will be a vital ingredient for success.

Pierre Barnabé
Executive vice-president,
Head of Big Data & Security, Atos

A more automated cybersecurity approach is essential to address the sheer scale, complexity and volatility of risks in the digital age.

As Robert S. Mueller, ex-Director of the FBI once said, we cannot undo the impact of technology – nor would we want to. We must use our connectivity to stop those who seek to do us harm.

At Atos, we believe that data, combined with human intelligence and insight, is key to fighting today's threats. We harness automation and machine learning to understand – and predict – the threat landscape. We're also getting ready for the next digital shockwaves – not least the arrival of quantum computing. Yet with the attack surface expanding, cybersecurity is no longer just for the IT department. It's an executive leadership issue involving every individual in an organization.

Cybersecurity: the business challenge

Over 18 million
new malware samples are captured every 3 months, expected to rise from 1 per week in 2015 to 1 per day by 2021

60%
of enterprises will be victims of major breaches by 2020

1.8 million
By 2020, over 1.8 million cybersecurity jobs will not be filled due to a shortage of skills

10%
By 2020, organizations that have adopted best practices for protecting their customers' privacy will gain 10% more in revenue over competitors that are caught lagging according to a recent Gartner report

Businesses' approach to cybersecurity must adapt.
But businesses are still unprepared:

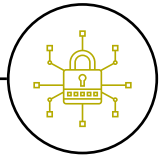
61%
hold personal data on
their customers electronically

Only 20%
have sent staff on cybersecurity trainings
over the last 12 months

Only 10%
have a cybersecurity management in place

However 85%
of targeted cyberattacks are preventable through
appropriate risk-mitigation measures

Pierre Barnabé, Executive vice-president, Head of Big Data & Security, Atos



The cybersecurity challenge: leaving the fortress

In the space of just a handful of years cybersecurity has become a key item on every boardroom agenda and sits as one of the top business risks. You would be hard-pressed to find anyone who wasn't acutely aware of the need for security. The conversation is certainly open but are we always identifying the correct challenges?

Most security risks are focused around your most valuable asset. For cybercrime, this is data – the new source of value and potential value for an organization. Data needs to be viewed as a treasured commodity and asset and for this reason, also as a target for cybercrime that must be well protected.

Part of this is about re-evaluating the governance structure, culture and behavior around data. Organizations need to be clear where their data is, what it is, who has access to it and how it's being secured.

Leaving the fortress

The other aspect to this is being brave enough to change the way you protect your organization.

Your most valuable assets are no longer concentrated in one place. Data will be dispersed throughout your business across different units. This now means leaving the fortress you built to protect yourself – as terrifying and counter intuitive as this sounds!

The fortress can no longer protect an organization. No matter how good it is, the walls will be scaled probably in an area of your business you had not even considered a risk.

The right technology

The best defense is a combination of the right technology and the right people. This means both defense grade technologies and highly specialized cybersecurity experts and services. You need technology that is quicker and smarter than the criminals have access to. It needs to utilize automation, robotics and AI. You also need the people who know how to proactively hunt for threats and keep ahead of new criminal behavior. Alongside this it also must be decentralized.

Decentralized security

Sometimes it's not about the size of your army but about their armory and position. Federated and decentralized security is key. You need to be where the data is and cover all the possible pain points. With the advent of IoT and autonomous devices this will only become more vital.

Sub premises will now need to be controlled as well as powered with local cybersecurity intelligence. Each of these will need to utilize the best in products and services – from encryption to automation to AI. With technology able to analyze vast amounts of data and flag attacks or potential attacks well before a human would be capable, allowing for decision-making on response by individuals but also automatic protection.

In the future

The rise of IoT and autonomous objects will make this decentralizing of security even more acute. Each object will need to be able to protect itself from threat. To do this you must be as close as possible to where data is generated.

Find the right partner for this journey. One who has the technology and product base to encrypt and manage access, can bring AI, automation and robotics and can bring edge technology and security. Having the cybersecurity conversation is not enough, what's vital is understanding the ever-shifting challenges and being able to stay a step ahead at all times.

> In the digital economy, the grim reality that every business must accept, is that it's no longer a matter of 'if' but 'when' a security breach will occur...
>
> **Zeina Zakhour, Global CTO for cybersecurity, distinguished expert and member of the Scientific Community, Atos**

Zeina Zakhour, Global CTO for cybersecurity, distinguished expert, member of the Scientific Community, Atos

Searching for the lost trust

2018 was indeed the year where personal data protection moved at the top of the board's agenda for most organizations. Driven by the adoption of new regional data protection laws starting with GDPR to China's cybersecurity law, "India's data protection bill, California's "Consumer Privacy Law and more... and replete with increasingly high profile data breaches.

Since the GDPR came into force in May 2018, the EU National Data Protection Authorities (DPAs) have examined thousands of complaints and recorded an increasing number of data breach notifications. DPAs in countries like Austria, Portugal, Germany,UK and France have even issued hefty fines for companies violating the GDPR regulation.

The French DPA (CNIL) issued a 50 million euro fine against Google for their failure to inform people of how they are processing data and a lack of valid consent regarding the personalization of their ads.

A shift in public perception

Following the public outcry after the Facebook/Cambridge Analytica debacle in March 2018, consumers are more concerned about their digital footprint and how their personal data are harvested and used by corporations.

Even if Facebook did not lose millions of users (FOMO – Fear of Missing Out - is still going strong!), 54% of surveyed US, UK, German and French citizens stated that they are more wary of sharing personal data online andan 78% are more likely to turn their back on a brand if it had recently been breached.

The changing approach to privacy

Despite this strengthened regulatory framework and citizens' heightened sensitivity to privacy issues, many organizations are still lagging in terms of data protection and data privacy governance.

50% of organizations still believe that they are far from being compliant with GDPR and many believe that they will never be fully compliant with the regulation.

GDPR is considered as a challenge by organizations because it is an afterthought. In their race for digitization, most organizations did not bother with data protection and privacy considerations. Therefore, organizations have now to review how their digital environment has been built and how it has evolved. They need to understand where personal data is stored, duplicated and used to put in place the necessary foundation for proper data governance and data management as per the various regulations.

Even if these key steps seem tedious, by assessing their current security measures and overall data protection and privacy maturity, organizations can identify the path to Privacy and Trust.

