Whitepaper

# ready for anything

## Business driven security for the digital era

Your business technologists. **Powering progress**

Atos

# Building trust and ensuring compliance

## A new alliance to put security at the heart of business and innovation

**Are you ready to succeed in digital transformation? To safely and securely interact with millions of connected citizens? To openly foster the development of new private partner ecosystems? To redesign new models for delivering public services? In a nutshell, are you ready to make trust and compliance a new success pillar for your digital strategy?**

**We are living in a time of paradox. With digital transformation, never have the opportunities for innovation been so rich. Yet with those opportunities come new risks – and security systems, in most cases, need to catch up. A staggering 90% of enterprises recognise that their defences are insufficient. Recent calculations of cyber-crime costs are already hitting $345bn per year, and dangers are escalating with the upsurge of the Internet of Things (IoT), 3D printing and intelligent machines. Some experts predict that privacy itself will become a thing of the past.**

**It may feel as if cyber-security is becoming a Sisyphean task. But fore-thinking decision-makers will recognise this as the start of a new era that calls for a new security approach that will empower public bodies to be as ready for opportunities as they are for threats.**

### We have heard it for years: digitisation increases risks

From Sony to Target, from JP Morgan to governments throughout the world, reports of cyber-attack demonstrate the dangers facing corporations and governments alike. Threats are growing by 20% per year and as the world goes digital, so do economic and military battlefields. While the risks from fraud, sabotage, blackmail, espionage and cyber-war have never been so high, there is huge pressure on security departments to protect corporations and public bodies. And so the great divide: while security managers diligently recommend increased security efforts, business leaders are looking for freedom to reinvent operating models and connect with customers and citizens in completely new ways. Is this proof that the time has come for a change of attitude, for new security strategies that can embrace a changing, open and unpredictable world?

# 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 practice consistently reveals three simple rules that are essential for cyber-security in the digital age.**

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

In a digital world, deploying ring-fenced security has become an endless task. How can organisations handle ecosystems comprising thousands of public bodies, hundreds of thousands of public agents, dozens of millions of enterprises, billions of citizens and dozens of billions of things, interconnected and vaporised into the cloud? Of course, multi-layer perimeter protection, identity and access management federation, end-to-end endpoint and application security will continue to help. But the question continues to be: which are the key assets to secure? Cyber-security in the digital age 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 digitisation:

- Will a digital scenario improve citizen service or weaken trust in public services?
- Will it boost operational excellence or create opportunities for fraud?
- Will it sustain digital advantage for economic growth or threaten data confidentiality?
- Will it have impacts on privacy and therefore on citizen trust, compliance and legal issues?

These questions must always be grounded by a central question: what is the potential value for citizens, enterprises, NGOs and public stakeholders? In a world where complexity grows and yet digital speed of development is essential, it is critical to define fully public service-driven security policies, with service-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 analyse in-depth which are the truly critical risks from a business or public point of view, and to arbitrate on protection measures from these perspectives. While several risk-balancing methods have existed for years, analysts estimate that only 20% of organisations have put in place effective risk management. To succeed, three approaches will be essential:

**1. Make security a core track of the digital strategy, constantly linking security with innovation**

The objective here is for decision-makers to take security into account for digital initiatives, rather than seeing it as an inhibitor. For example, one of Atos' clients, a large central government, has been able to accelerate its digital transformation and meet citizens' security and privacy concerns by integrating security into its innovation strategy and linking service value to security. The result: fully combining service simplification and citizen trust, by securely connecting millions of citizens to its unified public service portal, giving seamless digital access to all public services – and assuring personal data privacy.

**2. Take all the ecosystems and value chains into account**

As boundaries blur between digital and physical worlds, between public services and stakeholders, between corporations and partners, between suppliers and customers, the trust value chains are rapidly evolving. In the past, organisations have often been accustomed to operating 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 large public service, has measured the security risks across its entire extended ecosystem, to streamline new generation identity and access management for thousands of employees, suppliers, partners. The result: a boost to both security and user experience.

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

The digital revolution puts the citizen back at the centre. Security must not be an exception. It must be designed to protect the most important thing for any organisation: the citizens, stakeholders or customers it serves. 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**

Should everything be protected? The answer may not be a simple yes or no. A third solution exists: cyber-insurance. This is a growing field for large insurance groups – notably to protect their customers from regulation risks and prepare for upcoming European laws on customer data privacy. No-one understands better than insurance companies the importance of risk quantification. 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 Operational Technologies (OT), including technical infrastructures and smart connected objects. Leveraging its industrial expertise, Atos has developed a global methodology to help organisations 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. This kind of approach can be of value to public stakeholders who can ensure their private partners become fully secure, notably in smart cities and healthcare.

