Runecast

WHITEPAPER

AUTOMATING HEALTHCARE SECURITY: PROTECTING CRITICAL WORKLOADS AND SENSITIVE DATA

OVERVIEW

Healthcare professionals deal with extremely sensitive patient data daily, including medical records, personal information, and billing details. As a result, healthcare providers and insurers serve as the primary guardians of patient's health and personal data. This information is highly valued by threat actors and must be protected regardless of its storage location, transmission method, or access permissions.

Failing to adequately secure this confidential and sensitive data can result in significant consequences including legal and financial penalties, reputational damage, operational disruptions, and data recovery costs.

In addition to these security concerns, healthcare organizations must also comply with specific regulations such as HIPAA, GDPR, and, in some cases, PCI, to ensure that electronic Protected Health Information (ePHI) is handled, stored, transferred, and received in a confidential and secure manner.

To reduce vulnerable entry points and improve their security posture, healthcare organizations require a solution that provides automated and continuous vulnerability and compliance monitoring and assessment. Without it, they will be vulnerable to sophisticated attacks, such as ransomware designed to encrypt information, extort large sums of money, or carry out other malicious activities.

KEY TAKEAWAYS

- Complying with regulations such as HIPAA, GDPR, and PCI and controlling patient information processes are the main challenges for healthcare organizations.
- Healthcare organizations are vulnerable to various attack scenarios, including data breaches, malware, and ransomware attacks, insider threats, and third-party risks.
- Antivirus solutions are no longer enough to protect endpoints against ransomware and other types of malware. An AI-powered automation system to provide predictive and prescriptive insights is key to having a proactive approach to cyber threats.

DISTRIBUTED ARCHITECTURES CAN LEAD TO DISTRIBUTED PROBLEMS

As in many other sectors, healthcare organizations run their workloads in highly distributed environments with a combination of different tech stacks. This not only increases the risk of blind spots but also turns the effort of keeping environments up-to-date with the latest standards and best practices into a time-consuming and cost-prohibitive task without the aid of automated processes.

New norms, such as clinical administrators working from home or the rise of telemedicine, the expanding networking of devices – smartphones, tablets, wearables, digital medical equipment – multiply the number of potential entry points for bad actors and increase the risk to which healthcare organizations are exposed.

This high level of digitalization, combined with a lack of effective solutions and budget, makes them particularly vulnerable to cyber-attacks.

CRITICAL VULNERABILITIES IN HEALTHCARE INSTITUTIONS: OUTSIDER AND INSIDER THREATS

As healthcare institutions become increasingly reliant on technology, they face a growing risk of threats, both from external attackers and insiders.

Typical attack scenarios and risks faced by healthcare organizations are

- **Configuration drift**: Consistent configuration is a crucial part of stable and predictable infrastructure. Ad-hoc software and hardware changes in the environment create configuration drift and are usually not recorded or tracked in a thorough or efficient manner which causes a significant risk of misconfigured workloads over time. This is a primary factor contributing to data breaches. Such breaches are extremely costly for healthcare organizations, both in terms of financial losses and reputational harm.

- **Malware and ransomware**: Malware and ransomware attacks are becoming increasingly common and sophisticated. Healthcare institutions are particularly susceptible to those attacks because threat actors understand the value of the data that are stored and the healthcare network has numerous entry points for attackers. Traditional solutions such as anti-virus software are no longer sufficient to prevent the exploitation of vulnerabilities and security gaps.

- **Insider threats**: Healthcare organizations must be vigilant against insider threats, including employees who intentionally or unintentionally compromise patient data. This may involve unauthorized access to patient information or falling victim to phishing scams.

- **Third-party risks**: Hospitals and clinics often work with third-party vendors and contractors, which can introduce additional security risks. Healthcare providers must ensure that these vendors and contractors adhere to security and compliance standards.

Given these factors, healthcare organizations must safeguard sensitive patient information by implementing robust measures for patient data protection, including access controls, encryption, regular backups, security monitoring, and regulation compliance. Thus, they can guarantee the security and confidentiality of that patient data and prevent unauthorized access to patient information.

