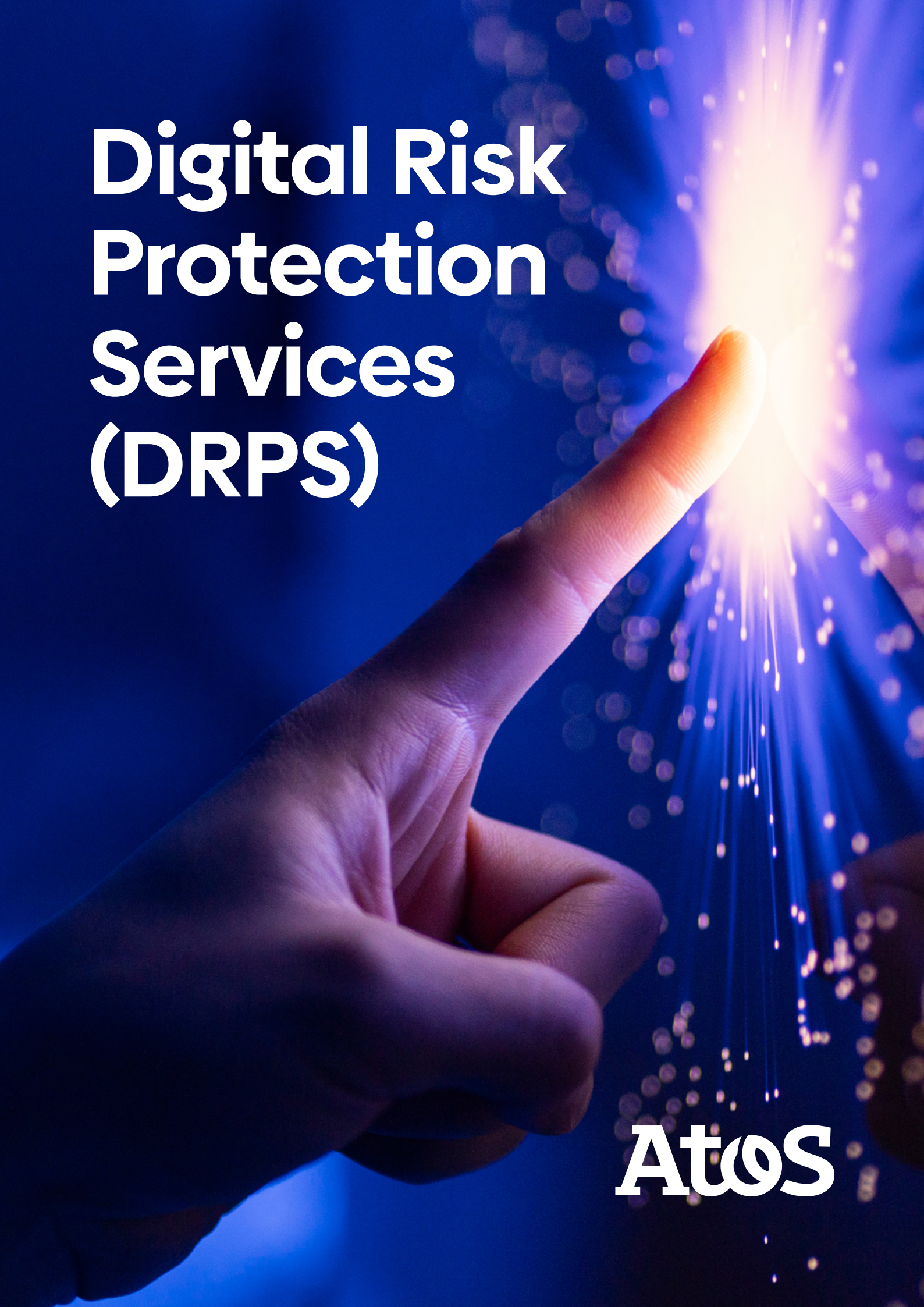
Digital Risk Protection Services (DRPS)



Atos

As cybercrime becomes more advanced, businesses will need cutting-edge Digital risk protection(DRP) to stay ahead of evolving digital and social engineering threats. Stringent data privacy regulations will drive the demand for robust DRP solutions to meet compliance requirements which will further fuel the need for DRP solutions as businesses seek to protect themselves from emerging cyber risks.

