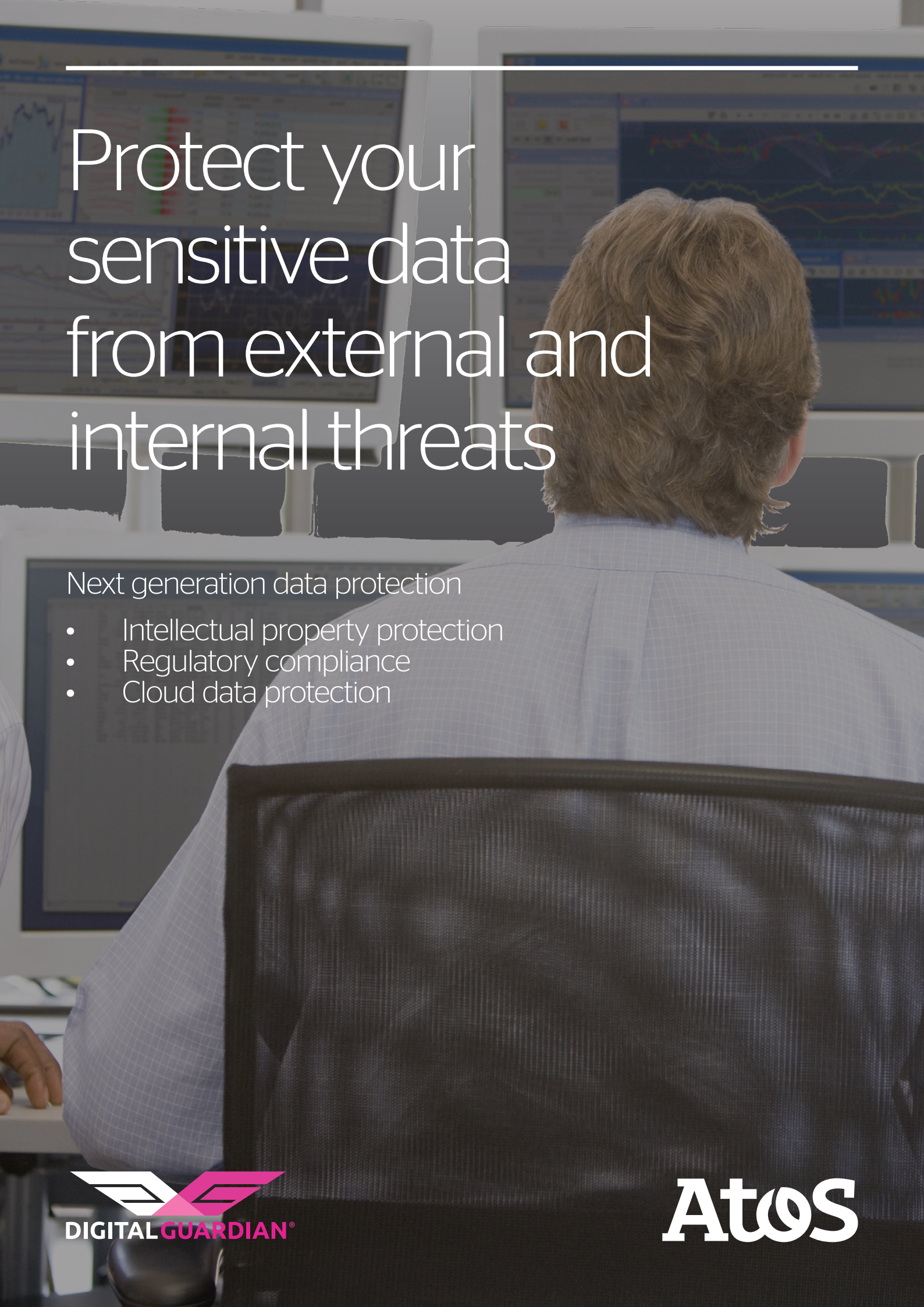


Protect your sensitive data from external and internal threats

Next generation data protection

- Intellectual property protection
- Regulatory compliance
- Cloud data protection

DIGITAL GUARDIAN®

Atos

Guarding critical information

The modern business ecosystem is built around a model of open collaboration and trust –the very attributes being exploited by an increasing number of global adversaries. Constant information flow is the lifeblood of the business ecosystem. Data is distributed and disbursed throughout the ecosystem, expanding the domain requiring protection. Adversaries are actively targeting critical data assets throughout the ecosystem – significantly increasing the exposure and impact to businesses.

