SOLUTION BRIEF

Overcome the Unique Challenges of Healthcare in the Cloud with Lacework FortiCNAPP and AWS

Executive Summary

At Fortinet, we understand the tough obstacles organizations face when embracing digital transformation. We have been helping organizations tackle security and compliance challenges since our founding in 2000. We know different industries face different levels of scrutiny. Some are so highly regulated that they must expend enormous time and energy dealing with regulatory requirements. These same industries are often targeted by cybercriminals due to the value of their data, making compliance and security a part of their organization's fabric.

Ranking high on that list are healthcare organizations. Like software companies, they have the same security requirements for protecting their applications from build through runtime, with additional requirements for HIPAA, SOC 2, and ISO.

Whether you are cloud-savvy and new to the healthcare industry or experienced in healthcare but trying to embrace cloud technology, you undoubtedly understand that with the great agility and scalability that cloud computing offers comes risk. Cybercriminals continuously scan cloud networks for misconfigurations, and attackers know that industries like healthcare retain data that holds enormous value.

Your patient and customer trust is paramount, so it's essential that you invest in modern cybersecurity tools and resources. Fortinet and Amazon Web Services (AWS) are here for you with a healthy approach to managing your cloud security posture, keeping local and global threats at bay.

Protecting Your Healthcare Business and Patients Alike

Insecure cloud environments put a company's reputation and revenue at risk. According to the 2023 IBM Cost of a Data Breach Report, "Healthcare breach costs hit a new record high. The average breach in healthcare has increased to US$10.93 million—the highest among all industries. Healthcare breach costs have been the most expensive industry for 12 years running, increasing by 41.6% since the 2020 report."[1] The stakes are high when it comes to handling health data. And achieving proper cloud security can seem overwhelming or out of reach. The weight of penalties, fines, lawsuits, settlements, and loss of critical patient data can have a huge impact on your organization. There is a solution, though.

To keep patient data secure, typically with limited resources, healthcare organizations have sought a platform that provides comprehensive protection for their cloud environments. French healthcare company and AWS user Dreem can attest. It needed to protect patient data and meet HIPAA compliance standards. It needed to reduce its attack surface and enable its lone DevOps engineer to handle all security alerts.

Dreem is hosted on AWS. It's application architecture uses microservices orchestrated by Kubernetes. It had multiple AWS services, targeting the right tools for each situation. But even with the right tools, it found a comprehensive cloud security platform solution, like Lacework FortiCNAPP, better secured its cloud and reduced its technology costs.

Important considerations

- The compliance landscape is complicated. From HIPAA to SOC 2 to PCI, how will you demonstrate continuous compliance to auditors?
- Traditional on-premises approaches don't apply to cloud technology. Do you have the right skill set for needed automation and cloud controls?
- How do you manage the cost of IT when your organizational goals are focused on healthcare?
- It's vital to secure your data, including access. How do you guarantee the privacy of your data and control who has access to it?

Key challenges

- Implementing security best practices
- Future-proofing infrastructure
- Building a fail-fast culture for developers
- Lack of automation capabilities
- Inability to scale
- Easily maintain compliance with regulations

Managing Multiple Point Security Tools Is Not Beneficial for Business

Cloud-native application protection platforms, or CNAPPs, are security solutions that provide developer, security, and operations teams one centralized place to view and manage security controls while creating and maintaining applications in the cloud. A proper CNAPP integrates with the systems and tools that businesses already use to develop and run cloud applications, protecting those applications throughout each step in the process.

One of the great advantages of a CNAPP is that it enables you to consolidate tools. Healthcare companies can experience significant benefits by consolidating many of their security tools, including cloud security posture management (CSPM), cloud workload protection platforms (CWPPs), cloud infrastructure entitlement management (CIEM), and Infrastructure-as-Code (IaC) tools, into a single platform. Using one tool to find vulnerabilities, report compliance, and detect threats across multiple clouds will save you time and money.

In addition, you'll only need to teach your teams how to use one security tool (which means fewer training sessions), and you won't need to renew nearly as many software licenses each year.

Fortinet and AWS Help to Quickly and Securely Aid Healthcare Organizations

Healthcare applications in the cloud are on the rise despite the continuous security, resiliency, and regulatory compliance restraints that take time and resources. These cloud-based solutions accelerate innovation and improve the development, manufacturing, and distribution processes. They also benefit organizations undergoing early drug discovery, clinical trial testing, FDA approval, and post-market monitoring. Although your healthcare organization may not be born in the cloud, cloud migration and adoption are likely part of your business goals, and utilizing partners that are focused on such capabilities is essential.