When organizations measure the risk of personal data misuse, they can identify the proper privacy risk mitigation approach. Such an approach will rely on technologies, processes and governance to:

- Embed privacy by design in the digital transformation process
- Enhance data discovery and classification
- Enable control over personal data usage
- Create transparency by adopting global privacy, ethics and accountability policies and practice
- Implement privacy controls to protect data (data encryption solutions)
- Implement the necessary controls to demonstrate compliance through Security Operation Center monitoring and reporting

You can check our approach to GDPR compliance spanning from GDPR readiness, to customer rights management, to data breach notification and privacy by design.

We have always encouraged organizations to adopt data privacy regulations as enabler of Trust. In the blog articles posted on our platform, we have highlighted that consumers are warier of none transparent data handling policies and are savvier in terms of protecting their digital footprint.

We have long believed that ethical and transparent personal data management will be a business differentiator in this pivotal next phase of the digital revolution. And we have the figures to prove it!

In Gartner's report on privacy vendors, they noted that by 2020 organizations that have adopted best practices for protecting their customers' privacy will gain 10% more in revenue over competitors that are caught lagging.

So, what are you waiting for?

Cyberattacks and data breaches

The threat landscape is evolving and getting more complex, while the attack surface is growing with the appearance of new technologies. 2017 was the year of ransomware, 2018 the year of cryptojacking and 2019 will be the year of file-less cross platform attacks. Companies need to adapt their strategies and change their mindset.

Marriott data breach
November 2018: Marriott suffered a massive data breach with information about 500 million people who stayed in its Starwood hotels being compromised.

Shamoon, the most destructive cyberattack
The Shamoon virus attack crippled between 300 and 400 servers and up to 100 personal computers out of a total of about 4,000 machines from Italian oil services firm Saipem. The cyberattack hit servers based in the Middle East, India, Aberdeen. The virus was used in some of the most damaging cyberattacks in history, starting in 2012 when it crippled tens of thousands of computers at Saudi Aramco and RasGas Co Ltd in the Middle East. It went dormant until it resurfaced in late 2016 in a series of Middle East attacks that continued through early 2017 and back again end of 2018.

Collection #1 is the world's biggest data dump. Check your passwords
Reported in January 2019, a massive database containing usernames and passwords belonging to millions of people has been circulating online. Across 700 million email accounts, there were 21m unique passwords being used.
While Collection #1 isn't the result of a single data breach it's the biggest known file of personal information that has surfaced. The largest data breach ever to have happened was Yahoo!'s 2013 hack. All of its three billion user accounts were hit in some form but information from the attack has never appeared online.

Lessons learnt

1

An attack can come **anywhere anytime**, and can spread wherever it can – not just to specific targets.

2

Always keep endpoints **patched** (even after WannaCry attack, some businesses still failed to patch systems).

3

Always run supported **operating systems** and **applications** (many businesses still use unsupported versions of Windows XP and Server 2003 to run the business-critical operations).

4

Establish and test **Security Incident Response** procedures to react to an attack.

5

Ensure employees are properly **informed and trained** to spot suspicious activity.

6

Use **Threat Intelligence and Behavioral Analysis**: using Antivirus software alone is not enough.

7

Implement and test a **backup strategy** to support businesses-critical assets and operational data after a ransomware attack.

8

Establish appropriate **business continuity and disaster recovery** plans and rehearse them regularly to make sure they are fit for purpose.

Farah Rigal, Global Security Operations Center (SOC) transformation program director, Atos

Leveraging data the right way to build security for your organization

Creating value from data is considered the biggest area of opportunity for organizations today. But often, data is kept in different silos of an organization, potentially resulting in missed opportunities. Consider, however, what impact these silos can have when the data is relevant for the organizations security. These silos of data can mean low or no visibility of the full potential attack surface (IT, ICT, IoT).

Data silos and security

You can only protect the areas you see need protecting. These silos or data pockets mean blindness and potential entry points for hackers to build fragmented and low signal attack scenarios, which remain under the radar of most traditional controls. They can also make an organization's reaction to a security breach slow and ineffective.

A lot of recent well-known attacks have illustrated how these silos can be easily exploited by attackers. They demonstrate the need for effective situational cybersecurity, for data convergence and correlation with all relevant business data - in and outside the enterprise - through an increased depth of data analysis. Data analysis should find the most effective ways to achieve security without necessarily requiring all data to be held in the same place. For example, running distributed forms of analytics/artificial intelligence and merging results.

Closing the loop

The Security Operations Centers strive to detect, identify and qualify threats and remediate them before they create damage. When a security issue is found, the response team usually responds by alerting and instructing other teams to make changes in systems they cannot access. The convergence of detection-to-reaction processes in as closed a loop as possible exponentially impacts the enterprise's ability to manage threats and crises effectively. This is an example of where orchestration and automation can bridge gaps between silos without decreeing that teams, tools or environments must merge as one or consolidate their data in one place.

We have developed the concept of the Prescriptive Security Operations Center in order to effectively break data silos, increase depth of analysis and compress the time it takes to react with the combination of meaningful data analytics, artificial intelligence, orchestration and automation.

Read the White paper on Prescriptive SOC: atos.net/wp-content/uploads/2017/10/atos-psoc-op-en.pdf

Charles Piron, Head of business development, IOT security, Atos

Cybersecurity, the emerging challenge of the IoT

By allowing the physical world to be attached to the world of information, the Internet of Things opens the door to the development of countless services both inside companies and for their clients. But this global interconnection of people, processes and context - known as the Internet of Everything (IoE) - will only keep all of its promises if the underlying infrastructure offers heightened guarantees of security and reliability. That's why cybersecurity has now become a fundamental issue. This realization is often followed by an observation of lack of knowledge, which can halt a number of projects.

Security questions are indeed often badly understood, partly because they affect different employees within the company and also due to the lack of advisors with all the necessary skills who are capable of providing a universal and integrated solution. In fact, the security of the IoT depends on four things:

- Securing sensors and their operations
- The confidentiality and integrity of data in transit
- Securing stored data
- Securing access to information

While the first aspect relates to the world of physical security and critical systems, and the last two, more traditionally, to the security of information systems and big data, the problem of data in transit is truly specific to the IoT. Packaged, routed, and eventually processed and stored, the data passes through different hands until it is used. Its integrity and confidentiality must therefore be secured throughout its journey across this ecosystem, right down to the end user, who To do this, it is vital to implement a security strategy suited to the specific technology of the IoT, whether this means low-power long-range protocols (LoRa, Sigfox, etc.) suited to systems of sensors distributed on non-electrical objects, or short-range protocols (Wi-Fi, ZigBee, Bluetooth Low Power, etc.) that can be integrated into electrical devices and/or benefit from the link of a gateway.