A wide range of adversaries	..Who are highly motivated	..Who are highly motivated	... Creating unprecedented risks for your organization
Nation State	• Economic, political, and/ or military advantage	• Trade secrets Business • Information Emerging • Technologies critical • Infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure
Organised crimes	• Immediate financial gain Collect information for future financial gains	• Financial / Payment Systems PII, PCI, PHI	• Regulatory inquiries and penalties Lawsuits Financial loss Loss of confidence
Hackivist	• Influence political and /or social change Pressure business to change their practices	• Corporate secrets Business information Information of key executives, employees PII, PCI, PHI	• Disruption of business activities Damage to brand and reputation Loss of consumer con˜idence
Insiders	• Personal advantage, monetary gain Professional revenge Patriotism	• Sales, figures, market strategies Corporate secrets, IP, R&D Business operations Personnel information	• Trade secret disclosure Operational disruption Brand and reputation National security impact

We protect

629%

rise in cryptojacking in Q1 2018.

1. source: businessinsider

https://www.businessinsider.com/cryptojacking-exploded-this-year-heres-whow-it-may-be-affecting-you-2018-6

37%

of malware hashes are seen once, and never again

2. source: 2018 Data Breach Investigations Report, Verizon

44%

of malware contained ransomware

3. source: 2018 Data Breach Investigations Report, Verizon

It may take days or even months for defenders to discover threats

197

days on average to discover a data breach

4. source: Ponemon Institut

69

days on average to contain the breach, post discovery

5. source: Ponemon Institut

Compliance and IP are at risk across a wide range of industries

Personally Identifiable Information (PII)
Personal Credit Card Information (PCI)
Protected Health Information (PHI)

Compliance data at risk

Intellectual property at risk

Product design plans (CAD)
Software (source code)
Trade secrets
Formules & algorithms

Financial Services

Personally Identifiable Information (PII)
Personal Credit Card Information (PCI)
IP (Trading Algorithms, Business Processes, Financials, IPO Plans, M&A Plans, Business Plans, Pricing)

Manufacturing

IP (Product Designs, Formulas, Trade Secrets, Pricing, R&D Data, Business Processes)

Public Sector

Protected Health Information (PHI)
Personally Identifiable Information (PII)
Personal Credit Card Information (PCI)
Confidential email
State Secrets

Healthcare

Protected Health Information (PHI)
Personally Identifiable Information (PII)
Personal Credit Card Information (PCI)

Media and Telecom

Personally Identifiable Information (PII)
Personal Credit Card Information (PCI)
IP (Source Code, Business Plant)

Utilities

Personally Identifiable Information (PII)
Personal Credit Card Information (PCI)
IP (Exploration and Production plan)

Our approach

DLP assessment & advisory → **Visibility Study** → **On-premise DLP integration** → **DLP as a service**

Understand the maturity of your data & information protection strategy, processes and technology	Determine what is really going on with your data and information assets	Avoid data leakage and misuse of information assets	Reduce CAPEX and rapidly defend data and information assets

Stage 1:

DLP Assessment & Visibility Study

Our specialist consultants help you to determine the level of maturity of your current data and information protection strategy, processes and technology, in relation to the data most important to your industry. We recommend undergoing the DLP Assessment in conjunction with the Visibility Study, during which we will help you to outline a strategy to protect your data and sensitive information assets suff iciently.

The Atos Visibility Study is designed to provide actionable intelligence on policy compliance, privileged user and insider activity, as well as potential targeted cyber-attacks. On a selected group of up to 100 users, we will show you over a period of four to six weeks what is really going on with your data and sensitive information assets. The Visibility Study is non-intrusive and provides you with in-depth insights of the maturity level of data protection at your environment.

Our data protection experts will help you review the reports, identify risks, and advise actionable steps to help manage potential threats throughout the engagement.

