Reach

Securing Healthcare:

Using Exposure Management to Stop Ransomware and Other Threats

The Healthcare Cybersecurity Challenge

Healthcare organizations face a growing number of cybersecurity threats, from regulatory compliance pressures to insider threats, misconfigured security controls, and third-party risks. With increasing reliance on digital systems, connected medical devices, and cloud-based patient data management, securing healthcare environments has never been more complex. Security teams are often under-resourced, making it challenging to stay ahead of evolving threats. Exposure management provides a proactive approach, ensuring that organizations can continuously identify, prioritize, and remediate security risks before attackers exploit them.

The Role of Exposure Management in Ransomware Defense

Healthcare organizations are often forced to do more with less, as security teams face resource constraints and an overwhelming attack surface. Reach helps maximize the productivity of both your security stack and your team, providing the visibility and action needed to defend your organization against ransomware and other threats.

By applying exposure management, security teams can:

- Identify and fix security gaps proactively by taking action before attackers exploit them.
- Prioritize remediation efforts based on real-world threats and the potential impact on users or devices in the network, ensuring he most impactful actions are taken first.
- Accomplish more while reducing mundane and error prone tasks by automating and streamlining security updates.

Exposure management provides the insights needed to harden defenses, enforce least privilege, and reduce attack surfaces, helping organizations proactively address vulnerabilities before they are exploited.

Why Reach?

Maximize Security Investments

Ensure every dollar spent on security tools delivers value, eliminating underutilized features and blind spots.

Amplify Your Security Team

Automate critical remediation tasks, reducing manual workload and allowing teams to focus on high-priority risks.

Continuous Validation

Ensure defenses against threats like ransomware remain aligned with real-world attack tactics and regulatory compliance over time.

sales@reach.security
reach.security/connect

Reach Capability	Description
Identify Security Blind Spots 	- Continuously analyze security controls across identity, email, endpoint, and network security. - Detect misconfigurations, unused security features, and gaps in coverage that leave healthcare systems vulnerable.
Prioritize Action 	- Focus security efforts on the most impactful remediation steps based on real-world threats. - Provide context to optimize security investments, ensuring licensed tools are fully utilized.
Guide Remediation 	- Deliver step-by-step deployment guidance and automate updates and enforcement through integrations with ServiceNow, Jira, and security platforms to harden security configurations in existing tools. - Continuously validate that security policies remain effective against evolving threats including ransomware. - Predict the impact control changes will make to an organization, reducing the possibility of unintentional healthcare system service disruptions.

Proven Results: Amplifying Security with Reach

Organizations across a wide range of industries rely on Reach to drive meaningful security and efficiency improvements, demonstrating its ability to deliver results in complex environments:

- A Fortune 500 company reduced security misconfigurations by 47% in just 90 days, strengthening protections across identity, network, and endpoint security
- One customer used Reach to automatically generate 70% of the remediation steps required, reducing the manual burden on their security team.
- A company identified that just 4% of users accounted for 70% of risk, allowing targeted action to drastically reduce the threat surface and potential business impact.

Protect Healthcare Operations with Reach

To join the community of customers enjoying the benefits of Reach and learn more about how it can transform your security posture, visit:

reach.security/try-reach

sales@reach.security
reach.security/connect