OVERCOMING CHALLENGES IN HEALTHCARE IT SECURITY AND COMPLIANCE

Healthcare IT departments often deal with several challenges and pain points when it comes to upholding their security posture. These are some examples:

- **Complexity of IT systems**: The majority of organizations run their workloads in hybrid or multi-cloud environments. Staying on top of the various security and compliance requirements of each of these technologies is costly and time-consuming. To overcome this challenge, healthcare organizations must find a solution able to provide full visibility into vulnerabilities, configuration drift, security standards and compliance assessments across their entire technology stack.

- **Outdated technology and a lack of updates**: Added to this hybrid environment, healthcare organizations are often forced to use potentially outdated systems and devices. There are several reasons for using unsupported software versions such as lack of budget, system integration requirements, business priorities, etc. This scenario, combined with the increasing use of electronic devices, broadens an organization's attack surface and increases the likelihood of compliance violations and being targeted by attackers.

- **Strict rules and regulations**: Healthcare providers need to follow several frameworks like HIPAA, HITECH, GDPR, ISO 27001, and PCI DSS to name just a few in order to ensure secure electronic data interchange (eDI). Complying with these legal requirements can be difficult as they often necessitate investing in additional technology, subject matter expert personnel, and training. However, not adhering to these legal requirements is costly and can lead to financial penalties, reputational damage, and loss of revenue.

Healthcare organizations need a solution that continuously tracks risk, compliance, and environmental health in a consistent and unified way. Without it, organizations are vulnerable to advanced attacks that can potentially exfiltrate sensitive patient data, demand large sums of money, or block access to crucial systems that may impact the critical care of patients.

PROACTIVE PROTECTION OF MISSION-CRITICAL ASSETS TO IDENTIFY BLIND SPOTS AND REDUCE ATTACK SURFACE

One of the major concerns of any organization is the lack of visibility into mission critical workloads and consequently, the existence of blind spots and security gaps.

The first step to protecting your environment is acknowledging the fact that it is not feasible to 100% safeguard it from cyber-attacks. Pragmatically, what healthcare organizations can do is adopt a single source of truth to bridge the gap between IT Ops and Security teams and prevent these attacks before they occur.

Runecast uses an AI-based automation system that offers proactive, predictive, and prescriptive insights to help healthcare organizations protect their infrastructure against cyber threats.

RUNECAST ENABLES HEALTHCARE ORGANIZATIONS TO:

- Obtain a **real-time automated analysis** of VMware, AWS, Azure, Google Cloud, Operating Systems – Windows and Linux – and Kubernetes environments.
- **Choose between agentless or agent-based** analysis for on-prem and cloud environments.
- Get **unified visibility** and consistent reporting for vulnerability assessment, compliance checks, and IT Operations Management in a single platform.
- Conduct **continuous automated security** auditing and inspection for critical compliance standards in healthcare, such as HIPAA, GDPR, or PCI DSS.
- **Effectively assess vulnerabilities** based on severity and impact scoring from CISA's CVE and KEV identification. It also evaluates specific criteria related to the use case to accurately determine the validity of reported vulnerabilities, in addition to verifying the host version and build number.
- **Save time and budget** in employee training thanks to its intuitive user interface.
- Ensure that **patient data is secure and protected**, with all data processing done locally on the appliance.
- Analyze their systems even in **air-gapped environments** to minimize the risk of exposing infrastructure data to the public network.
- **Detect configuration drift** over time that can lead to security breaches.
- Speed time to resolution by providing **detailed remediation** information and **tailored scripts**.

Runecast helps healthcare organizations protect their mission-critical workloads and streamline security and operations by combining vulnerability assessment with continuous analysis against security compliance standards and hardening guides.

OUR CUSTOMERS REPORT IMMEDIATE ROI

CISOs, CIOs, Security, and Ops Teams are benefiting from Runecast Intelligence

- 100% security audits passed successfully
- 75-90% time savings on vulnerability management and troubleshooting
- Up to 100% service uptime
- Increased operational efficiency and observability
- Stability of mission-critical urgent-healthcare systems

Most prominent customers in the healthcare sector:
Bayer, **DHU healthcare**, **NYC Health Hospitals**, **Kiel Municipal Hospital**

USE CASE: TOP COMMUNITY HOSPITAL

Summary

One of the top municipal community hospitals in Germany offers top-notch healthcare services to thousands of patients annually, including radiological examinations.