Stage 2:

On-premise DLP Integration

If weaknesses have been identified in your current data protection strategy, processes and technology, we will help you to evolve. Together with our Gartner Magic Quadrant Leader technology partner, Digital Guardian, we will provide you with a future-proven solution with a host of unique differentiators:

- Automatic data classification (context and content based)
- Complete visibility on endpoints of system and user behavior without pre-defined policies
- Fast and accurate rule tuning based on broad visibility
- Stealth mode, Tamper resistant
- Broadest controls to stop data egress/ ingress and data sprawl
- Ability to correlate multiple events on endpoint in real time
- Full platform coverage(Windows, Mac, Linux, Cloud).

Stage 3:

DLP as a Service

DLP is a solution that helps you control your most valuable assets.

But it needs to be well secured. Atos can run the entire infrastructure platform and application in a highly-secured cloud environment - globally shared for lowest cost - or locally based for compliance with local regulations.

This gives you:

- actionable steps to help manage potential threats throughout the engagement.
- Reduced Capital expenditure
- Increased Flexibility
- Integrated Security Management
  Rapid time to value
  24/7 Cyber Threat Management
- On demand access to thousands of security experts.

Don't Just Detect. Fix.

Today's security threats require a holistic view and an integrated remediation approach. Standalone security products and non-integrated delivery teams are unlikely to provide the best security posture, resulting in a possibly catastrophic lag between detection and remediation.

The Atos advantage is that we provide an integrated approach that off ers an ideal combination of both detection and response. Our three-tiered approach, as shown below, combines security operations, incident and event monitoring, and remediation into one complete cyber security service.

