Atos Healthcare Cybersecurity Overview and Portfolio of Services

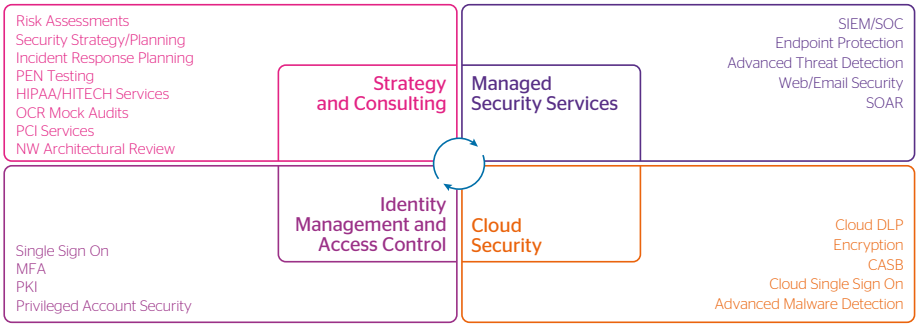
Trusted partner for your **Digital Journey**

Atos

Today's healthcare organizations face a daunting and ever-increasing level of risk. Coping with the wide array of threats is difficult enough and made no easier by the perceived absence of a single partner to whom healthcare organizations can turn.

Gartner recently ranked Atos as a Top 5 Managed Security Services Provider globally. By partnering with Atos, healthcare organizations can achieve best-in-class security across a spectrum of integrated services, such as those pictured on the right.

Atos has a rare combination of risk management consulting, strategic planning and managed security services that can provide healthcare organizations with genuine end-to-end cybersecurity solutions. Healthcare organizations often rely on a series of vendors to help them manage security, typically with non-integrated point solutions requiring additional onsite staff and expertise. This results in higher costs, an increased risk profile, and promotes "technology sprawl," a problem that severely compromises the capacity to identify and address potential incidents. It also is a distraction from the core mission of serving your patients. Atos cybersecurity services are aligned with the NIST Cyber Security Framework, shown on the right:



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Atos Cybersecurity Services Portfolio

Strategy and Consulting

For healthcare organizations, strategic planning and consulting can be a valuable first step. Atos has deep healthcare consulting experience and this service is typically the starting point for partnering with our customers. Our strategy and consulting offerings are aligned with the first phase in the NIST Cyber Security model: Identify

The objective of our Strategy and Consulting services is first to provide the client with an understanding of its current security posture and specific risk profile. Only by truly understanding your risk profile can we then develop an ongoing strategy that balances the required cyber security investment with the appropriate level of risk mitigation and overall protection. In order to achieve this, Atos offers a variety of consulting services from compliance-based engagements including HIPAA/HITECH, PCI, OCR Mock Audits to full scope Security Risk Assessments and Penetration Testing. This results in a strategic plan that includes recommendations, remediation initiatives to close the risk gaps, a formal roadmap showing sequencing and prioritization of activities, and project cost, timing and duration of each remediation initiative.

What makes Atos unique is that we offer best-in-class services to address and resolve the risk gaps that the Atos consultants identify. The services described below comprise the remaining primary Atos cybersecurity portfolio elements. They include remediation services and ongoing support solutions to address the everchanging healthcare threat landscape.

Identity Management and Access Control

Arguably the single most important action a healthcare organization can take to protect itself is to understand who has access to assets and information, who should have (and not have) access, and the ability to log and audit that access. In Atos' experience, improving control of access, authentication and authorization can by itself substantially improve risk posture. This skillset (which falls primarily under the Protect portion of the NIST framework) includes, among other services:

- **Privileged Access Security (PAS).** Privileged accounts includes individuals that have access to restricted or sensitive data, applications and hardware, and require strong protections. Atos protects that access by securing privileged credentials and auditing the use of those credentials.
- **Multifactor Authentication (MFA).** Because of the sensitivity of patient data, password protection is no longer adequate. Atos offers a range of multifactor authentication alternatives such as mobile phone authentication, SMS, smart cards, biometrics and more. Atos can help you understand the benefits and costs of each option so that your company can make the most sensible business decision.
- **PKI.** Atos offers certificate-based security for digital signing and encryption. This offers a far greater degree of privacy protection and data integrity than standard security. Healthcare organizations must provide robust privacy protections to patient data and PKI helps to achieve this.

Cloud Security

More and more healthcare provider and payer organizations are utilizing and leveraging the cloud to help control and manage costs. But establishing your own data center or relying on built-in security that cloud providers offer may not be ideal. Safeguarding ePHI must remain a top priority, and native cloud security can leave ePHI vulnerable.