The case of Low Power presents the strongest and most specific constraint: a high level of security must be maintained at the lowest cost, using the minimum amount of energy. As messages are limited to a few bytes, we rely on simple, standardized algorithms, that will be integrated into the chip itself. For example the Advanced Encryption Standard (AES) algorithm, which is very secure and only consumes a tiny quantity of energy. This means the question of security has to be addressed right from the design stage, and component manufacturers must be integrated into this ecosystem. This physical layer is the first one in a security system like a Russian doll, with elements added at each stage of transit.

Thus, when the signal reaches a gateway, additional security can be integrated (SSL, VPN, etc.) and when the end users retrieve the information, they only have to open the successive boxes to obtain the data. The data then enters the information system, often a Big Data system, and then from that point traditional security measures apply.

The security of the IoT and thus the IoE is based on a series of locks and the associated keys to ensure the confidentiality of the data and independence of its users.

Currently, there is no model in place to establish who will manage this and who will guarantee it. In this way, it is possible to establish a solution that is secure from end to end, that integrates all partners in the ecosystem and offers a foundation of trust in the services of the IoE has for one chosen to confide universally in should be able to rely on it in all confidence.

“How can organizations protect themselves in the cybersecurity era? Everyone within the organization needs to be on board with cybersecurity policies, staff must be educated on password etiquette and on how to be cyberaware. Security should be part of the development process. And firms must assume that the right security isn’t just something you can buy over the counter: dedicated, outsourced security professionals whose full time job it is to protect against cyberattacks are key.

With the right security measures in place, businesses can protect themselves and avoid becoming the next brand to hit the headlines for the wrong reasons”

Christophe Moret, Senior vice president cybersecurity services, Atos

Zeina Zakhour, Global CTO for cybersecurity, distinguished expert, member of the Scientific Community, Atos

Prescriptive security: using the haystack to find the needle

In our increasingly data-driven world, organizations are engaged in a race to gather operational and customer data and apply analytics to transform that data into valuable business insights. Yet one important application that is still rarely addressed is cybersecurity data analytics.

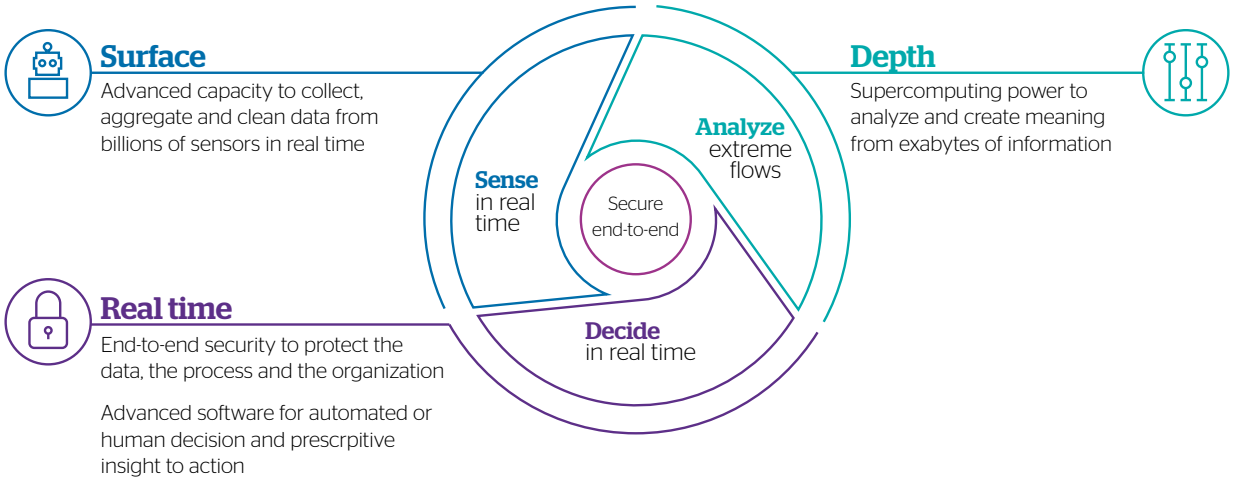
From proactive to prescriptive

We regularly hear about major cybersecurity breaches and wonder whether they were preventable. Prescriptive security is about exactly that: preventing breaches from happening by leveraging big data and supercomputing capabilities. As technologies advance, cybersecurity is shifting away from a reactive and proactive model to a prescriptive model that can analyze analytics patterns in order to identify the next threats and to automate the security control responses.

While cybersecurity has been focused on finding the needle in the haystack, prescriptive security instead uses the haystack to find the needle by leveraging big data and machine learning analytics and utilising all data generated within the organization and outside the organization, in order to bring 360° security visibility and eliminate all potential blind-spots.

With a Prescriptive Security Operations Centre (SOC), organizations will be able to:

- **Face the ever-evolving threat landscape:** the threat landscape has been increasing exponentially as the adoption of new technologies such as Internet of Things (IoT), big data and cloud computing are expanding the attack surface. Every three months, over 18 million new malware samples are captured, with zero-day exploits (malware that goes undetected by traditional anti-virus software) expected to rise from one per week in 2015 to one per day by 2021. With prescriptive security, threat intelligence is no longer a separate technology-watching process managed through alert bulletins, but an integrated part of the SOC where threat intelligence feeds give actionable risk scorings and can detect unknown threats before they even reach the organization.



- **Significantly improve detection and response times:** time is on the side of any adversary who is patient, persistent and creative. We're fighting human ingenuity and attackers aren't playing by the same rules as we are. Prescriptive SOCs can change current operational models and considerably improve detection times and response times. Instead of thinking in days and months to detect and correct threats, with machine learning and automation we can neutralize emerging threats in real time and prevent future attacks.

- **Optimize cybersecurity resources:** while cyberattacks are growing in volume, complexity and pervasiveness, organizations will need to counter these using limited resources. The latest research estimates that by 2020, over 1.8 million cybersecurity jobs will not be filled due to a shortage of skills. Prescriptive security, by introducing artificial intelligence and automatic response, will optimize the use of cybersecurity professionals who will be able to automate responses to common cyberattacks and focus on the more complex and persistent ones. It will also introduce new cybersecurity roles, such as cybersecurity data scientists to integrate statistical and mathematical models and provide innovative mechanisms to detect future cyberattacks.

