Solution brief

Prescriptive Security for Financial Services

Trusted partner for your **Digital Journey**

Atos

Contents

To stay ahead of the increasing volume, complexity and disruption of cyber threats in the Financial Services sector, Atos Prescriptive Security continually learns, detects and orchestrates automated security actions which neutralise cyber threats before they strike.

By prescribing actions which prevent cyber attacks from happening, your security performance improves and the organization avoids recovery costs, reputational damage and abnormal customer losses.

Atos and Prescriptive Security

"The potential of artificial intelligence to transform business performance is only now starting to be more widely understood in Financial Services. This is nowhere clearer than in the security domain, where the fusion of big data, advanced analytics and machine learning holds out the promise of startling improvements in cyber defenses through the introduction of Prescriptive Security.

Moving beyond predictive security into the world of prescriptive security is an exciting development that none can afford to miss. We look forward to talking with you on this critical topic."

Mark Ingleby,
Group SVP, Global Financial Services
and Insurance, Atos

"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 both to understand and predict the threat landscape and to prescribe actions to neutralize them before they materialize. 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, so I urge you all to take the opportunity to improve your organization's security performance in this way and look forward to your feedback."

Pierre Barnabe,
Executive Vice President,
Head of Big Data and Cybersecurity, Atos

Business Context

The reputation of any financial services organization rests squarely on trust, security and professional integrity. Breaches of any of these profoundly damages the belief of markets, investors and customers in the others.

Every financial services organization is engaged at some level on modernizing itself to remain fit for its twentieth first century purpose. At the heart of this endeavor is the pervasive switch to digital technologies in every part of the organization, so creating a fundamentally new dependency on digital systems and processes. With this new enterprise-wide dependency comes new risk, as well as new opportunity.

The risks have long been recognized and reflected in modernized business and technical controls, better integrated governance, risk and compliance management and, critically, in Board-level oversight of the organization's performance in containing and mitigating them.

Despite these responses, some complicating factors have emerged to challenge the sector's overall management of pervasive digital risk.

1. New technologies are maturing and converging at a much faster rate and are being delivered through many different channels, particularly third-party Cloud services and mobile devices.

2. The level of scrutiny from industry regulators has been overlaid by that of governmental bodies, probing for the reasons why digital risks turn too frequently into digital issues, seen in high profile service outages, system upgrade failures, data corruption and customer losses.

3. The demands placed on the organization to exploit them have increased steeply, as business leaders demand investment to become more competitive, creating both the emergence of 'business-led IT' and greater pressure on IT to bring new technologies rapidly into the organization.

4. The technical operating environment has become less predictable through the efforts of malign actors, from state-sponsored programs to individual cyber hackers, both of which work tirelessly to disrupt the smooth working of public and private sector organizations for personal gain, political advantage or both.

The results of these complicating factors are all too well known; large scale cyber theft enabled by stolen bank account details; cyber-related card fraud, using stolen credit card details to perpetrate Card Not Present fraud; online customer applications and services taken out of service for prolonged periods, creating ill-will, financial disruption to business and personal customers and unwanted attention from regulators and government.

No financial services organization chooses to leave itself vulnerable to digital risk. Every forward-looking financial services organization strives to operate as securely as it can, to safeguard its reputation, delight its customers and so improve its standing with investors, regulators and wider publics. This is not just enlightened selfinterest. It is a clear recognition that high performance in security, without exaggeration, is the lifeblood on which the long-term prosperity of the sector now depends.

The sector is under attack

Financial Services has proved consistently to be the most cyber attacked sector of many developed and developing economies, for the simple reason that banks hold vast stores of wealth on behalf of their customers, markets organizations trade billions of securities every day and insurance companies hold huge reserves both to service claims and invest to generate capital returns.

Whilst the specifics of data security performance may vary, the key trends for Financial Services are sobering.

1 Data breach recovery costs are going up

The financial services sector globally stands to lose an estimated $701m at risk from cybercrime-derived losses in the period 2019-23 alone; more than Utilities, Energy or Defense; more than Healthcare, Industrial Equipment or Retail[1].

The direct cost per financial services record lost is increasing, standing at $245, up 23% on its four-year average. The indirect costs of cyber-derived losses are generally at least as great as the direct costs of technical and business remediation[2], in major Western economies spread between c. 120% and 180%.