## Rule 2: deploy data-centric protection measures

**Data is now a critical asset. Once a side-product of applications, data is fast becoming an enterprise's core 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 a valuable new commodity. It can produce a better understanding of customer behaviour, a better capacity to optimise business processes in real time, and new insights that can be exchanged or sold to create new business models.

Info-centric corporations are already 20% more profitable and achieve twice the market value of their peers. In the same way, Open Data has proved a powerful way for public services to better serve citizens and accelerate economic development.

Yet it's essential that public data is not altered for fraud or political motivations, and that confidential data remains so, for both the public bodies and the citizens. Government and public services are targets for fraudsters, hacktivists and hostile nations. In a digital world where data is at the heart of value, it must also be at the heart of security.

### Innovative trend

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

What should public bodies worry more about: protecting critical data from the insider threat, or protecting it from organised cyber-criminals looking to sell assets 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 Centre and expertise in DLP. It provides a robust risk management service and strongly prevents data theft, whether it be from unauthorised 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 and processes. Gartner estimates that "through 2016, more than 80% of organisations will fail to develop a consolidated data security policy across silos, leading to potential noncompliance, security breaches and financial liabilities". Atos has developed specific methodologies to meet this challenge. For example, we have helped a major government organisation to protect critical data across all Enterprise Resource Planning processes, managing a large part of the country's GDP. The result: strategic business intelligence data available for public decision-makers, 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 behaviour 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**

Public or business data is not inert: 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 research organisation, so that R&D data can now be safely monitored, avoiding losses that could cost billions in Intellectual Property.

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

**The digital world is not only more complex, it is also faster paced. It took 18 years to amass the first 50 million mobile phone users in the 70s and 80s, compared to just three months for Google+ at the beginning of this decade. And still the pace accelerates.**

As a result, foreseeing problems and opportunities is ever more difficult. Security that may have been well planned in the past may not stay immune to new kinds of attack. In a complex world that's evolving in real time, it is essential to re-orient security budgets from generic protection to rapid detection and reaction responses.

Real-time security mechanisms will be needed to constantly monitor, identify suspicious activities, counter-react without delay, and set up immediate remedial actions. This is a new pre-emptive security approach, whose essential operational management importance is highlighted by the rise of next-generation Security Operation Centres and forensic strategies for public organisations.

## 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 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 Centres (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 some of the largest and most sensitive corporations and public organisations in the world, we provide 24x7 protection and instant reactions – as showcased at the last Olympic Games, where hundreds of millions of threats resulted in zero breaches. Atos also helps public bodies and enterprises to benefit from their own private SOC to deploy advanced sovereign security operation centres.

### 2. Deploy forensic teams

Endpoint forensic teams will be increasingly needed to examine and sort vast amounts of digital information to find evidence trails that can be used in courts of law. Associated to SOC, they must combine international and local expertise to handle regional context and regulations. For example, Atos is helping its customers quickly and effectively contain targeted attacks to limit the business or public service impact. Atos CSIRT forensic teams also reverse-engineer attempted breaches 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 responds to crimes once 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 for an international customer an advanced persistent threat detection and remedial solution in order to detect targeted attacks on 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 neutralise such attacks, reducing the business impact to almost zero.

## Innovative trend

**Big Data analytics at the heart of next-generation SOCs**

With billions of logs and millions of users, security has entered the Big Data era with SOCs and SIEM. With the ever-growing level of threat and the increasing complexity of attacks, a new approach is needed for detection. Public services and enterprises will need advanced predictive security and context-aware, actionable security intelligence that exploits the power of next-generation analytics 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 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. This enables pre-emptive protection for most sectors – from national security to financial fraud management and theft management in utilities.

# Building trust, leveraging opportunities

**In everyday life, a pre-requisite for effective collaboration is trust. Can you have faith in the organisation you're dealing with? In the digital world, trust has always been a key concern, but the rise of the Internet of Things gives it a new dimension.**

**When you know that a government may have the right to access all your data and will therefore know everything about you and your life; when you furnish your home with smart public utilities devices whose sensors could be hijacked; when you put your life into the hands of a self-driving subway whose software may be taken over by malware; when your life may rely on connected healthcare such as artificial heart systems – then you require absolute trust.**

In the digital age, just as data is becoming the new currency, trust may well be the most intangible yet critical business asset. For years, rating systems have shown how businesses in the retail or travel sectors depend on reputation. Tomorrow's hyper-connected world will take this concept to a new level, for public bodies and corporations alike.