The IT team faced challenges in dealing with security and maintaining operations, with limited visibility of vulnerabilities and configurations. Their approach was reactive, with a lot of manual work, and with very limited visibility of vulnerabilities and configurations.

Like any medical organization, the IT team also had to face the challenge of having to comply with new security regulations such as BSI IT-Grundschutz and potentially healthcare-specific standards such as HIPAA for securing patient personal records. This is why they decided to deploy Runecast.

Challenge

The IT team faced the challenge of complying with new security regulations as a healthcare provider. To proactively achieve and demonstrate security compliance, they needed a solution to monitor the infrastructure for vulnerabilities and misconfigurations. They had 12 ESXi hosts, almost 300 VMs, a database cluster, and many Windows and Linux machines distributed throughout the hospital to check for security legal requirements and vulnerabilities. The team spent half their time on security with a reactive approach and limited visibility of vulnerabilities. They lacked confidence in proving compliance manually and needed high availability. Therefore, they looked for a solution to transform their approach into a proactive one. They needed to prove measures for vulnerability management and security compliance.

Solution: Runecast

The hospital deployed Runecast in an hour and the first scan revealed vulnerabilities, misconfigurations in their VMware security posture, Windows OS misconfigurations, and other bugs.

They used the platform to prioritize remediation based on criticality and resolved 80% of VMware issues in two to three weeks. The OS issues would take a few months due to them being production machines.

The Runecast platform provided the solution to mitigate all vulnerabilities and misconfigurations to get the infrastructure compliant with security regulations. They were surprised by the amount of information but found everything in one platform and simple.

RESULTS

By deploying Runecast, the hospital gets the following benefits:

- Critical issues are now visible, easily prioritized, and able to be worked on proactively
- Proactively achieve and demonstrate security compliance
- 2 months of manual work saved in mitigating vulnerabilities
- 100s of hours saved with remediation scripts alone
- Saves the cost of them needing to find and add more team members

SUMMARY

We are witnessing a moment in which cyber-attacks on healthcare organizations are becoming more frequent. Cybercriminals have developed highly sophisticated modes of attack to extract sensitive information and block access to critical systems, thus being able to extort and blackmail these organizations to avoid putting the data and health of their patients at risk.

These risks are known and understood, but many hospitals and clinics still work with outdated and un-updated systems or continue to manually monitor their systems to find vulnerabilities or security breaches. This increases the risk of human error, data leakage, and non-compliance with regulations. At Runecast, our goal is to provide healthcare organizations with an efficient solution that can help them automate vulnerability assessment, system configuration drift, and compliance with regulations to ensure patient information is safe and minimize their attack surface.

Improved security and compliance posture
- Risk-based vulnerability assessment
- Checks against over 13 security compliance standards
- Automatic update checks for security patches, bug fixes, and new feature releases

Fast remediation
- Detailed remediation steps based on recommendations from VMware, cloud providers, and industry best practices
- Tailored scripts

Increased staff productivity
- Centralized dashboard for IT Operations and Security Management
- Intuitive user interface
- Easy reporting

Enhanced system stability and performance
- Configuration drift management
- Best practice analysis
- Real-time log analysis
- Upgrade simulation and hardware compatibility checks

Learn more
For more information please visit runecast.com or try Runecast on your environment by requesting an online demo at runecast.com/runecast-analyzer-online-demo.

Runecast

When your organization increases the complexity of its IT architecture and your workload spans across multiple systems and technologies, reducing complexity, lower operational overhead, and having full visibility of your environment becomes a critical burden to address.

To achieve unified issue visibility and reporting, organizations need to adopt a single platform that connects all disparate infrastructure technologies, from bare metal and hypervisor technologies to cloud service providers and containerized workloads.

Runecast brings organizations an integrated approach to security and compliance by tracking the exposure risk, compliance status, and environmental health via a single and automated platform.

For more information please visit runecast.com

Runecast Solutions Ltd.

124 City Road,
London, EC1V 2NX
United Kingdom

Runecast Solutions Inc.

300 Delaware Ave
Suite 210, Box #241
Wilmington, DE 19801
USA