Next-generation infrastructure

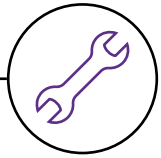
Prescriptive security advances a tri-dimensional paradigm by increasing the detection surface, increasing the velocity of response and decreasing the reaction time. By using big data, analytics and supercomputing, it also effectively optimizes the cost factor (human resources cost plus storage/compute power costs).

Prescriptive security SOCs will be the next-generation cybersecurity infrastructure that the digital economy needs to enable and engender confidence. With this in place, organizations will be able to effectively protect their business assets including valuable business data and customer personal data.

Role of a Security Operations Centre (SOC)

A SOC is a secure facility equipped to function as the central hub for cybersecurity incident prevention, detection and response capabilities. SOCs are usually manned 24 hour a day, 7 days a week, 365 days a year by SOC analysts and incident response teams. Atos has a network of 14 24x7 security operations centres worldwide providing cybersecurity services to national and global clients across all sectors.

Kevin Cooke, Head of cybersecurity delivery, Big Data & Security, Atos UK&I



The importance of threat intelligence as a positive tool

With an ever-expanding threat landscape, are you aware of how your organization could be targeted today?

In the digital economy, the grim reality that every business must accept is that it's no longer a matter of 'if' but 'when' a security breach will occur. Traditional security solutions are not enough to protect against sophisticated cybercriminals who are increasingly successful at getting inside companies' networks and compromizing sensitive data. Organizations must recognize that an effective cybersecurity posture involves not only detection and recovery from compromize, but also a proactive approach to prevention.

Evolution of IoT security

With approximately seven billion devices connected to the internet worldwide today and 20 billion estimated to be connected by 2020, the risk to privacy, information leakage and size of an organization's attack surface is increasing. This does not account for the introduction of General Data Protection Regulation (GDPR) in May 2018, with stricter controls around the governance and protection of sensitive data. However, security concerns relating to the Internet of Things (IoT) span much further than purely unauthorized access to data. IoT devices are still in their infancy when it comes to security, which makes them easier to target due to vulnerabilities such as software reconfiguration and default passwords.

Next generation of cyberattacks elevates business risk to a new level

The growth of IoT has led to a notable increase in cybercriminal activity and capability. Malicious actors have capitalized on the ability to quickly establish large-scale botnets. These are wide scale, coordinated attacks that use the IoT to spread through company networks and can result in major disruption called 'distributed denial of service' (DDoS). Sometimes known as 'DDoS of Things' attacks, they have become commonplace, with the most notorious being Mirai and Brickerbot in recent times. Industry analysts predict[1] that ransomware will increasingly migrate to IoT and become a primary threat, potentially leading to significant impact on both commercial and critical national infrastructure.

Why organizations need proactive and strategic threat intelligence

Hacktivists, cybercriminality, state-sponsored attacks and insider threats combine to form a dangerous threat landscape for organizations today - not to mention the ease of access to 'off-the-shelf' attacks (such as malware distribution and phishing campaigns) available in the dark web marketplace. This plethora of threats emphasises the importance of maintaining awareness by effectively using threat intelligence.

Threat intelligence is not new and in relation to cybersecurity means: 'evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard'.[2]

What is new is the ability to derive actionable intelligence from the sheer volume of threat intelligence now available. The value of threat intelligence is in helping organizations to prioritize actions in proportion to the threat and an analysis of overall risk. Over the years, organizations have attempted to introduce threat intelligence into their security tooling in order to detect and protect against known malicious domains, blacklisted internet addresses and other identifiers. The problem was, this intelligence consisted of millions of indicators that needed filtering and prioritizing and were soon out of date.

[1]McAfee Labs 2017 Threat Predictions Report
[2]Gartner Analyst Rob McMillan
[3]Gartner 2015

In recent times, industry analysts[3] identified three key levels of cyberthreat intelligence:

- **Tactical:** technical intelligence such as using threat indicators to proactively hunt for and defend against adversaries
- **Operational:** intelligence focused on the motivations, intent and capabilities of adversaries
- **Strategic:** intelligence about the risks and implications associated with threats used to inform business decisions and direct cybersecurity investment.

Identifying threats means that organizations can combine different levels and types of intelligence (including human intelligence) to obtain targeted, contextual threat intelligence in relation to their brand, their people and their technology. This proactive and structured approach adds immense value by enabling greater insight into what threats the organization faces, the tactics, techniques and procedures of its adversaries, and how this can be used to minimize business disruption and reduce the window of opportunity for threat actors.

> “The value of threat intelligence is in helping organizations to prioritize actions in proportion to the threat and an analysis of overall risk.”

Lukasz Olszewski, Computer security incident response and threat intelligence lead, Europe & senior expert, Atos

Proactive threat hunting: no longer a whim?

We are undoubtedly in the era of huge security alert fatigue. This has been caused by the vast number of false positive alerts generated every day by countless security products that organizations put in place to improve their defences.

Because of this, it's hard to justify resources who would essentially focus on producing even more alerts instead of reacting to the current ones. Those who do, however, want to invest in a second layer of more fine-grained detection often steer their organization toward proactive threat hunting activities.
The ultimate goal of the threat hunting process is to find malicious actors already present in the environment who have the intent, capability and opportunity to cause harm.

This is accomplished in parallel to and in cooperation with other detection systems and methods like Anti-Virus (AV), Host Intrusion Prevention System (HIPS), Endpoint Detection and Response (EDR), Intrusion Prevention System (IPS), Security, Security Information and Event management (SIEM), Advanced Threat Defense (ATD), etc. Successful threat hunting activity should provide at least three visible effects:

1. Security Incidents being reported only for identified and properly scoped intrusions. Reducing false positives.
2. High quality threat intelligence combined with indicators of compromise that can be utilized by detection and remediation tools being created. This intelligence can't be fully replaced by third party feeds. Security savvy organizations in general do not share intelligence about what they believe are the active advanced persistent threat attackers (at least not as soon as they have it). Doing so would mean losing the leverage they've gained.
3. Gradually improving the automation of hunting and detection capabilities.

"Manual" threat hunting is also available to supplement and utilize existing security monitoring mechanisms and not to replace them. Two good use cases are:

1. Finding previously unseen threats (including not only malware but also tactics, techniques and procedures used by adversaries).
2. Better scoping and understanding of events that manifest themselves in some manner, like IPS or AV detection, but in many cases are ignored and considered as successfully remediated when in fact they could be some tiny crumbs dropped by a much more serious intrusion.