2 Customer losses are abnormally high

Abnormal customer attrition following a data breach is higher in financial services globally than any other sector of the economy, averaging 7.5%, exceeding even Healthcare, Services and Technology companies. Associated lost business costs (increased customer recruitment costs, reputational damage and diminished goodwill) typically cost between $1m and $4m per organization in major economies.

3 Time to identify breaches remains stubbornly high

It takes on average between 160 and 214 days globally for an organization to identify a data breach. Malicious or criminal attacks taking the longest and human error the shortest time[3].

It costs more to recover from long-unidentified breaches.

Recovery costs increase the longer the breach lies undetected, adding 38% on average to total recovery costs[3].

4 Malicious or criminal attack most common cause

Data breaches from malicious or criminal attacks are consistently the most common cause of data breaches in major economies, exceeding either system faults or human error and responsible for between 45 – 60% of total breaches[3].

5 Malicious or criminal attack is most costly

Data breaches from malicious or criminal attacks are consistently between 15% to 25% more costly to correct than breaches arising from system faults or human error[3].

6 Bigger breaches mean higher costs

The direct and indirect costs of correcting a data breach accelerate in line with the size of the breach, expressed in the number of thousands of lost records. Data breaches of more than 50,000 records cost on average $6.3m to correct[3].

The message for Financial Services is clear

Improvement in the identification and remediation of data breaches is a commercial imperative for the Financial Services sector, both when united as a sector in cross-industry information-sharing and as individual institutions defending their own businesses and reputations.

Technologies which improve an organization's ability to spot and neutralize threats to its systems and their data will:

- drive down the number of breaches suffered,
- prevent cyber theft and fraud losses,
- avoid the direct costs of escalation, notification and response,
- remove the costs and threat of customer attrition,
- avoid collateral damage to business reputation,
- avoid adverse sentiment from investors,
- avoid unwanted attention and censure from the media,
- maintain its standing with regulators and government.

Human capital business controls and processes which improve an organization's ability to hire, train, retain and instill professional integrity in its employees and third-party contractors are also critically important, both to cut the incidence of human error and the possibility of malign action from a disaffected employee or contractor.
Achieving the shift from an organization which reacts to incidents, to one which prevents them occurring lies at the heart of each of these imperatives.

Bringing artificial intelligence to bear on security performance

The key attributes of technologies most able to improve an organization's security performance from reaction to prevention are augmented intelligence and, as a result, prescription.

Augmented Intelligence, created by combining artificially intelligent tools and techniques, enables more data sources in widely differing formats to be ingested and applied through machine learning to identify and expose otherwise hidden relationships in data sets.

The nature of these relationships, once identified, is tested and refined through the operation of supervised and unsupervised learning models, enabling expert cybersecurity specialists to receive, interpret and act more quickly to neutralize threats to data security than would have been possible without the augmented intelligence.

Prescription, the semi- or completely autonomous machine decision to act to neutralize a threat immediately, or subject to further controls, is a step which can therefore follow the receipt of newly identified threats to data with the degree of freedom to act granted to the machine remaining firmly under the control and management of the organization.

These two attributes are encapsulated in the term **Prescriptive Security**.

1. Securing the digital economy: reinventing the internet for trust - Accenture
2. The true cost of a data breach - Interconnection. http://interconnection.org/pdf/The_True_Cost_of_a_Data_Breach-with_images.pdf
3. 2017 Cost of Data Breach Study: Global Overview– Ponemon Institute LLC

Prescriptive Security defined

Prescriptive Security is a state towards which forward-looking financial services organizations will work to achieve a step-change in data security performance.

To the familiar attributes of Security Incident and Event Management (SIEM) services - firewalls, malware protection, mail and web gateways, logs, audits, events and alerts – Prescriptive Security adds four new, broad dimensions:

- Enhanced analytics,
- Artificial intelligence,
- Enhanced threat intelligence,
- Security orchestration, automation, and response.

Enhanced Analytics combines the ability to ingest and analyze multiple massive and heterogenous data sets on an Advanced Analytics Platform, including the analysis of user behaviors to identify and distinguish genuinely threatening attributes from apparently threatening, but innocent attributes.