Security Operation Center

Security Incident and Event Monitoring

- Integrated security management
- Spans entire infrastructure

CSIRT

Incident Response Management

- Handling of high priority incidents
- Analysis and resolution

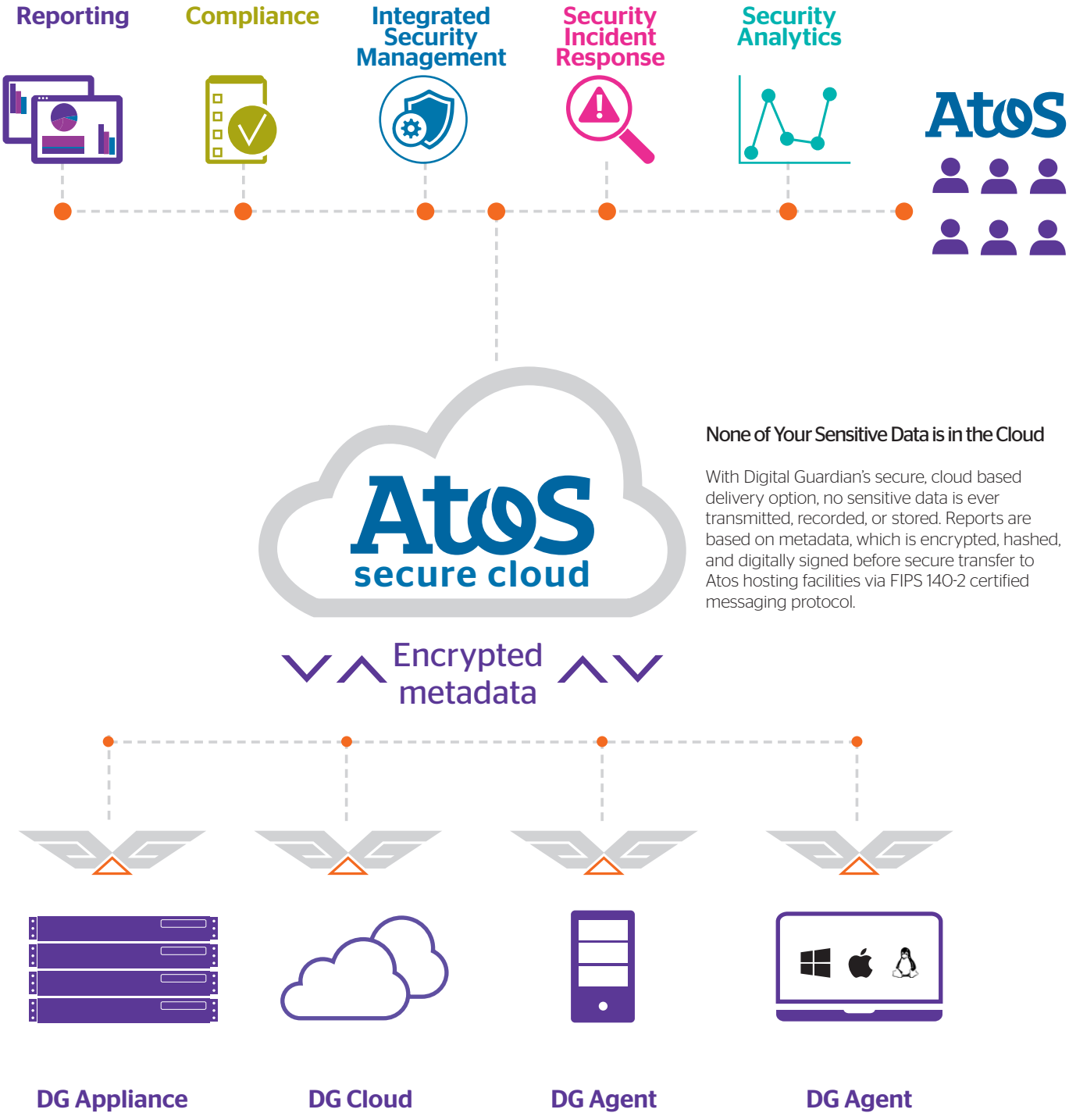
Security Management Service

DLP/EDR/IAM

- Data Loss Prevention Services
- Endpoint Detection & Response
- Identity and Access Management

The Atos and Digital Guardian partnership

This partnership brings together the best of two leading security organizations: Atos – a Global leader in Security Services and Digital Guardian's Gartner Magic Quadrant leader data protection software.



None of Your Sensitive Data is in the Cloud

With Digital Guardian's secure, cloud based delivery option, no sensitive data is ever transmitted, recorded, or stored. Reports are based on metadata, which is encrypted, hashed, and digitally signed before secure transfer to Atos hosting facilities via FIPS 140-2 certified messaging protocol.

Compliance requires transparency. Protection requires control. Atos' Data & Information Protection offers both.

Your company will immediately get the right level of confidence by knowing where your sensitive data resides, who accesses it, and how it is used. Whether you are focused on protecting Personal Information, Intellectual Property or both, Atos has the right solution.

- Atos covers protection of sensitive information end-to-end, from Consulting & Advisory to Systems Integration and Cloud based DLP services.
- Atos' Data & Information Protection Service provides the only true European Cloud Information Protection service.
- Protection for your full environment, including Windows, OS X and Linux endpoints.
- It is the only service that offers both Data Loss Prevention and Endpoint Detection and Response simultaneously from a single agent.
- Atos' Data & Information Protection can permit, advise or block end-user activity depending upon policy. This happens right on the endpoint (the point of risk) – so no complex integration with network devices is required.
- Fastest time to value of any data protection solution because of our Automatic Data Classification and SaaS infrastructure.
- Deployment is easy and options are very flexible—including Saas.
- Only data protection solution that scales to 350,000 users with one management console.
- Integrated security management across your enterprise, with a consolidated view of your security posture.
- Improved flexibility, rapidly adapt to changes in policies and compliance demands.

$500

billion dollars,
theft of trade secrets and intellectual property

source: study commissioned by Bromium

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue over € 12 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/career

Let's start a discussion together

About Digital Guardian

Digital Guardian provides the industry's only data protection platform that is purpose-built to stop data theft from both insiders and external adversaries. The Digital Guardian Data Protection Platform performs across the corporate network, traditional endpoints, and cloud applications. It's buttressed by the DG Cloud, a big data security analytics backend that sees and blocks all threats to sensitive information. For more than 15 years, it has enabled data-rich organizations to protect their most valuable assets with a choice of on premises, SaaS or managed service deployment.

Digital Guardian's unique data awareness, combined with threat detection and response, enables organizations to protect data without slowing the pace of their business.

Find out more about us
digitalguardian.com

For more information: **marketing@atos.net**

CT_190322_LPM_Digital-Guardian_Protect_your sensitive_data_BR_en2