Whitepaper

ready for anything

Business driven security for the digital era

Your business technologists. **Powering progress**

Atos

Building trust and ensuring compliance

The new alliance of business goals and security needs for digital transformation

Are you ready to succeed in digital transformation? To safely and securely welcome millions of new customers? To openly foster the development of new partner ecosystems? To easily leverage yet undiscovered business models? In a nutshell, are you ready to make trust and compliance a new success pillar for your digital strategy? And are you ready to evolve your company's security from a burden into a revenue generator for the digital age?

We are living in a time of paradox. Riding the wave of digital transformation, business opportunities have never been so rich. And yet, with those opportunities come new, almost unfathomable risks – and security systems, in most cases, have simply not caught up. A staggering 90% of enterprises recognize that their defenses are insufficient. Recent calculations of cyber crime costs are already hitting $345bn per year, and dangers are escalating each day with the upsurge of the Internet of Things (IoT), 3D printing and intelligent machines – indeed, some experts predict privacy itself will become a thing of the past.

It may feel as if cyber security in the digital age is becoming a Sisyphean task. It may feel as if our corporations lie inevitably in the hands of providence, in a world becoming each day more complex, dangerous and unpredictable. But competitive businesses will recognize this as the rise of a new era, calling for a new security approach: an approach where security will not only be designed to manage these uncertainties, but will be designed at the very heart of the digital growth strategy. Thus creating a new alliance between security and business, and empowering businesses to be as ready for opportunities as they are for threats.

We have heard it for years: digitalization increases risks

From Sony to Target, from JP Morgan to the White House, attack reports demonstrate daily the dangers facing corporations and governments alike. Indeed, with the convergence of the physical and digital worlds, security becomes a wicked problem. Threats not only grow by 20% per year; they grow in magnitude and voracity. Hackers are no longer just those lonely few individuals with a nasty hobby; they are organizations working at mafia, terrorist group and even state level. And the risks reach far beyond the $345bn yearly financial damages; they also put corporate and national viability in jeopardy. As the world goes digital, so do economic and military battlefields. It's no wonder that analysts predict that, by 2020, 25% of global enterprises will engage the services of a 'cyberwar mercenary' organization.*

Yet, while fraud, sabotage, blackmail, espionage, and cyberwar risks have never been so high, never has protection been so comparatively weak.

The reason? As digitalization is vital to success, the general perception is that the potential benefits outweigh the risks. Clearly, for many it seems better to create immediate advantage with new mobile applications or connected devices, interconnect with new ecosystems, or go to the cloud, than to wait for the necessary security to match.

And so the great divide: while CISOs diligently recommend increased security efforts, protection simply is not growing proportionately to the speed and magnitude of risks.

But does all this mean we should simply wait for the inevitable, and bluntly recognize, as FBI Director James Comey does, that

"there are two kinds of big companies... those who've been hacked... and those who don't know they've been hacked"?

Is this growing divide between potential risks and concrete security measures all the proof we need that, in the never ending battle between the sword and the shield. The time has come for a change of attitude, for new security strategies that can embrace a changing, open and unpredictable world.

*Source: Gartner

The end of security as we know it

The new golden rules for digital transformation

For years, security experts have defined strategies, deployed protection technologies, and set up compliance processes. Existing security techniques remain essential. But analysis of best practices consistently shows that three essential commands are now of vital importance – three very simple rules that are at the heart of security for the new digital age.

Rule 1: evolve from risk-driven to business-driven security

Let's face the truth: in a digital world, deploying ring-fenced security has become an endless task. How to handle ecosystems comprising hundreds of partners, thousands of employees, millions of customers and things, interconnected and vaporized into the cloud? Of course, multi-layer perimeter protection, identity and access management federation, endpoint and application security will continue to help. But focus continues to be the enigma: which will be the key assets to secure? These questions have always been the daily concerns of Chief Security Officers. But tomorrow's security will demand a new paradigm. All risks can be triaged for management: should the risk be tolerated, transferred, treated or terminated? Corporations need to seriously consider their risk analysis of digitalization:

- Will a digital scenario grow customer experience or weaken reputation?
- Will it boost operational excellence or generate opportunities for fraud?
- Will it sustain business advantage or threaten intellectual property?
- Will it have an impact on privacy and therefore customer trust, compliance and legal issues?

But these questions must persistently be grounded by a central question: what is the potential business value? In a world where complexity grows and yet digital speed of development is essential, it is critical to define fully business-driven security policies. With business-oriented scorecards, tools, and assessments involving all stakeholders.