Artificial Intelligence directs computing power to mimic human intelligence to carry out deductive and interpretive tasks through a range of technologies and techniques including machine learning, which uses algorithms to analyze and draw deeper inferences from data to enable it make a decision or prediction about something.

Machine learning includes Deep Learning which uses neural networks and very large data sets to train the system progressively to improve the accuracy and utility of its results.

Enhanced threat intelligence extends and integrates the range of internal and external sources of threat information including semi- and unstructured data sets. Enabled both by artificial intelligence and advanced analytics, enhanced threat intelligence is made available to the network of security systems either as a starting point for a machine-led investigation or as corroborative data during one.

These services are coordinated and directed by a **Security Orchestration, Automation and Response** platform, a single, comprehensive incident response engine which can deliver major - and accelerating - improvements to security performance over time.

Prescriptive Security architecture

A functional view of the components which can be coordinated to enable prescriptive security is given in the figure below, the Security Operations Analytics Platform Architecture ('SOAPA').

SOAPA[4] replaces the commonly encountered security operations practice of setting up and managing a set of independent and fragmented security tools with a tightly-integrated security stack, comprising:

- Common data services which ingest, process and make available terabytes of data daily for analysis
- Software services which deliver data elements to the right engines in correct formats
- Analytics layer in which data analytics delivers insight from the range of data inputs including threat intelligence, events and alerts and behavioral analytics
- Security operations layer in which, once insight has been delivered, operational actions are initiated, whether quarantining a system, modifying a security control, or installing a software patch

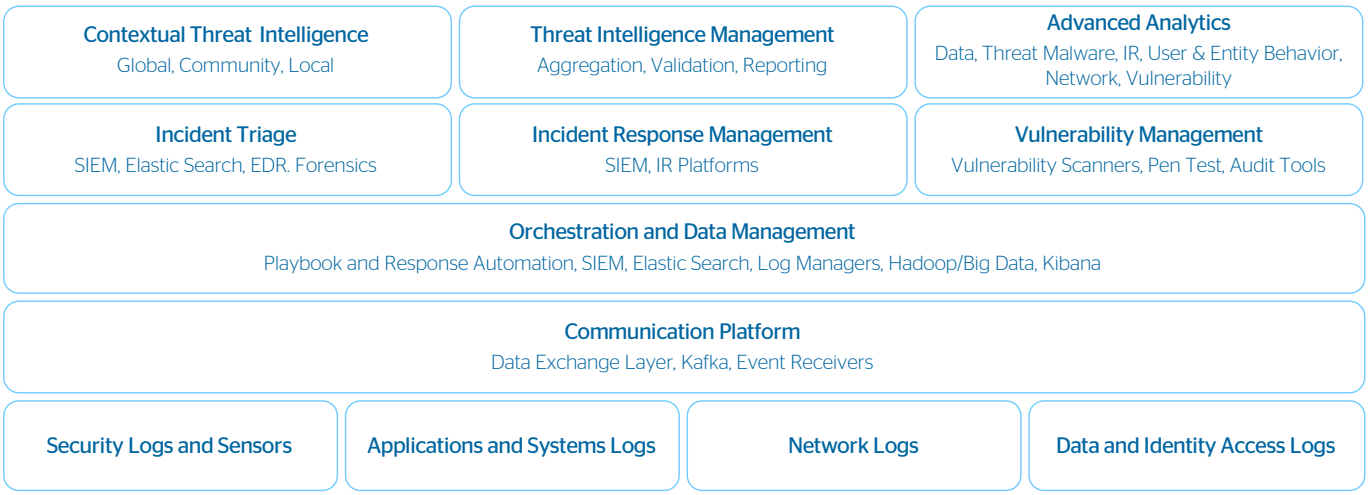

Figure 1: Security Operations Analytics Platform Architecture

SOAPA[5] incorporates and surrounds SIEM functionality, bringing together a wider set of security data from new sources and uses a different set of technologies to unify them on a single platform, delivering machine-readable data capable of being ingested, analyzed and acted on. This streamlines processes and makes security operations more efficient.

It is designed to be a dynamic model, allowing new data sources and tools to be added as well enabling data scientists to work rapidly between different tools and data sources to take action in real time.

