Modernizing Cybersecurity for Healthcare

Protecting healthcare organizations from evolving cyberthreats across endpoints, identities, data, and applications.

Integration Highlights:

- Prevent: Adaptive zero trust access to applications on shared workstations; identify and classify sensitive data to prevent the loss of PHI data
- Detect and respond: Mitigate potential breaches with integrated threat intelligence, shared telemetry, and automated workflows across platforms
- Recover: Minimize down time and safeguard PHI with rapid recovery from ransomware attacks

The Challenge: Securing Healthcare in a High-Risk Landscape

Healthcare organizations face unique cybersecurity challenges.

- **Rising volume and sophistication of ransomware attacks:** The healthcare industry has 50% more sensitive data than the global average,[1] making it one of the most targeted industries for attacks. Attackers use increasingly advanced methods to infiltrate networks and devices, making it difficult for organizations to keep up and prevent breaches that disrupt patient care and compromise PHI.
- **Data privacy and compliance pressure:** With stringent regulations like HIPAA, healthcare organizations must ensure compliance. Protecting sensitive patient data across devices (including shared workstations), cloud applications, and remote endpoints, while maintaining patient data privacy and regulatory compliance, requires advanced security and continuous monitoring to avoid costly violations and fines.
- **Minimizing the impact of cyberattacks on patient care and business operations:** Cyberattacks can cause major disruptions to hospital operations, including doctors being unable to access patient records, surgeries being postponed, and more. Healthcare organizations must not only work towards preventing cyberattacks but also achieving cyber resiliency for maintaining patient care continuity.

[1] Rubrik Zero Labs Report

Healthcare Organization Needs

To combat these challenges, healthcare organizations need modern, integrated solutions that deliver end-to-end zero trust security, ensuring uninterrupted access to critical patient data, devices, and systems—all while enabling a seamless user experience for clinicians that doesn't impact performance, even when under attack.

Organizations must be able to rapidly detect advanced threats and respond to incidents in a timely manner. In the event of a ransomware attack, organizations must be able to recover critical data and systems quickly to prevent business and patient care disruption while avoiding reinfection.

The Solution: Unified Cybersecurity for Healthcare

CrowdStrike, Imprivata, Rubrik, and Zscaler combine to enhance security and resilience for healthcare organizations by protecting them from cyberthreats, including ransomware—the threat that keeps healthcare CIOs up at night. Together, these partners deliver a modern, automated approach to prevent, respond, and recover from ransomware attacks while enabling zero trust access to data and applications.

Anatomy of a Ransomware Attack

Ransomware attacks can have devastating impacts on healthcare organizations. In fact, they cause a 37% increase in patient care delays, and it typically takes an organization 2-3 weeks to return to typical patient care levels following an attack.[2] How do these attacks work?

1. **Access:** Malicious actors gain access to a healthcare organization's network (e.g., through a compromised workstation).
2. **Initiation:** Attackers encrypt critical patient/medical data, so it's no longer accessible.
3. **Ransom:** Attackers demand a heavy ransom for decrypting the files and restoring the data. They may also threaten to leak the data that is stolen.

[2] Rubrik Zero Labs Report

Key benefits include, but are not limited to, the following:

Threat prevention with adaptive zero trust access: CrowdStrike, Imprivata, and Zscaler help prevent ransomware attacks by delivering zero trust security for shared workstations. The integrations ensure clinicians can only access authorized applications and data, adapting access policies in real time based on user (i.e., doctor or nurse) and device context (i.e., high vs. low risk). In addition, Rubrik's Sensitive Data Monitoring discovers and classifies sensitive data across enterprise, cloud, and SaaS environments. This information is then shared with Zscaler Data Loss Prevention (DLP), which applies security policies to prevent unauthorized data transfers, ensuring the protection of sensitive information such as protected health information (PHI).

Unified visibility and proactive threat response: With integrated threat intelligence, shared telemetry, and automated workflows across all four platforms, security teams gain comprehensive insights into the entire threat landscape across endpoints, networks, identities, and data, enabling faster detection and streamlined response to mitigate the impact of potential breaches and cyberattacks.

Enhanced cyber resilience and rapid recovery: CrowdStrike, Rubrik, and Zscaler enable healthcare organizations to recover from ransomware attacks quickly while preventing sensitive data from being stolen. Rubrik delivers cyber resilience for EHR and other clinical applications by combining backup and cybersecurity into one platform. Healthcare organizations can proactively minimize PHI exposure risks, investigate and contain threats, and rapidly restore data integrity when systems are attacked—avoiding costly recoveries, lengthy downtime, and reputation damage.