Atos insight

by Alexis Caurette, Cyber Security Consulting & Integration Director, Atos Big Data & Security

At Atos, we believe that risk mitigation and security are a business issue before being a technical and process one. To ensure adequate security, it is essential to analyze in depth which are the truly critical risks from a business point of view, and to arbitrate on protection measures from these business perspectives. While several risk-balancing methods have existed for years, analysts estimate that only 20% of businesses have put in place effective risk management. To succeed today, three approaches will be essential:

1. Make security a core track of the digital strategy, constantly linking security and business

The objective here is for C-level executives to take security into account for digital initiatives, rather than seeing it as a business inhibitor. For example, one of Atos' clients, a large electricity utility company, has been able to accelerate its digital transformation and meet customers' security and privacy concerns by integrating security into its innovation strategy and linking business value to security. The result: fully combining business growth and customer trust, by securely connecting four million homes to its new smart meter network and assuring personal data privacy for all its clients.

2. Take all the ecosystems and value chains into account

As boundaries blur between digital and physical worlds, between corporations and partners, between suppliers and customers, the trust value chains are rapidly evolving. In the past, corporations have often been accustomed to operate in an 'us' and 'them' culture. These frontiers fade. As a result, holistic thinking is not only useful – it is a vital necessity. For example, another Atos client, this time a multinational manufacturing company, has measured the security risks across its entire extended ecosystem, to streamline new generation identity and access management for millions of customers, suppliers, partners and employees. The result: boosting both security and customer experience.

3. Put customer trust and privacy at the core of your strategy

The current digital revolution puts the customer back at the center. Security must not be an exception. It must be designed to protect the most important thing for a corporation: its customers. For example, Atos has helped a European sovereign public Cloud, launch a highly secure cloud offering. The impact: not only a high protection level, but a strong business asset that is growing opportunities with security sensitive industries and public bodies.

Innovative trend

The rise of cyber insurance, for both IT and Operational Technologies (OT)

Should everything be protected? The answer may not be a simple yes or no. A third solution exists: cyber insurance. This is a growing domain for large insurance groups – notably to protect their customers from regulation risks, and prepare for upcoming European laws on customer data privacy. No-one can understand better than insurance companies how essential risk quantification is. It opens up interesting opportunities: a partnership between insurance players and security specialists for initial audit and potential forensics.

This is the choice of insurers such as Gras Savoye, who are developing with Atos a unique end-to-end security strategy. This approach has strong added value as cyber attacks are no longer confined to IT, but are also targeting OT, including technical infrastructures and smart connected objects. Leveraging its industrial expertise, Atos has developed a global methodology to help organizations identify their vulnerabilities, and control and mitigate the risks across OT and IT. Based on both IT and OT security standards, Atos is therefore unique in the market in fully securing the IT/OT value chain. Examples include connected cars for Renault, payment devices with WorldLine, OT with Siemens – the list goes on.

Rule 2: deploy data-centric protection measures

Data is now surely the most critical asset in the digital world. Once a side-product of applications, data is fast becoming the core enterprise capital. With the emergence of the Internet of Things, we're entering a world where universal embedded intelligence will transform any object into a smart device. And the one thing that will bring people, processes and things together is data.

Logs, conversations, transactions... data is becoming the new resource that will power tomorrow's economy, as finance did in the previous century. At stake is a better understanding of customer behavior, a better capacity to optimize business processes in real time, and new insights that can be exchanged, bartered or even sold to create new business models. Infocentric corporations are already 20% more profitable and achieve twice the market value of their peers.

There can be no surprise that data now is the focus of cyber attacks. As the Sony or WikiLeaks cases showed, data leakage is one of the most pressing issues today.

The consequence is clear: in a digital world where data is at the heart of enterprise value, it must also be at the heart of enterprise security.

Innovative trend

Cloud-based Data Loss Prevention (DLP) as a service

What should companies worry about most – protecting critical data from the insider threat, or protecting business from organized cyber criminals looking to sell their IP to the highest bidder? To make advanced Data Loss Prevention services easily available, Atos has launched an innovative new cloud-based DLP service deliverable anywhere in the world and enabling rapid deployment and scalability over a short payback period. This fully managed cloud service incorporates Atos' Security Operation Center and expertise in DLP. It provides a robust risk management service and strongly prevents data theft, whether it be from unauthorized insider activity or external threats.