What is needed: in short – visibility

The common issue organizations face with security incident detection and response is that they focus on the Interruption step (the numerous alerts) without assuring mature monitoring processes (to ensure all alerts are necessary). Large sums of money are invested in tooling but there is no resource allocated to operating and using these tools beyond responding to automatically detected events – real or unreal. This results in a fractional understanding of any given threat's real scope and leaves organizations chasing their own tails when it comes to fighting off advanced persistent threats.

Threat hunting is not a recent invention. It's been there in various forms for many years. What is new is the mindset and approach that needs to be applied. Setting up a successful threat hunting process requires:

- Dedicating full time people to this in the same way as is done in the case of security operation center analysts, responders etc. These people should not be responsible for Incident Response (IR) process.
- Integrating with existing detection methods.
- Some additional tools that are rarely deployed will be needed like threat intelligence exchange framework, data analytics solutions, network traffic recording and analysis capability, enterprise scale endpoint visibility.
- Baselines need to be created and constantly updated to understand 'the normal'.
- Building a solid understanding about the protected environment.
- Defining realistic goals. Threat hunters can't be required to find X intrusions in a month or they will focus on trivial things.

Marc Llanes Badia, cybersecurity global business development,
senior expert, member of the Scientific Community, Atos

Why managed Internet of Things security services is the next big thing

Imagine getting into your – future - office's front door and it is not opening because an IoT Distributed Denial-of-Service (DDoS) attack disrupted all the IoT-based access to it.

Yes you have multifactor authentication to get in, but your mobile (one of the factors) has no signal, your IoT-glasses do not have 5G connection anymore and even the smart-lock on the door is not working as the IoT gateways behind are not responding. Who to call?

We are not that far from this kind of IoT connected scenario. Internet of Things is here to stay. IoT took time to settle in the market but now it is moving from a buzz word to a key business enabler.

This is true today for Industrial environments (IIoT) but it will soon be adopted in all verticals and heterogeneous business areas, extending beyond IT or operations as it is today to all kind of processes in your organization... perhaps even the physical access to your office!

As Gartner predicts[1], IoT will increasingly involve changes for a broad range of processes in multiple business units as diverse as:

- **Sales** - IoT often enables a move from products to services;
- **Finance** - reflecting new revenue sources;
- **Marketing** - with new direct routes to customers;
- **Product management** - for life cycle management and product feedback;
- **Customer care** - for better insight into user behavior;
- **the CEO Office** - as this transformation will permeate so much of the organization.

The more IoT will expand within organizations the more it will deserve proper management, especially from a security perspective. Today, it is already a challenge to get any kind of standardizations in the IoT world either around hardware, software, platforms or communication protocols.

The adoption of new processes and verticals with new requirements will just increase this diversity... Such an increase will lead to an even more complex ecosystem which, in turn, will translate into a massive threat landscape.

No single vendor will be able to propose an end-to-end security solution for such heterogeneous IoT ecosystems thus Managed Security Services Providers (MSSPs) will become the only ones able to position themselves as the guardians of an IoT based businesses. MSSPs are already working toward such security platforms. Their experience in managed security services provides a competitive advantage against traditional vendors as:

- **Many services from cybersecurity can be extended to the IoT security world:** SIEM as a service for IT and OT, Identity of Things as a service, etc. However, every single service requires careful specialization and integration capabilities.
- **Multi-skilled MSSPs** having multiple capabilities and experience as software development and/or hardware manufacturing will pave the way to such complex integrations.
- **Leveraging being part of much larger IT services organization** will enable MSSPs to manage more parts of the IoT vaue chain.

Finally establishing the right partnerships and alliances will be absolutely key: it is not only about partnering with software and hardware companies specialized in IoT products, but also partnering with customers in proof of concepts and joint innovation programs.

Gartner[2] again forecasts worldwide IoT security spending will be beyond $3 billion in 2021. IoT managed security services will definitely be a big part of it.

[1] Gartner, Inc. "Market Trends: Strategies for Optimizing IoT POCs"
[2] Gartner, Inc. "Forecast: IoT Security, Worldwide, 2018"

Vasco Gomes, Global CTO for cybersecurity products, senior expert, member of the Scientific Community, Atos

Leveraging cloud: enhanced security in a multi-cloud environment

The cloud is a key enabler of digital transformation, allowing new levels of speed and agility for today's fast-paced digital world. Unfortunately, as well as multiplying opportunities, cloud computing has also spawned an alarming range of new security threats.

Cloud security has the boardroom's attention and is preventing some organizations from benefiting from the full power of cloud computing. Let's explore how businesses can increase trust in cloud technologies as the threat landscape evolves.

Security in a multi-cloud environment

Cloud computing sees your organizational data move beyond the traditional perimeter, expanding the attack surface. With cloud computing, you potentially share a platform with other organizations, and therefore potentially those intent on harm.
While your cloud service provider has some security responsibilities, their native security controls cannot protect you against the risks fallind under your responsibility, including those posed by your own employees. You need to monitor your internal environment: shadow IT, your data, your on-premises servers and infrastructure, or your owned virtual networks and workloads inside the cloud, whether virtual machines, containers or applications. You must manage the security of all these things, along with user identity and access.

Simply monitoring cloud services for any anomalies is not enough to secure your environment in a complex, multi-cloud world.
A new hybrid cloud cybersecurity approach is needed that gives you visibility of everything that happens in your internal landscape.

Hybrid cloud security in a nutshell

Enterprises' hybrid security approach must integrate all security controls into one overall strategy that is managed centrally, as well as consistently over your on premise and cloud (single or multiple) environments.
Central real-time monitoring and analytics provide global visibility into the consumption of IT resources inside and outside the organization and move quickly to close breaches of policies and regulations. They can identify any compromised accounts and threats such as unsanctioned devices, applications or users accessing or using cloud services or on the enterprise network. They also allow you to apply your security controls from a single console, consistently over your on premises IT and your cloud (IaaS, PaaS and SaaS) environments.
Data is protected from inadvertent disclosure or unauthorized sharing from insiders, including data that belongs to a company's intellectual property, whether that be proprietary software code or sensitive corporate information.

An automated approach is essential; removing the potential for human error. Security audits, controls, patching and configuration management can all be automated, reducing the risk significantly.

Three steps to hybrid cloud security

Addressing the cloud security challenges in today's hybrid, multi-cloud environment requires a transformation of your security organization, policies and controls. At Atos, we propose a three-step security approach:

- Assess: identify the risk and requirements. Analyze the current situation. Identify where you store sensitive data and the scope of shadow IT. Take external regulations and internal constraints into account.
- Protect: implement and update security controls. Protect your networks, workloads and data. Adopt encryption, for instance, to prevent data from being accessed, understood or used if other security controls fail. Implement a strong Identity Access Management (IAM) control to ensure only entitled users have access to your data as well as your decryption keys.
- Detect & respond: ensure real-time detection of security deviations and incidents, along with the means to automate an immediate response.