4. Security Operations Activities to Watch in 2019, Jon Oltsik, ESG
https://www.esg-global.com/blog/security-operations-activities-to-watch-in-2019
5. What is Security Operations and Analytics Platform? Digital Guardian
https://digitalguardian.com/blog/what-security-operations-and-analytics-platform-architecture-definition-soapa-how-it-works

Moving your organization towards Prescriptive Security

Each Financial Services organization has its own existing security footprint and delivery arrangements. Accordingly, the steps to be taken to realize a fully prescriptive security capability will vary widely.

Recognizing this, Atos provides a spectrum of assistance, from technical consulting, through individual project, major programme to partially- or fully managed services. Our goal is to work with you to develop, from a careful consideration of technical, logistical and commercial options, the right road map which delivers the objective which you define.

To illustrate, figure 3 suggests a number of progressive steps towards prescriptive security, for an organization which has decided to reap the fullest rewards from its investment.

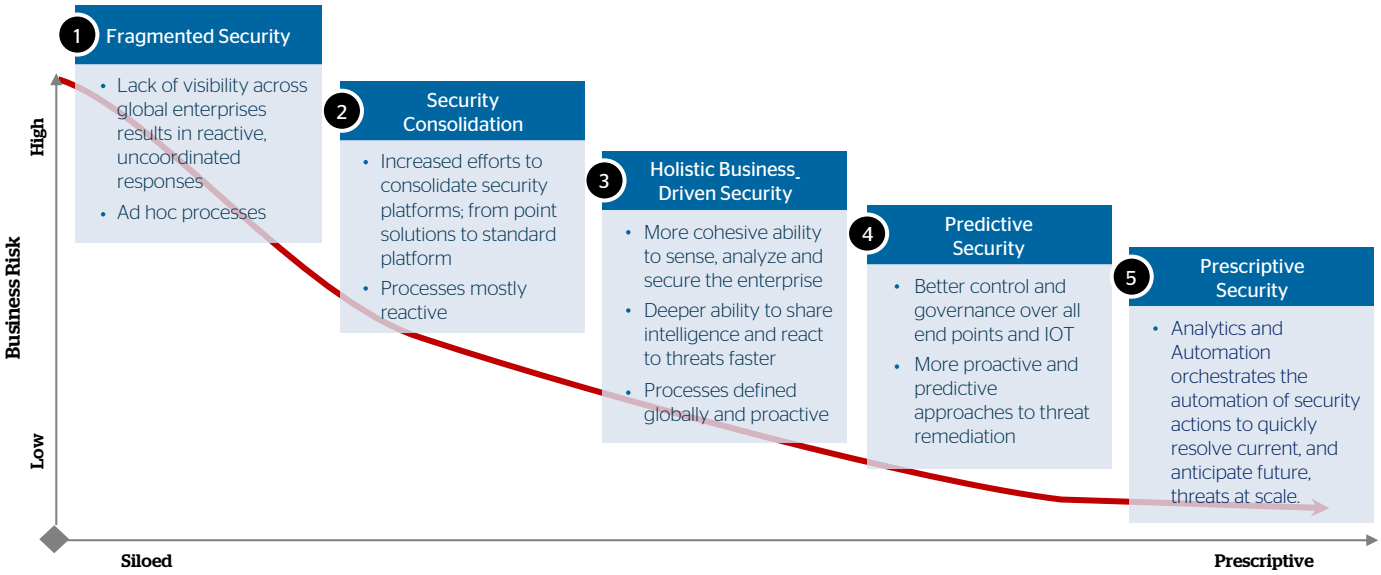

Figure 2: Functional steps on the path to progressively realizing the highest level of Prescriptive Security

Prescriptive Security delivered through an Operations Centre is a complex undertaking that is designed as a packaged offering. The offering has a Mandatory Core set of modules which deliver all the standard services that you will require, and Optional modules to further advance your security performance and to adapt to the demands of a dynamic security environment.

Although the Prescriptive Security Operations Centre offering will often be chosen as a fully managed service delivered through one or more of Atos's global Security Operations Centres, it may equally be consumed in stages and in hybrid deployment arrangements.