Atos insight

by Gerrit Pot, Global Offering Manager, Cyber Security, Atos

At Atos, we believe that data security policies demand an extension of current security strategies. That is to say, it's not only a revision of policies that is required; but also a revision of architectures and tools, from end points to infrastructures. To succeed, three approaches will be essential:

1. Break silos to ensure a holistic data-driven approach to security

The old security adage is well known: why hang a reinforced door if you leave the window wide open? Too often data is scattered around multiple databases with different processes. Gartner estimates that "through 2016, more than 80% of organizations will fail to develop a consolidated data security policy across silos, leading to potential non-compliance, security breaches and financial liabilities". Atos has developed specific methodologies to handle this challenge. For example, we have helped a major multinational company to specifically protect critical data across silos by designing an advanced Application Resource Island. The result: golden nuggets available for business use representing several billions of Euros in revenue, but kept under tight control and secure monitoring.

2. Deploy data-centric technologies

Beyond encryption, data masking, DCAP (Data-Centric Audit and Protection) technologies and so on, new layers of contextual identity and access management are needed. Is the user the right person with the right role to access the right data to perform the right actions? Both context and behavior need to be examined so that appropriate correlation engines will be able to take appropriate decisions. Atos has helped several of the largest European banks set up high-end security for trading desks, saving billions of dollars.

3. Take into account the evolution of the data life cycle

Business data is not an inert material; it is a living component. For example, non-sensitive data can be correlated to become sensitive; and archived data may require declassification after some time. Data security must take this evolution into account, and move from static to dynamic assessment. For example, Atos has delivered a data-centric security solution for a world-leading pharmaceutical company, so that R&D data can now be safely monitored, avoiding IP losses that could cost billions.

Rule 3: evolve to real-time pre-emptive security management and forensics

The rising digital world is not only more complex; it is also faster-paced. To gather the first 50 million users took 18 years for mobile phones in the seventies and eighties – but only three months for Google+ at the beginning of this decade. And still the pace accelerates.

As a result, foreseeing future problems and opportunities is ever more difficult. Security may have been well planned in the past, but it cannot be immune to new kinds of unknown attacks. So in an increasingly complex world evolving in real time, it is essential to re-orient security budgets from generic protection to rapid detection and reaction responses. New security strategies must adapt to an increasingly real-time, inherently unpredictable world; one, where being able to react to the unknown, or even trying to predict it, will be a matter of life and death.

Real-time security mechanisms will be necessary to constantly monitor and identify suspicious activities, counter-react without delay, and set up immediate remediation actions. It will be a new "defcon" (defense condition) and pre-emptive security approach, whose essential operational management importance is highlighted by the rise of next generation Security Operation Centers and forensic strategies.

Atos insight

by Zeina Zakhour, Cyber Security Chief Technical Officer, Atos Big Data & Security

At Atos, we believe that security is increasingly becoming a Big Data challenge: not just how to sense and respond to threats in real time, but more: how to evolve from reactive to proactive and even pre-emptive security? To succeed, three approaches will be essential:

1. Set up a real-time security governance process

Advanced Security Operations Centers (SOC) and Security Information & Event Management (SIEM) must be integral to new security strategies. Atos has notably built 'Atos High Performance Security' – an advanced network of SOCs/CSIRTs (Computer Security Incident Response Teams) to answer this need 'as a service', by leveraging the latest insights on threats and protection landscapes. Used by many of the largest and most sensitive corporations worldwide, we provide 24x7 protection and instant reactions – as demonstrated during the latest Olympic Games, where hundreds of millions of threats came to zero breaches. Atos also helps corporations willing to benefit from their own private SOC to deploy advanced sovereign security operation centers.

2. Deploy forensic teams

Endpoint forensics teams will be increasingly needed to examine and sort vast amounts of digital computing information to find chains of evidence that can be used in courts of law. Associated to SOC, they must combine international and local expertize, to handle regional context and regulations. For example, Atos is helping its customers quickly and effectively contain targeted attacks to limit the business impact. Atos CSIRT forensic teams also reverse engineer attempted breaches in order to track down the perpetrators, collect the evidence and bring them to justice.

3. Move from reactive to pre-emptive security

While most forensic work today responds to crimes after they have been committed, putting in place real-time controls to prevent cyber attack (proactive security) and anticipate threats (pre-emptive security) will be more and more essential in the years to come. For example, Atos has implemented an advanced persistent threat detection and remediation solution for an international customer in order to detect targeted attacks from Day Zero. Not only does Atos SOC detect in real time unknown and pervasive attacks, but it also provides the automated mechanisms in order to block and neutralize such attacks, reducing the business impact to almost zero.

Innovative trend

Big Data analytics at the heart of next generation Security Operation Centers (SOCs)

Billions of logs, millions of users: security has entered the Big Data era with SOCs and SIEM. With the ever-growing level of threats and the increasing complexity of attacks, a new approach is needed for detection. Companies will need advanced predictive security and context-aware, actionable security intelligence that exploits the power of next-generation analytics in order to detect suspicious patterns.