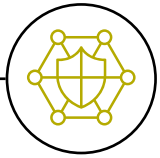
Embedding security since the development phases

We've seen that cloud computing can bring new security threats, but it can also deliver powerful new ways of implementing security controls. Infrastructure as a code, immutable infrastructure and network micro and nano segmentation, provide us with opportunities to ensure security controls are deployed early and consistently through the DevOps cycle, are delivered in an automated way and orchestrated with each other. This enables security organizations to tackle challenges such as controls exhaustivity, speed of security or lack of visibility and/or resources. It also makes it easier to respond to infrastructure security audits.
This 'Shift left' mentality helps by integrating security controls as early as possible in the development cycle but highlights how critical this cycle becomes.

Some early adopters are pioneering a new DevSecOps approach, introducing security early in the lifecycle by automating and embedding the appropriate controls into application development. DevSecOps encourages 'secure by design' approaches, in which source code is analyzed for flaws and vulnerabilities as it is developed, including open source libraries, and security controls are included the infrastructure deployment templates. As a consequence, it becomes mandatory to apply privileged access management principles to development environments, controlling the DevOps activities and the CICD (Continuous integration / Continuous Deployment) tools usage sensitive credentials.

As the threat landscape continues to change, the security strategies of all organizations can expect to experience severe tests. With a robust approach to cybersecurity based on a secure multi-cloud platform, protecting data that is shared across both public and private clouds, enterprises can benefit from the full power of cloud computing.

Simon Ulmer, Business development cybersecurity, strategic partnership with Siemens,
member of the Scientific Community, Atos



Collaboration for a cybersecure future

Establishing and maintaining trust is vital in the new digital economy. If trust is lost, markets will close, and businesses will fail. This is the stark reality for the digital transformation of companies. No one can afford to pass up the enormous potential of digitalization but at the same time no one can afford to run a system that is vulnerable to attack and data leakage.

Being entrusted with the data of customers, objects and processes is a privilege. It will improve and transform business models. But to be worthy of this privilege requires a clear approach to control security and maintain trust. This becomes even harder as companies are interconnected via global supply chains and global data chains are permeating more and more sectors.

Cybersecurity is not only an individual problem but a global challenge. We need to include everyone on the journey to a secure digital economy.

Charter of Trust

Understanding the importance of trust, we founded the Charter of Trust with 9 other global companies from different sectors, soon joined by 6 more. We agreed as partners that we should not wait for others to solve the cybersecurity issue at hand. We have developed a principled approach to implement smart business-driven solutions.

As a company deeply engaged in digital transformation and its implications, we understand what it means to manage, secure and use data and what happens to our businesses and to customers and end-users when we get it wrong.

Industry collaboration is vital

The frontier for cybersecurity has shifted. Hackers now not only exploit weaknesses in IT infrastructure but also those that have historically been less exposed, such as industrial control systems (ICS) or operational technology (OT). These cross-domain attacks are on the rise, as industrial companies move towards Industry 4.0 and the industrial IoT.

All processes covering the digital and physical realm must be protected – IT, OT and IoT.

This is where collaboration and partnership are key. An example of this is between ourselves and Siemens. We bring our experience in end-to-end digital transformation, IT security and data management, and Siemens, as global industrial technology leader, its knowledge of industrial processes, equipment and networks. Working together we are able to ensure that all networked systems are reliable and secure while bringing the benefits of digital transformation to our clients.

Digitalization adds tremendous value and will be a revolution on a par with electrification. However the challenge of cybersecurity could significantly deter the transformation. We have decided to work together for security and trust, to enable digital transformation and reap its benefits for humanity. We are proud to be a founding member of the Charter of Trust.

McAfee

Nigel Hawthorn, McAfee Cloud Business Unit, EMEA Marketing Director

Cloud security – It's not black and white

The people writing the software for self-driving cars are having difficulties. Telling a car to stop at a red light is relatively easy, but recent articles have pointed out the difficulties of merging into fast moving traffic and dealing with roundabouts.

In IT security we have some of the same issues – the basic decision making on unauthorized hackers or malware is straightforward, even if dealing with them is not. For cloud security, much of the decision-making is more complex – cloud services are rarely all good or all bad, so we need to look at traffic patterns from multiple angles to be able to decide if a particular request should be allowed.

There's no doubt of the need to secure cloud. Recent figures from the McAfee Cloud and Risk Report show that every company has some cloud use, 21% of files in the cloud contain sensitive data, 48% of users share data via the cloud and while IT often believe the number of cloud services is below 100, the average number of different services in a company is over 1,500.

It's easy to see why cloud has exploded, the apps are typically easy to use, the commercial terms are flexible and our own policies may actually force people to use the cloud. When I speak at events I typically ask how many companies have a restriction on the size of attachment allowed via email and more than 50% of people put their hands up. As email traffic is usually logged and often the first place that DLP is deployed, why do we have this policy? Typically, the answer is "we've always had it". Does anyone think that users will stop sending large files because of this restriction? What happens is that the user either uses an approved cloud app to transfer the data or simply searches for a way to send it and finds a free cloud service – probably not logged, not with DLP and who knows where the data ultimately goes?

To address cloud security we need to start from the beginning and get visibility into all the cloud services in use, the traffic being sent/received, the user actions and to be able to drill down into details such as which collaborators are working with your employees and the cloud-to-cloud traffic that is a growing part of the whole cloud ecosystem. This is, of course, required for SaaS, IaaS and PaaS.

Then, organizations need the ability to set policies from the simple (block known bad/high risk clouds) to the more complex (don't allow unmanaged devices to download files, check user behavior for anomalies, stop sharing via the cloud to untrusted organizations and deploy the same sorts of security technologies in the cloud as on premises, such as DLP).

The difficulty we often come up against is helping organizations define their policies – this is the real hard work. IT security need to be able to discuss with other departments, such as governance, risk and compliance and with the users themselves what policies are appropriate to make sure that they organization can have the right balance of rights and security.

To enable cloud securely, I always recommend the setting up of a cloud adoption team that is multi-functional, that looks at the needs and concerns of all stakeholders – allowing IT to enforce the policies agreed by the whole company.