Key Supported Use Cases:

Zero Trust Access to Applications on Shared Workstations

Problem: A hacker can compromise a legacy perimeter- and firewall-based network by gaining access to a single workstation. Hospitals and healthcare organizations have large numbers of workstations shared by doctors and nurses, making these devices primary attack targets.

Solution: Imprivata, CrowdStrike, and Zscaler provide zero trust security for multi-user workstations in healthcare organizations. The Imprivata Enterprise Access Management identity management platform integrates with the Zscaler Zero Trust Exchange (ZTE) to ensure that only authorized users have access to approved applications. For example, nurses and doctors have access to different applications even if they're using the same workstation.

Zscaler also integrates with CrowdStrike by incorporating the CrowdStrike Falcon® Zero Trust Assessment (ZTA) score. Even if doctors and nurses are authorized to access certain applications, if a workstation is viewed as "high risk" based on the Falcon ZTA score, then neither clinician may be allowed to access any applications.

Benefits: The Zscaler ZTE adaptively enforces access control policies, ensuring that only authenticated users are allowed to access authorized applications. Imprivata allows clinicians to seamlessly and securely authenticate in and out of shared devices with the tap of their badge for a seamless user experience. User actions are logged for traceability and compliance purposes. This integration drives clinician productivity, reduces the risk of ransomware attacks and downtime, and strengthens regulatory compliance.

Additionally, Zscaler incorporates device context via the CrowdStrike Falcon ZTA score to ensure that only "high trust" workstations are able to access sensitive applications, which reduces the attack surface for shared workstations.

Preventing and Responding to an Attack

Problem: The healthcare industry is the number one target of ransomware attacks, which are increasing in number and sophistication due to the high value of PHI data and the critical need for continuity of care. Legacy systems make it challenging to effectively identify and prioritize threats amidst an overwhelming volume of alerts from disparate solutions.

Solution: CrowdStrike Falcon integrates with Rubrik Security Cloud to ingest rich data context, and separately with the Zscaler ZTE to consume threat intelligence. This combination of threat intelligence and context about the data under attack in one place enhances unified visibility, enabling faster, more effective threat detection and response against attacks on data. Specific integrations include:

- Zscaler Cloud Sandbox integrates with CrowdStrike Falcon telemetry to detect zero day malware and facilitate rapid quarantine actions on impacted endpoints.
- Zscaler shares relevant Zscaler logs with CrowdStrike for improved end-to-end visibility of endpoints, networks, and cloud applications to accelerate investigations.
- CrowdStrike Falcon® Next-Gen SIEM integrates with Zscaler via the Falcon Foundry for Zscaler app and provides full closed-loop remediation between ZIA's advanced sandboxing, CrowdStrike's next-generation SIEM, and ZIA's policy enforcement engine.
- Rubrik Security Cloud shares data context, such as sensitive file types and locations, with the CrowdStrike Falcon platform. This enables security teams to prioritize threats based on the criticality of the data involved, enhancing visibility into potential risks and reducing investigation time.

Benefits: CrowdStrike, Zscaler, and Rubrik work together to protect critical data by reducing alert noise, enabling you to quickly identify, prioritize, and mitigate the impact of attacks. By combining CrowdStrike's telemetry, Zscaler's threat intelligence, and Rubrik's data insights, healthcare organizations gain a unified view of data and network activity, accelerating threat hunting and remediation. The combined solutions support advanced zero-day threat detection and quarantine, cross-platform telemetry sharing and correlation, and cross-platform detection and response.

Minimizing the Impact of a Cyberattack

Problem: Attackers are now weaponizing data with double extortion ransomware attacks that involve encrypting the critical content and exfiltrating it out of the organization. This makes it more complex to recover the data and maintain business continuity, which is critical for quality patient care.

Solution: Rubrik's integration with Zscaler Data Protection proactively discovers and classifies sensitive data across enterprise, cloud, and SaaS environments so Zscaler can enforce data protection policies without impacting production systems. Rubrik also enables rapid post-attack recovery of infected systems and applications with automated processes and guided workflows.

Benefits: Rubrik Sensitive Data Monitoring and Management discovers and classifies sensitive data that matters so Zscaler can enforce data protection policies without the complexity and burden of taxing production systems. This ensures that sensitive data can't be exfiltrated in the event of a ransomware attack.

The Rubrik and Zscaler integration enables healthcare organizations to proactively reduce the risk of sensitive patient data (PHI) exposure before an attack happens. In the event of an attack, Rubrik enables rapid recovery of infected systems to a clean state to reduce the risk of data loss and patient care disruption, without paying a ransom.

About CrowdStrike: CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud native platform for protecting critical areas of enterprise risk—endpoints and cloud workloads, identity and data. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value. CrowdStrike: We stop breaches.

About Imprivata: Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

About Rubrik: Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

About Zscaler: Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.