Security is therefore at a turning point. Not only is it necessary to reduce risk and ensure compliance; but by reducing risks, public organisations can be empowered – to be more trusted, more agile, and take public service to new heights for all stakeholders: citizens, corporations and NGOs.

In a nutshell, beyond protection, security is becoming a new asset. An asset that will:

- **Grow citizen experience** – facilitating secure and seamless access to information and assuring citizen trust in data privacy
- **Boost operational excellence** – ensuring public services are not at risk
- **Support public service reinvention** – by securing innovation and protecting the most precious asset: data.

**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 better serve millions of new citizens – and particularly those from generations Y and Z who are born in the digital age
- Being agile enough to foster the development of ecosystems and Public Private Partnerships on secure APIs
- Being nimble enough to leverage the need for new service models in the new economy of data.

Europe's initiative to boost growth by contributing €415 billion per year to the European economy and create 3.8 million jobs through its 'Single Digital Market' initiative – including strong cyber-security measures to reinforce trust – is a striking example of this huge potential.

*This is a strategic move for cyber-security – a revolution that will put security at the heart of business.*

# Security: think globally, act vertically

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

**Balancing access to critical systems, networks and data with security, control and management is an ongoing challenge. And as security threats constantly evolve, this balancing act continues. Digital security is a global issue.**

While the solutions that many public bodies and corporations adopt are similar – security policy management, identity and access management, communication security, Security Operations Centres – the level of protection and specific business risks vary significantly between organisations and industry sectors.

Government is experiencing a particular step change (with process digitisation and open data) and is a critical foundation for defence and national security, justice and private sector organisations that are administered and regulated by the public sector. With the public sector a key target for cyber-terrorism, security issues need to be considered within the context of a global trust and compliance framework, encompassing domains such as risk management, transaction security, fraud prevention, critical systems design, compliance and regulatory reporting.

**Finance** is particularly exposed to threat and is a target for cyber-crime. Disgruntled traders and fraudsters have also demonstrated how they can manipulate finance centres. These events have resulted in security measures that go far beyond the IT department. They have also generated major business challenges and triggered in-depth reviews of compliance and regulation both locally and globally. Industry analysts estimate that 50% of banks' IT budgets may be impacted by regulations such as the Anti-Money Laundering Act, Foreign Account Tax Compliance Act, Dodd–Frank, stress tests and Basel II. The rise of new cryptocurrency technologies may also introduce major disruptive challenges in the near future.

**Media & Telecom**s are an obvious target for cyber-crime because of their high profile, 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 cyber-crime and misuse. Operational technologies are particularly important targets. When it comes to cyber-war, Utilities is recognised 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 transport the next strategic targets for cyber-crime, requiring highly specific protection measures, notably in IoT, machine learning, artificial intelligence and robotic security.

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

As a result, public service security needs an holistic approach, where the security of public bodies is essential, but where public organisations also take into account the whole security chains of their environment and of their private partners or stakeholders. The security challenge of smart cities, where public bodies, transport, utilities, telco, healthcare, etc. must provide services in synergy, is a perfect example of this trend.

# Conclusion

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

- Public service-driven selective risk management
- Data-centric protection strategies
- Increased investments in pre-emptive security and forensics
- Service-minded security to prepare for the unexpected.

## Atos cyber-security: a new breed of partner

To succeed, public bodies 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 Security Operations Centres (SOCs) 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 4,500 security specialists worldwide and eight 24x7 SOCs 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 public to health, from manufacturing, retail and transport to finance, from telco and media to utilities.

Atos' expertise builds on more than 25 years of experience in providing robust, comprehensive and fit-for-purpose security solutions and services for the most demanding organisations. It also builds on the acquisition of Bull in 2014, a recognised player in defence and Big Data, with advanced solutions in identity and access management, security analytics, encryption, and critical systems for defence and aerospace. As a result, Atos 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 defence, nuclear and aeronautics. Each day, millions of lives are protected by Atos critical defence systems, 13 million transactions are handled by Worldline, 100 million identities are securely managed with Atos IAM technologies, and two billion security events are analysed 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 organisations 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 your current 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.



Atos, the Atos logo, Atos Consulting, Atos Worldline, Atos Sphere, Atos Cloud and Atos Worldgrid are registered trademarks of Atos SE.
September 2015 © 2015 Atos.