Scaling up a business comes with digital risks

For companies undergoing digital transformation or any technological upgrade, their threat landscape also evolves with a digital risk increasing exponentially. Atos DRPS services ensures that upcoming digital risks are proactively identified and neutralized in near real-time.

DRPS services are empowered by vast amounts of data across multiple digital channels to identify any upcoming threat. Without a comprehensive Digital risk protection strategy and a trusted security partner, companies can face:

- Brand abuse: Brand being used illegally or without authorization for malicious practices.
- Data breaches: Leaked credentials and sensitive information
- Phishing attacks: Fraudulent websites and emails targeting your organization designed to steal information.
- Social media impersonation: Fake accounts on social media channels involved in malicious activities aimed at damaging your brand image

What is Atos DRPS

End-to-end security across all digital channels needs a comprehensive approach to ensure fullproof protection from cyber threats. Atos follows a four-step framework which helps to identify threats at an early stage, analyze the threat type and severity, mitigate risk to avoid any damage and finally report the incident with detailed insights to safeguard the company from future digital risks. Below is a snapshot of the process flow:

Identify

We continuously monitor the digital landscape, including the surface web, deep web, dark web, and social media, to identify potential threats to your brand, data, and reputation.

Analyze

Our expert analysts leverage advanced technologies like AI and machine learning to assess the severity and credibility of identified threats.

Mitigate

We take swift action to mitigate threats, including takedown requests, social media monitoring, and proactive measures to prevent data leakage.

Report

We provide you with detailed reports and insights on identified threats, our mitigation efforts, and recommendations for strengthening your security posture.

Potential Digital risks and Atos DRPS solutions:

Potential digital risks	Atos solutions	Service features
Domains mimicking your brand: Mimicking domains resemble your legitimate domains to conduct phishing, fraud, or impersonation, causing financial and reputational harm.	**Brand monitoring**	Our service detects mimicking domains early, protecting your brand, reducing phishing and fraud risks, and safeguarding customers. It minimizes financial losses, ensures continuity, and strengthens trust, demonstrating a commitment to cybersecurity.
Brand mention on dark web: Mentions of your brand on the dark web indicate potential exposure to malicious activities, such as the sale of stolen data, planning of attacks, or fraudulent schemes targeting your organization.	**Brand monitoring**	Proactive dark web monitoring helps to detect threats early, protecting data, brand, and reducing financial risk, while strengthening security and stakeholder confidence.
Phishing domain: A phishing domain targeting your organization poses a threat to customers, employees, and brand reputation, aiming to steal information and cause harm.	**Domain takedown service**	Our service quickly neutralizes phishing domains, enhancing security, protecting reputation, ensuring continuity, reducing breach costs, and ensuring compliance with cybersecurity standards.
Malicious email: A malicious email targeting your organization with spear-phishing poses risks to security, reputation, and operations by deceiving recipients into revealing sensitive information.	**Email takedown service**	Our service eliminates malicious emails, reducing data breach risks, protecting brand reputation, and ensuring continuity while minimizing financial and operational impacts and ensuring compliance.
Brand mention on social media: Brand mentions on social media, especially involving misinformation or fraud, can quickly damage reputation, customer trust, and market presence.	**Email takedown service**	Monitoring social media for brand mentions helps to manage reputational risks, address misinformation, and protect brand use, strengthening trust and preventing crises.