From a technology point of view, IT security needs this list of capabilities to provide the visibility and controls required. With this set of tools, they can go into the cloud adoption team discussions with enough knowledge and capabilities to define a robust series of policies – allowing users to take all the advantages of the cloud while safeguarding the organization's confidential data.

- Quick accurate ability to define trusted and untrusted clouds.
- Stats on cloud use – with live updates and alerts and policy enforcement on unusual traffic.
- Multiple enforcement points that work for all, such as travelling remote users.
- Enforcement technologies – UBA, access control, sharing/collaboration control.
- The ability to intercept user requests and push to trusted clouds.

Sandy Forrest, Client executive, cybersecurity, Atos

Game changers for cybersecurity

While digital transformation delivers enormous value to business and society, it is only sustainable if it is achieved in a secured cyberspace.

We now have a far more connected world, with the exponential growth in the Internet of Things (IoT) and more sharing of data between information and operational systems. At the same time, cybercrimes such as data theft and ransomware that spread across corporate networks are endemic, with the motivation and perpetrators often unknown; and the Dark Web is awash with stolen credentials for sale.

Cyberspace without borders

In recent global cyberincidents, it wasn't just the effect that was important, it was the impact. One attack infected 100,000 servers and led to patching of tens of millions of others, causing disruption on a worldwide scale. Viruses tend to go where they can, not necessarily only where they were intended. WannaCry wasn't a targeted attack on the NHS in the UK; it just found its way by exploiting connectivity. Similarly, the NotPetya attack targeting Ukraine ended up infecting a UK ad agency, a global law firm and an Indian container port. It's a game of unintended consequences.

Cyberspace has no borders. The ability for cybercriminals to attack has been expanded dramatically through the leaking of state-developed tools, the open sharing of exploits by hackers, the re-purposing of penetration testing software by criminals, and the uncontrolled circulation by 'researchers' and 'bug bounty hunters' of vulnerabilities they have found. Cyberattacks are by their nature 'asymmetric', which means they can come from anywhere: you don't need many original skills to mount a successful one – the necessary advice and tools are available online.

New frontiers

To address these and other challenges, we need to create some new frontiers. One approach is to be more effective in segmenting our infrastructure at national, organizational and personal level, and by effectively monitoring data flowing in, out and within it.

New concepts in cybersecurity such as 'micro-segmentation' and 'application containers' are designed to limit potential damage to an area that is as small as possible then corralling it there.

Shared responsibilities

In the 1970s, the concept of Secured by design advanced our understanding of how to make communities safer, by creating "a residential environment whose physical characteristics – building layout and site plan – function to allow inhabitants themselves to become key agents in ensuring their security" (Oscar Newman – *Defensible Space* 1972). This thinking can even now provide valuable insight for our new cyberworld and how to make it safe. Common areas (the internet) belong to everybody, so we all have a vested interest in securing them.

We can put controls in place to reduce the potential for harm, but these will be ineffective if not matched by a responsible and informed attitude to computer use by all users. User behavior is as important as security controls. These concepts of personal responsibility, shared ownership, acceptable surveillance and defence in depth, treated together as an ecosystem, rather than individual elements, translate well to cyberspace.

Prescriptive security

With porous external boundaries, we need a more granular approach that creates boundaries inside the network: reducing the target area, and preventing illicit lateral movement and exfiltration of data. We also need to evaluate risk based on evidence. That evidence comes, in the main, from cybersecurity monitoring systems combined with collated, actionable intelligence about threats.

Atos' vision for cybersecurity recognizes all these interdependencies – and encourages a more balanced approach to protection, detection, reaction and recovery, with a move to prescriptive security. This means that in addition to powerful computing and sophisticated analytics, there is an effective combination of human behavior and machine capabilities, enriched by effective management of threat intelligence.

> Even if your cloud environment is secure, it can still be compromised through the way it's used internally and through malicious activity.
>
> To be able to fully trust your cloud you must keep control of the whole environment, both inside and out. This means managing and maintaining ownership of the identities that can access it, providing your own encryption mechanisms and closely monitoring for external intrusion.
>
> **Alexis Caurette, Group Vice President, Head of Cybersecurity Products, Atos**

Noémie Vasche, Business developer - Cryptographic products, Trustway & cybersecurity, Atos

Encryption, a necessary brick in the foundations of GDPR

From the transposition ciphers in Ancient Greece, to the development of rotor cipher machines in World War I and the advent of computers in World War II, the methods used to carry out cryptography have become increasingly complex and its application more widespread.

Now, with the EU's GDPR legislation, encryption is attracting growing interest. The number of people affected globally by data breaches in 2017 soared by 88 per cent compared to the previous year, with 2.6 billion records stolen or compromised. This, reinforced by the arrival of GDPR, has seen encryption gain particular prominence because of its ability to render breached data useless to anyone that is not authorized to access it. Indeed, encryption is one of the recommended solution in the context of the GDPR. Of course, encryption doesn't exonerate the company of its responsibilities but relieves it considerably in case of a data breach to the point that some could see it as a miracle cure.

To be clear, cryptography is only one element among many safety measures that must always be considered as a whole. Although encryption can also be a significant drain on budget (around 15 percent of the IT average security budget) and network performance, it enables organizations to better protect their data and avoid to pay penalties up to 4% of the total turnover, in the GDPR context. Therefore, despite its advantages, it is important for businesses to only use encryption where it is most suitable.

Centralize to manage diversity

In terms of encryption, a centralized hardware platform in its data centre under its own control remains the safest, most convenient and clearest solution in terms of accountability. One of the specificities of encryption in the context of the GDPR is that it concerns many more varied types of data and environments than in the security contexts where it is traditionally used. We will eventually have to encrypt structured and unstructured data, virtualized and archiving environments and applications in the cloud. Another peculiarity is that we will not only encrypt dynamic data, to protect it during transfer, but also static data, "at rest", especially in databases.

To respond to this diversity of situations, the encryption solution must be sufficiently agile and service-independent. In particular, it will rely on technology standards and the entire ecosystem of software vendors so that it can easily fit into the company's computer systems.

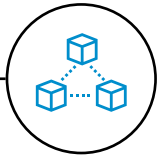
To maximize this flexibility, it is better for business leaders to opt for a centralized platform, which will become the sole trusted resource for all information systems because a centralized platform allows the Chief Information Security Officer (CISO) to regain control over encryption.

Cryptography, a future beyond GDPR?