The architecture has been designed to embrace such other deployment offerings where they may be needed. In practice, the way we work this out with you is through a combination of professional services:

- **Cybersecurity consulting** where we will safeguard data, privacy, and security through Risk Assessment and gap analysis. Additionally, our consultants will help improve your cybersecurity roadmap through the Atos Prescriptive Security Operations Centre cybersecurity improvement programme.
- **Cybersecurity projects** where Atos will assist you to build your own, or integrate a partner's, prescriptive security component. These could include security analytics solutions which would include the co-development of big data analytics use cases; consulting and designing the role the solution will play in the prescriptive security architecture; and designing and implementing the required security processes.
- **Cybersecurity services** where we provide a Prescriptive Security Operations Centre to deliver, manage and maintain security services for your organization's IT.

Atos and Prescriptive Security

Atos has developed a comprehensive Prescriptive Security architecture which matches the need of Financial Services organizations in the front line of the fight against security breaches, irrespective of:

- the size and complexity of their enterprise-wide Information Technology estate,
- the existing security technology footprint,
- whether security services are managed wholly in-house, wholly by third parties or in a hybrid arrangement.

The key service components set out in Figure 3 show the architecture in the form of Atos's Prescriptive Security Operations Centre in which Atos would set up, deliver and manage prescriptive security services.

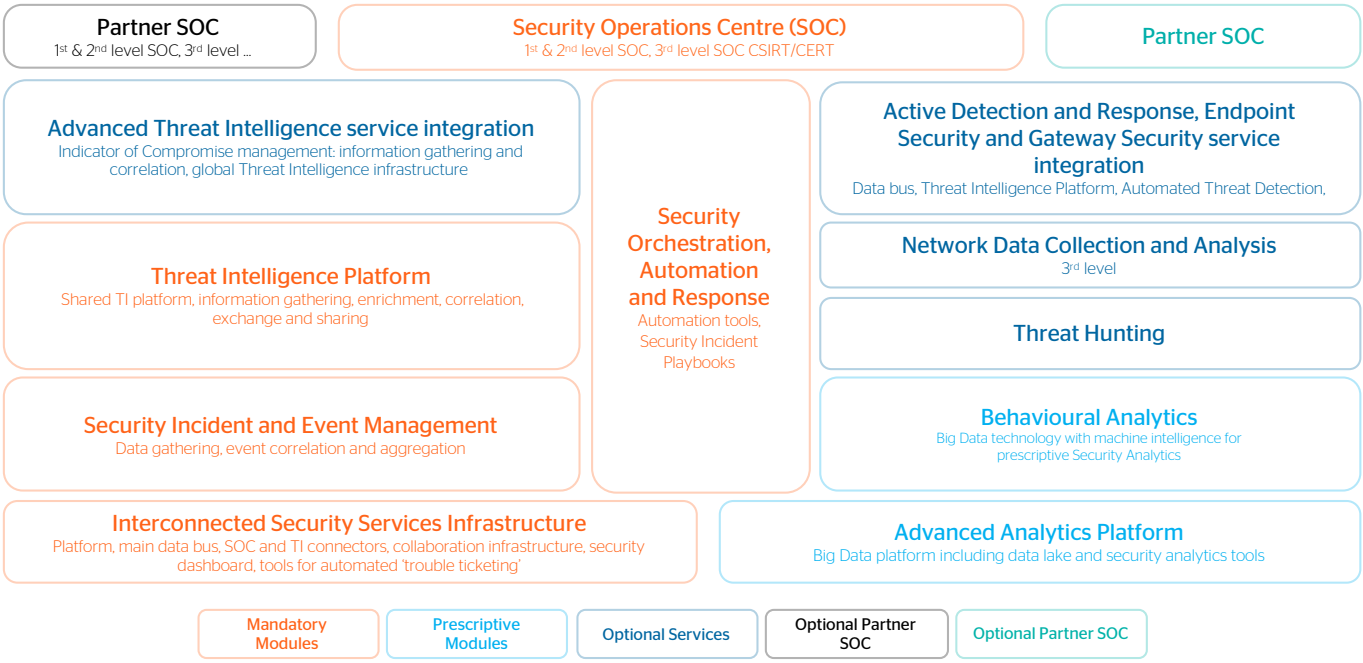

Figure 3: Key Service Components of the Atos Prescriptive Service Operations Centre

Integrated, intelligent services for improved security performance

The Atos Prescriptive Security Operations Centre provides financial services organizations, with its Interconnected Security Services Infrastructure, the basic infrastructure and tooling including its interfaces and processes required to operate the services.