Potential digital risks	Atos solutions	Service features
Company profile impersonation on social media: Company impersonation on social media threatens your brand, deceiving stakeholders, spreading misinformation, and causing reputational damage.	**Social media monitoring**	Proactive impersonation monitoring protects your reputation, maintains trust, and prevents financial and operational risks, reinforcing your commitment to stakeholders.
Publicly available exposed databases: Exposed or misconfigured databases risk unauthorized access, data leakage, and compliance violations, leading to financial loss, reputational damage, and penalties.	**Data leakage monitoring**	Effective data leakage detection mitigates unauthorized access, protects sensitive information, ensures compliance, and minimizes financial and reputational impact.
Leaked company assets on code repositories: Company assets like credentials or API keys on platforms like GitHub can lead to unauthorized access, data breaches, and security risks.	**Data leakage monitoring**	Monitoring of exposed assets protect sensitive information, mitigates access risks, and prevents costly breaches, enhancing security and safeguarding operations.
Credential leaks caused by Infostealers: Credential leaks from Infostealer malware expose corporate emails and user credentials to unauthorized access, phishing, and exploitation.	**Infostealer monitoring**	Promptly addressing credential leaks reduces access risks, protects sensitive data, and minimizes exposure to phishing and cyberattacks, strengthening security and ensuring data protection.
Threat actor activity: Threat actors targeting your organization pose evolving risks, including data breaches, financial loss, and reputational damage.	**Threat landscape monitoring**	Continuous monitoring of threat actor activity helps to anticipate attacks, strengthen defenses, protect assets, and ensure operational resilience, boosting stakeholder trust.
Initial Access Brokers selling accesses: Initial Access Brokers sell unauthorized access to systems, enabling cybercriminals to launch attacks like ransomware and data breaches, jeopardizing security.	**Threat landscape monitoring**	Monitoring of initial access brokers helps to identify threats early, preventing unauthorized access and reducing large-scale attack risks, strengthening security and protecting sensitive data.

DRPS benefits

Comprehensive visibility by collecting massive amounts of data across digital channels (e.g., Surface, Deep, Dark Web, Mobile App Stores, Social Networks, Paste Sites, Gripe Sites, Blogs).

Identify and prioritizing threats as per your business context and relevance

Safeguard company's brand integrity and customer trust by identifying and neutralizing brand/executive impersonation

Save costs by preventing potentially financial losses, recovery costs, legal fees, and regulation fines

Industry Use cases

Energy & utilities

Prevent disruptions to power grids and ensure operational continuity by identifying and mitigating vulnerabilities in internet-facing systems, including SCADA systems, smart meters, and customer portals.

Healthcare & life sciences

Protect sensitive patient data, maintain HIPAA-compliance, and secure connected medical devices from unauthorized access and cyberattacks.

Financial services & insurance

Secure financial transactions, prevent fraud, and meet stringent regulatory requirements by continuously monitoring and securing all external-facing applications, APIs, and systems.

Manufacturing

Protect intellectual property, secure operational technology (OT) environments, and prevent supply chain disruptions by identifying and mitigating risks in connected factories, industrial control systems, and third-party connections.

Public sector & defense

Safeguard critical infrastructure, protect sensitive data from nation-state threats, and ensure national security by continuously monitoring and securing government websites, citizen portals, and defense systems.

Retail

Secure customer data, prevent online fraud, and protect brand reputation by identifying and mitigating vulnerabilities in e-commerce platforms, point-of-sale systems, and mobile applications.

Telecom

Secure communication networks, protect customer data, and prevent service outages by identifying and mitigating vulnerabilities in network infrastructure, customer portals, and mobile applications.

Media & technology

Secure communication networks, protect customer data, and prevent service outages by identifying and mitigating vulnerabilities in network infrastructure, customer portals, and mobile applications.

About Atos

Atos is a global leader in digital transformation with circa 78,000 employees and annual revenue of circa €10 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 68 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us

atos.net
atos.net/career
atos.net/drps
Let's start a discussion together

Regional contact numbers:

Global: +48 525 866 415
France: +33 (0)1 70 83 85 84
Germany: +49 30 398 202 777
Austria: +43 1 890 30 43 7777
Switzerland: +41 44 545 10 85
North America: +1-866-246-2848

Email: cybersecurity@atos.net

Atos