When choosing their tool, the CISO and the company must not lose sight of the fact that cryptography is not a solution quite like any other and that it does not always benefit from the latest technological trends. However the solution is fit to adapt to any kind of IT environment. As far as the increase in cloud computing is concerned, the CISO should be cautious that the encryption and decryption keys and the data that they protect should not be stored in the same place. When delegating to a cloud provider, the management and control of keys is a serious responsibility that can only be exercized in a strictly controlled contractual and operational framework. Furthermore data sovereignty is a key challenge that must be taken into consideration.

By encouraging more data protection, the GDPR, in addition to other sectoral regulations in health or banking are now making cryptography mainstream. While its potential remains largely unexplored, it will take its place in corporate security policy, as a tool that is by no means sufficient on its own, but one that is certainly necessary.

David Leporini, Director IoT security, member of the Scientific Community, Atos



Blockchain: beyond payments

Because the blockchain protocol was first designed for the development of the bitcoin cryptocurrency as its underlying architecture, it's only natural that so far it has been most widely used in the financial services and payments sectors.

After all, there are immediate attractions to a means of payment which does not rely on banks, which is not controlled by centralized institutions, and which creates complete trust between separate parties who are engaged in a monetary transaction.

But the real potential of blockchain goes far beyond the financial sector.

Today's market economies operate on the assumption that different players cannot trust each other without an accredited third party establishing that trust. But in a blockchain system, trust is intrinsic. It is native to all members of the network. All parties in a blockchain consortium can see the same certified information, at the same time. No single entity has more power than the others.

This has dramatic implications for all areas of economic activity. Any group of companies that share a common need to trace and record information, for example to manage shipments across a complex supply chain, can take advantage of the technology to develop new business models.

The basics

Blockchain is often described as a distributed or shared ledger, to which all parties in the network have access.

Different parties around the world can track and trace information, in the assurance that everyone in the network has the same version of that information. When changes are made to one copy of the ledger, all other copies are automatically updated. Inside this distributed ledger, transactions are encoded into blocks and then linked to each other cryptographically – hence the name, blockchain. It's not possible to tamper or delete information that enters the ledger. Any participant can verify the information at any time.

Private vs. public

The best-known blockchain networks include Bitcoin, which uses the protocol to enable secure crypto-monetary transactions, and Ethereum, which uses blockchain to record smart contracts (beyond just transactions, they permit execution of code on each node, leading to decentralized applications).

These uses of blockchain are public – anyone on the Internet can use them. This makes sense for mass blockchain applications such as bitcoin.

However, for commercial uses I believe that private, permissioned blockchain networks are more appealing. Only authenticated companies with the right credentials can access and participate in these consortia. There is no room for anonymity, and companies can have more control over the visibility of their data. Compared with public blockchain, these private networks also cost very little to run and consume much less power.

On the road again

Permissioned blockchain networks can transform the efficiency of markets across all sectors. For instance, Atos is participating to a collaborative project in the IRT SystemX institute exploring opportunities of Blockchain benefits for several verticals, including the automotive market. Currently, when someone buys a second hand vehicle, there is no sure way of knowing whether the information contained in the car maintenance record or on the milometer is accurate. A private blockchain network has been set up as part of this collaborative initiative to limit the potential of such fraud. When a car owner takes a vehicle into a garage for service or maintenance, all information about the car – including the distance it has travelled – will be entered into the shared, distributed ledger using blockchain. This cannot then be changed. Any potential buyer will just have to check the network to make sure that the information on the meter and in the maintenance book corresponds with the reality recorded using blockchain.

For the fraudulent, there will be no place to hide

The implications of innovations such as these – not just for the used car market but all over the economy – are far-reaching. Yet these developments are only scratching the surface of the technology.

Over the next years, I believe we will see companies and governments begin to wake up to the full potential of blockchain to transform the world we live in.

Jordi Cuesta, Evidian I&AM product Director, cybersecurity, Atos

Identity & access management: avoiding binary choices

As a major editor of identity & access management (IAM) solutions we are witnessing an increasing need for adaptive and agile delivery models in the IAM sector.

Today, organizational structures can be very complex. Large organizations are often split into separate business units which can operate very differently. To reduce costs and improve security and governance many organizations are now looking to harmonize processes across their entire business.

IAM for multi-entity groups: a new paradigm

In large groups, the smallest entities may not have the critical size to support in-house projects. The lack of human, technical and financial resources is the first hurdle for the implementation of IAM projects. 'Classic' on premise solutions can be too costly to acquire and own, and their implementation in every single entity would turn out to be overwhelming.

Today, one of the main IT trends is the shift from solutions hosted on premise to outsourced shared pools of configurable system resources and services, more commonly referred to as Software-as-a-Service (SaaS) or 'Cloud' solutions.

However, market experience and customer feedback has shown that many large companies haven't made a decision yet when it comes to IAM. Many prefer to try to keep these services in-house to maintain control and worry about the lack of service levels from cloud service providers.

A shared-services IAM solution is a "private cloud" where the main advantage is that organizations only need to buy a unique license for a solution that is centrally hosted and administered. Capital expenditures are shared and operational expenses optimized.

Various degrees of freedom

This type of project is also able to meet the demands of individual business units by allowing some flexibility on governance and IT.

Depending on the degree of freedom the leading entity grants to its business units, it sets the degree of customization of the solution. The configuration scope can go from only shared machines and software to a fully configured IAM solution with strict governance and unique processes.

After defining the functional scope of the solution, the implementation team assesses the technical specifications for the physical architecture necessary to the project. The functional distinctions between subsidiaries and the degree of customization allowed will impact the identity, the application and entitlement attribution lifecycles as well as administrative function.

The goal at this stage is to ensure the long-term sustainability of the solution and avoid the technical debt that could derive from a too high level of customization. The success of a shared-services IAM project relies on strong governance and the full engagement of the main stakeholders across all entities. Capacity to execute must be optimal to harmonize processes and manage change.

An adaptive approach

This type of delivery model is not new but tends to be overlooked as SaaS IAM solutions are now on the market. It provides an answer when a completely outsourced solution doesn't meet customers' needs.

We can avoid binary choices and be more flexible with solutions that meet the needs of those who would want on premise solutions but need the scalable and adaptive approach of cloud.

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 billion.

European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting-edge technologies and industry knowledge, Atos supports the digital transformation of its clients across all business sectors.
The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, Unify and Worldline. Atos is listed on the CAC40 Paris stock index.

Find out more about us
atos.net
atos.net/cyber-security

Let's start a discussion together

CT_190305_AS_DIGITAL-VISION-CYBERSECURITY(GMM)