Taking advantage of the event log feeds used by traditional SIEM, and combining these with many new data feeds, Atos is developing next-generation machine-learning and Bayesian analytics that enable deep analysis and may uncover Advanced Persistent Threats (APT). In addition, Atos has developed threat intelligence services that crawl the deep web and other underground forums to search for early warnings of threats and unknown threat patterns. By correlating monitoring services with threat intelligence, we can provide analysts and security solutions with a predictive view on threat evolution and potential business impact, that enables pre-emptive protection for most verticals – from homeland security to financial fraud management and theft management in utilities.

Building trust, leveraging opportunities

In everyday life, the first lever of business has always been trust. Can you have faith in the vendor you're dealing with? In the digital world, that has also always been a key concern, but the rise of the Internet of Things gives it a new dimension.

When you entrust your personal data to a telco that will therefore know everything about you and your life; when you give your financial assets to a bank that could wipe them in a few milliseconds on high-speed trading networks; when you pilot your home with smart utilities devices whose sensors could be hijacked; when you put your life into the hands of a self-driving car whose software may be taken over by malware; when your own life may rely tomorrow on connected healthcare such as artificial heart systems – then you require absolute trust.

Security is, in this sense, at a turning point. Not only is it necessary to reduce risk and ensure compliance with regulations. But by reducing risks, corporations can be empowered – to be more trusted, more agile, and take business to new heights. Security becomes a key enterprise asset for business, providing tangible business value for corporations striving to win the uncharted territories of the hyper-connected world.

In this way, cyber security **is not only the key to facing unexpected dangers, but to leveraging unexpected business opportunities as well.**

- Being able to accept millions of new customers
- Being agile enough to foster the development of unexpected partner ecosystems on secure APIs
- Being nimble enough to leverage the need for new business models in the upcoming economy of data

Indeed, in the coming digital age, just as data is becoming the new currency, trust may well be the most intangible business asset. For years, rating systems have shown how businesses in the retail or travel sectors can be dependent upon reputation. Tomorrow's hyper-connected world will take this concept to a new level.

In a nutshell, beyond protection, security is becoming a new business asset in the digital journey. An asset that will:

- Grow **customer experience** – facilitating secure and seamless access to information and assuring customer trust about data privacy
- Boost **operational excellence** – ensuring business value chains are not at risk (from production to distribution and customer service)
- Support **business reinvention** – by securing innovation and protecting the most precious asset: data

This is a strategic move for cyber security – and a Copernican revolution that will turn security from a burden and a cost center for the business, into a revenue generator.

Security: think globally, act vertically

Digital devices and platforms have created multiple opportunities for organizations of all sizes, and across all industries, to gain a competitive edge. Digital is now playing a fundamental role in businesses by helping us to work, stand out and communicate in new ways.

However, with every potential reward there's a potential threat. Balancing access to critical systems, networks and data with security, control and management is a constant challenge. And as security threats constantly evolve and shift, this balancing act is never resolved. Digital security is a global issue.

However, are there characteristics that are specific to each vertical? Even though the solutions that many businesses adopt are universal – security policy management, identity and access management, communication security, SOC – the level of protection and specific business risks vary tremendously across industry verticals and organizations.

Finance is particularly exposed to threat. Today, it is recognized as the prime target of cybercrime. Disgruntled traders have also recently demonstrated how they can use digital access to manipulate finance centers. The devastating impacts have resulted in imposing very high security measures for trading desks.

The impact of their actions goes far beyond the IT department. They have also generated major business challenges and triggered in-depth reviews of compliance and regulation at both a local and global level. It is now estimated by industry analysts that 50% of banks' IT budgets may be impacted by regulations such as the Anti-Money Laundering Act, Foreign Account Tax Compliance Act (FACTA), Dodd–Frank, stress tests and Basel II. The rise of new cryptocurrency technologies may also introduce tremendous disruptive challenges in the near future.

Media & Telecoms is another vertical at the forefront of security issues. Their public visibility makes them an obvious target, threatening either data integrity (defacement for propaganda), availability (denial of service attacks) or confidentiality (including customer data). There are also specific challenges such as digital rights management (DRM).

Energy & Utilities may well experience a surge of threats in the years to come. For Utilities, the rise of smart grid, smart metering and smart home are creating immense opportunities for business and consumers, but also opening up opportunities for cybercrime and misuse. Operational technologies are particularly important targets. When it comes to cyberwar, it is no surprise that Utilities is recognized as one of the most strategic potential targets, therefore demanding the most stringent protection strategies.