Atos cloud security protects ePHI by monitoring and securing both sanctioned and shadow IT. It offers encryption, data loss prevention, and 24x7x365 monitoring to ensure that private patient information is protected. Our cloud security service is built using the most highly regarded cloud security products and techniques in the industry today. The Atos security portfolio, in combination with our cloud security, provides 360-degree complete protection by integrating both cloud security and traditional security into our 'single pane of glass' SOC service.

In the NIST model, Atos Cloud Security covers the Protect, Detect and Respond phases.

Managed Security Services

As a top 5 Managed Security Service Provider, Atos can help your company navigate through the complexities of today's security. Protecting ePHI and providing patients with the highest level of privacy is of paramount importance to the healthcare industry. Yet, based on the qualified security resource shortage, budget constraints and other priorities, healthcare organizations many times don't provide the quality and level of risk management they'd like. This is where Atos comes in.

Atos offers best-of-breed managed security services that have been tested and used by our clients for many years, and across the globe. These services include:

SIEM: (Security Information and Event Management).
This is the backbone of Atos managed security services. It is the central 'brain' of our security operations and automatically monitors and manages threats across the organization. It monitors endpoints, networks, applications and the cloud for unusual activities and anomalies. It is carefully tuned and regularly updated to ensure that malware is identified as soon as possible, and that action is taken to reduce threats.

Endpoint Protection:
Although more and more data resides in the cloud, it also resides on endpoints, either permanently or transiently. Accordingly, Atos works with the leading endpoint security providers to ensure that healthcare personnel are protected by the latest technologies available, including advanced anti-malware, dynamic application containment, and proactive web security. Endpoint security is no longer simply about antivirus, but instead a range of endpoint-oriented services that guard laptops, desktops and mobile devices from malware and data loss.

Security Operations Center (SOC):
Healthcare companies need the best available security, and it isn't always possible to provide this degree of expertise and monitoring in-house. Security is part art, part science, and while one of Atos' unique value propositions is our degree of automation, sometimes deeper human analysis is required. Our SOC is manned by experienced, senior level security personnel who analyze security information to determine not only the degree of threat, but the priority as well. They monitor threat feeds, network and endpoint agents for suspicious activity to determine when threats are real or when they are simply part of the background noise. In addition, the utilization of these integrated tools along with the experience of our security team minimize the false positives and subsequent alert fatigue.

Web/Email security:
Many threats arise from outside the organization. The internet and email are two of the most important threat vectors. Even well-trained employees can visit harmful websites or open attachments that launch malware inside the organization.

Atos managed services protects both internet and email gateways, helping to reduce the risks they pose to healthcare.

A vitally important function of our Managed Security Service is aligned to the Recovery phase of the NIST framework. No matter how well security is planned and executed, threats will find their way through. It is vitally important to have in place a tested system to communicate with clients and make improvements. Atos does this in a variety of ways, including our ticketing system, regular contact with our customers, and Incident Response Planning engagements that provide for a formal, structured, orderly, and coordinated response to a cyber crisis. These tools and services can significantly reduce a breach's impact.

Atos Managed Security Services address all 5 phases of the NIST framework—from Identify through Recovery.

Summary

Shown here is a high-level view of the Atos Healthcare Cybersecurity Portfolio and how it is aligned to the NIST framework.

Your healthcare company needs protection at all phases of the NIST Framework, and as a top 5 MSSP, Atos can help you achieve the highest level of risk management

Atos Security Services Aligned to NIST Framework

Identify	Protect	Detect	Respond	Recover
Security Strategy/Planning	Endpoint Protection	SIEM	SOAR	Incident Response Planning
Risk Assessment	Identity Management	Data Loss Prevention	SOC	Forensics
PEN Testing	Cloud Security	Analytics	CERT	Improvement Planning
Mock Audit	Encryption	Advanced Threat Detection	Integrated Incident Management	
HIPAA/HITECH Services	Web/Email Security			
PCI Services	Privileged Account Security			

Strategy and Consulting: To help identify risk areas, prioritize them, and put in place a strategic risk mitigation plan to close the current gaps in your cybersecurity program and -- at the same time -- balance the investment required with the proper level of protection.

Identity Management and Access Control: To ensure only the right people have the right access to ePHI at the right time—a core component of any security program.

Cloud Security: To enable healthcare to leverage the cloud and its financial and operational benefits while reducing the substantial risks the cloud poses.

Managed Security Services: Incorporates all the above, including Atos SOC and SIEM services, into one cohesive, integrated outsourced package. This enables you to focus on patient care and provide the best healthcare services possible.

About Atos

Atos is a global leader in digital transformation with 120,000 employees in 73 countries and annual revenue of € 13 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
https://atos.net/en-na/north-america/healthcare-cyber-security-solutions

Let's start a discussion together

CT_11897_190122_RY_WP_HEALTHCARE