A data-driven CNAPP, Lacework FortiCNAPP, delivers a unified platform for complete cloud coverage. The Lacework FortiCNAPP platform harnesses your data and correlates behaviors so no threat can hide. Lacework FortiCNAPP gives you the ability to assess the security of your environment from code to cloud. By working at multiple stages of the software delivery life cycle, the Polygraph Data Platform enables you to detect and prevent security issues early, where it is easier to investigate and has less impact on your business. The growing list of AWS integrations, like AWS CloudTrail, AWS Security Hub, Amazon Security Lake, and more, means we are committed to enabling our customers' success in cloud security, including application modernization, container security, compliance (such as ISO 27001, SOC 2, PCI DSS, HIPAA, NIST 800) and cybersecurity best practices like the CIS benchmarks.

The combination of Lacework FortiCNAPP and AWS, including services like Amazon GuardDuty and AWS CloudTrail, helps us monitor and attribute behavior end to end, from initial activity to ensuring the appropriate changes get made. We can monitor suspicious behavior or anomalies, then link the behavior to the change that was made. It's about insight, for sure, but more importantly, efficiency, as the tools talk to each other."

Russell K.
Information Security Engineer
RapidSOS

"What's really nice about the Lacework FortiCNAPP UI is that it bubbles up errors. It allows us as security practitioners to be able to understand what's calling a particular AWS API or endpoint."

Greg Soner
Senior Director
Omada Health

The collaboration between Fortinet and AWS provides healthcare organizations with best-of-breed support. San Francisco, California–based Omada Health shared its story: "Before, if the company wanted to examine the encryption settings across Amazon S3 buckets, the team had to check individual settings on each one to determine if the data was encrypted or not. As the company grew, engineers had to do this for hundreds of buckets. Since Lacework FortiCNAPP allows the team to see all the information for each bucket in one dashboard, the DevOps team saves up to 20 hours on this process annually. Omada Health can now spot configurations not compliant with standards such as the HIPAA Security Rule and other cloud compliance and security measures in real time. As a result, the context-rich alerts from Lacework FortiCNAPP allow the company to prioritize and accelerate remediation. This improved visibility has made it easier for Omada Health to catch potential issues earlier."

Experience the Lacework Difference

Understand Your Cloud and Find Unknown Threats

Lacework CNAPP is the only solution to automatically identify net-new cloud behaviors and detect unknown threats.

Our patented technology automatically learns your cloud environment, visualizes all its complex relationships, baselines normal behavior and activity, and alerts you on changes that warrant attention all without manual configuration.

Single Platform Delivers Continuous Security and an Integrated Experience

Lacework CNAPP delivers a unified user experience for multi-cloud, hybrid, and Kubernetes coverage on Linux and Windows.

The Lacework FortiCNAPP platform has a flexible architecture that easily adapts to evolving cloud technologies for continuous security and a centralized view of auditable compliance evidence.

Focus on the Risks That Matter Most

Lacework CNAPP automatically correlates the entire data workflow, from code to cloud, to put risks into context.

Lacework FortiCNAPP natively integrates into existing workflows and toolchains and provides highly contextualized alerts that detail who, what, why, when, and where within a singular view so the right people on your team can take the right action.

Fast and Flexible to Operationalize at Scale

Lacework CNAPP natively integrates into your DevOps, IT, and security workflows for seamless scalability, visibility, and control.

Our full turnkey Software-as-a-Service platform can adapt with you as your cloud security needs evolve, whether you grow into multiple clouds, scale out the size of your environment, or need additional security capabilities.

Because Lacework FortiCNAPP was built in the cloud, for the cloud, our platform helps AWS users go further, faster in securing their modern applications. We see security as a data problem. And with our data-driven approach, the platform collects and processes your vast amounts of cloud data, automatically detects threats so you don't have to, and brings together the full security context for investigation and remediation.

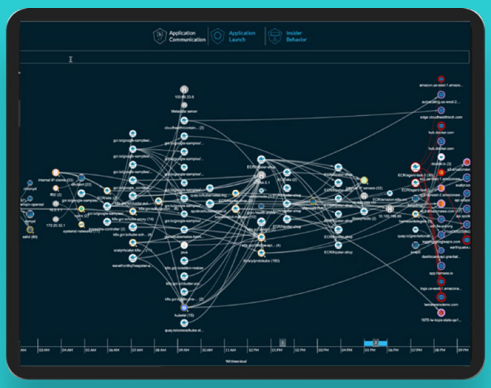
For healthcare technology in particular, this means we help you:

- Prioritize your cloud security risks through visibility and context of vulnerabilities throughout the application life cycle
- Find known and unknown threats faster, giving you high confidence in security findings based on anomaly detection from cloud audit logs and agent monitoring
- Increase operational efficiency so you can achieve more with less, lowering your total cost of ownership and improving time to value
- Achieve continuous cloud compliance on HIPAA, SOC 2, and ISO

Get started now

VISIT FORTINET IN AWS MARKETPLACE

CONTACT US



Visit fortinet.com/AWS for more details, demo videos, white papers, case studies, and customer testimonials.

[1] IBM Cost of a Data Breach Report.

FORTINET

www.fortinet.com

August 9, 2024 12:48 PM / 2802076-0-0-EN