Centrally, the Prescriptive Security Operations Centre includes a Security Orchestration, Automation and Response module (SOAR) which enables more rapid, comprehensive and accurate analysis to be undertaken.

This module can also interconnect the networks, technologies and processes of different Security Operations Centres into one virtual operational unit, enabling collaboration on cybersecurity issues across all technology areas.

Whilst basic security analytics based on static correlation rules may be performed in the Security Incident and Event Management module (SIEM), the Advanced Analytics Platform enables deeper, wider insight on the organization's security situation with Big Data storage holding high volumes of many data types for security analysis purposes. Big Data storage is deployed on a dedicated virtualization platform to create the maximum flexibility for future growth in data volumes.

Artificial intelligence and machine learning technologies, models and methods are applied to massive data sets held in a data lake, very significantly enhancing the quality, speed and business value of security analytics delivered and allowing for the handling of rapidly increasing data volumes from many heterogeneous sources, devices and technologies.

A detailed description of the Mandatory and Optional services available within the Atos Prescriptive Security architecture is given in the Atos publication *Prescriptive Security for Financial Services – Technical Brief.* This publication also discusses:

- the most common types of cyber attack experienced by the Financial Services sector,
- a range of prescriptive security use cases,
- the operation and benefits of proactive threat hunting.

A global Cybersecurity leader

Our Capability

Atos is number one cybersecurity provider in Europe and a global leader in cybersecurity services.

With a global team of over 5,000 security specialists and a worldwide network of Security Operations Centres, Atos offers end-to-end security partnership. We integrate the best security technologies and offer a full portfolio of security solutions, helping you turn risk into business value.

Atos has designed the Prescriptive Security architecture discussed in this Solution Brief and much of the software in that architecture is designed and built by companies in the Atos family including Codex for advanced analytics and Bull hardware for high performance computing.

During this process Atos has worked closely with Siemens under the Atos-Siemens Alliance on some of the fundamental thinking on the technical architecture.

Our Clients

Atos provides cybersecurity services to many large Financial Services organizations including:

Our Partners

Atos has chosen a wide range of software partners for key components and services, which include carefully selected global software brands such as: McAfee, Symantec, Palo Alto, Juniper with, in addition, a range of specialist cybersecurity services providers such as EDR, Crowdstrike, Active Response and Darktrace, for, as examples, advanced security analytics.

Analyst Recognition

Atos has been recognized by global analysts as leaders in key areas of cybersecurity.

Leader

- Managed Security Services Europe
- Managed Security Services WW & EMEA GDPR Services WW
- Identity Provisioning Global
- IT Security Europe

Niche Player

- Identity Governance & Admin WW
- Access Management WW

3rd

- Managed Security Services WW Marketshare

Your next move, our invitation

To find out more, contact us for a discussion at https://atos.net/en/solutions/cyber-security.
To read our latest thought leadership on prescriptive security, go to https://atos.net/wp-content/uploads/2017/10/atos-psoc-op-en.pdf

Sources
1. Securing the digital economy: reinventing the internet for trust - Accenture
2. The true cost of a data breach - Interconnection. http://interconnection.org/pdf/The_True_Cost_of_a_Data_Breach-with_images.pdf
3. 2017 Cost of Data Breach Study: Global Overview– Ponemon Institute LLC
4. Security Operations Activities to Watch in 2019, Jon Oltsik, ESG
https://www.esg-global.com/blog/security-operations-activities-to-watch-in-2019
5. What is Security Operations and Analytics Platform? Digital Guardian
https://digitalguardian.com/blog/what-security-operations-and-analytics-platform-architecture-definition-soapa-how-it-works

About Atos

Atos is a global leader in digital transformation with over 110,000 employees in 73 countries and annual revenue of over € 11 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. The group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information technology space. Its expertise and services support the development of knowledge, education as well as multicultural and pluralistic approaches to research that contribute to scientific and technological excellence. Across the world, the group enables its customers, employees and collaborators, and members of societies at large to live, work and develop sustainably and confidently in the information technology space..

Find out more about us
Atos.net/Banking
Atos.net/Insurance

Let's start a discussion together

CT_J2545_190321_RY_WP_PRESCRIPTI