Oil & Gas companies must protect customer data and shield essential resources from the threat of cyber-terrorism, while responding to increasing regulatory reporting obligations – such as social and environmental compliance – in a timely and transparent fashion.

Retail has been frequently attacked at the front-office level, with threats in the form of fraud or blackmail. Unfortunately, these threats will never go away. In addition, the rise of integrated 3D value chains (demand-oriented, data-driven, digitally executed) and connected objects may well make **manufacturing** and **transportation** become the next strategic targets for cybercrime, requiring highly specific protection measures, notably in IoT, machine learning, artificial intelligence and robotic security.

Healthcare is also at risk. The rise of 'connected health' initiatives create opportunities for digital attacks. Compromising healthcare data could directly threaten life itself. This potential makes it one of the most critical verticals for the future of security.

Public Sector is also experiencing a step-change thanks to digital, both at its own level (with process digitalization and open data) and as a critical foundation for all other verticals, such as defense and homeland security, regulations, justice and common public services. As a whole, this is very attractive ground for cyber-terrorism and security issues must not only be treated in isolation, but also within a more global trust and compliance framework, encompassing domains such as risk management, transaction security, fraud prevention, critical systems design, compliance governance and regulatory reporting.

With a seamless alliance between business and technology thinking, this is an approach that Atos has put at the core of its digital transformation offering in all verticals.

Conclusion

In this new world, security will never be the same. To succeed, enterprises need to change their security mindset, embrace new security "rules" and embark on a fresh, holistic approach with:

- Business driven selective risk management
- Data-centric protection strategies
- Increased investments in pre-emptive security and forensics
- And business-minded security to prepare for the unexpected

Atos cyber security: a new breed of partner

To succeed, companies will need a different breed of partner. Partners that link security and business within a consistent digital transformation approach. Partners that assess and manage risks along the whole value chain, from connected devices to infrastructures. Partners that grow data-centric strategies. Partners that have evolved from reactive to pre-emptive security strategies, with advanced SOC and forensics around the globe. In a nutshell they will need companies that intrinsically link security and business, consulting and operations, services and technology. To make trust not only a defensive asset, but a true lever for business value.

Atos is a leader in digital services with 93,000 employees in 72 countries. As the trusted partner in digital transformation, Atos helps large corporations and governments ensure business-driven and uncompromised trust and compliance.

A world leader in integrated cyber security, Atos is unique in providing an end-to-end protection, encompassing:

- Global security lifecycle management, from consulting to managed cyber security services, with more than 4500 security specialists worldwide and eight 24x7 Security Operations Centers across the world
- Global IT/OT security expertise across digital value chains, from connected objects and cloud applications to back-office platforms and critical IT infrastructures
- Global business security expertise across specific markets, from manufacturing, retail and transports to finance, telco, media, utilities, public and health

Atos' expertize builds on more than 25 years of experience in providing robust, comprehensive and fit-for-purpose security solutions and services for the most demanding organizations. It also builds on the acquisition of Bull in 2014, a recognized player in defense and Big Data, with advanced solutions in identity and access management, security analytics, encryption, and critical systems for defense and aerospace. As a result, Atos not only offers the largest set of security technologies to build and run appropriate, custom and business-driven security solutions, thanks to its vast ecosystem of partners. It also provides breakthrough technologies when high-end and sovereign security solutions are needed.

Atos innovation flagships include the leading European payment and secure transactions platform with Worldline; the first natively secure smartphone in the world, Hoox; advanced smart objects security for example with the connected car or Smart Grid; advanced security for trading floors; and extreme security systems in the most critical domains such as defense, nuclear and aeronautics. Each day, millions of lives are protected by Atos critical defense systems, 13 million transactions are handled by Worldline, 100 million identities are securely managed with Atos IAM technologies, and two billion security events are analyzed in Atos SOCS, resulting in hundreds of billions of Euros of digital business secured each day.

Take action now

To find out how Atos could be the partner you need, why not attend one of our assessment or innovation workshops – where you can learn how we have helped other organizations tackle new kinds of exposure, and hear more about the latest best practice in cyber security?

You can also apply for one of our free consultations, such as the Atos Security Scan. In these sessions we can assess the current state of your security position and determine whether it is fit for purpose given current and emerging threats.

Read more at: www.atos.net/security

About Atos

Atos SE (Societas Europaea) is a leader in digital services with 2014 pro forma annual revenue of circa € 11 billion and 93,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defence, Financial Services, Health, Manufacturing, Media, Utilities, Public Sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organisations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Healthcare, Atos Worldgrid, Bull, Canopy, and Worldline.