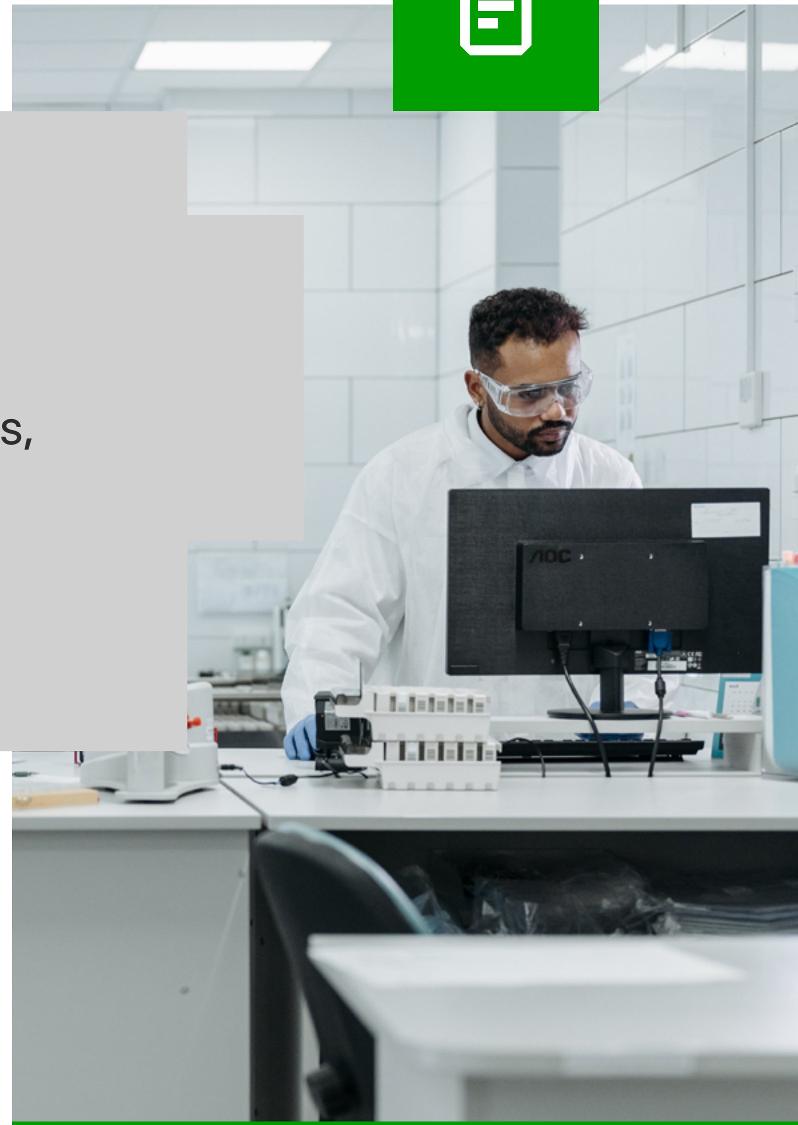
exabeam

Solution Brief

Healthcare

Mitigate your cybersecurity risks, support a culture of regulatory compliance, and overcome the cybersecurity skills shortage



The healthcare sector, already a prime target of hackers and rogue insiders looking to access electronic medical records (EMR) is evolving.

The healthcare industry is increasingly embracing emerging medical technologies such as IoT, digital therapeutics, cloud hosting, and AI. In doing so, they've significantly increased the complexity of safeguarding protected health information (PHI) and networks. Fueled by a growing need to share critical patient data across providers via electronic health records (EHR), the healthcare industry has become an attractive target for ransomware attacks.

Exabeam helps healthcare organizations address today's cybersecurity challenges.

Exabeam ingests log files from your security and IT applications, analyzes the logs, and applies behavioral analytics to detect early indicators of compromise (IoCs) and malicious insider threats. By helping you to mitigate your cybersecurity risks and secure the Internet of Medical Things (IoMT), your organization can overcome the cybersecurity skills shortage by improving operational efficiency with automation, while supporting a culture of regulatory compliance.

> With Exabeam, we're able to go back to the business and say with some intelligence that we are watching what the users are doing. We can see activity across the board, and we have something that's showing us, based on what this person normally does, that they could be an outlier, and that we should investigate. We can document our investigations and move on with other operational tasks."
>
> **- Kelsey-Seybold Clinic**

Key points

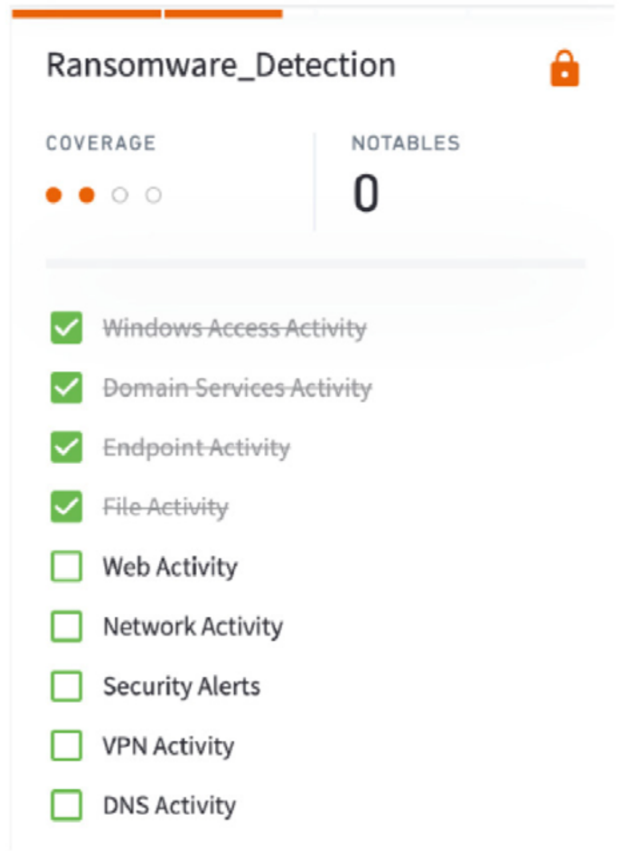
- Gain visibility into insider threats and indicators of compromise
- Secure electronic health record systems
- Monitor medical devices for unusual behavior
- Secure protected health information
- Meet HIPAA and data regulatory requirements
- Reduce time spent on security tasks by 51%

Mitigating cybersecurity risk

Many healthcare Security Operations Center (SOC) teams are burdened with unwieldy SIEMs to centralize and search security and network data. Effectively retrieving data from such tools is time-consuming, often requiring specialist coding skills, and results in cumbersome investigations, inhibiting the early detection of ransomware attacks and visibility into insider threats. The Exabeam Security Management Platform is designed to accurately detect high-risk, anomalous user and entity activity across your network, including EHR and cloud applications through behavioral analytics.

By analyzing user behavior, your security team is directed, in near real-time, to instances of a potentially malicious employee, or indicators of compromise such as early signs of a potential ransomware attack.

Ransomware, while unique from other malware, still exhibits several tell-tale signs which can point out an infection underway. By using machine learning to analyze users' day-to-day behavior in real-time for specific anomalies, it is possible to detect these early warning signs and stop a ransomware infection before it takes hold across your network.



Ransomware_Detection

COVERAGE ● ● ○ ○

NOTABLES 0

☑ ~~Windows Access Activity~~

☑ ~~Domain Services Activity~~

☑ ~~Endpoint Activity~~

☑ ~~File Activity~~

□ Web Activity

□ Network Activity

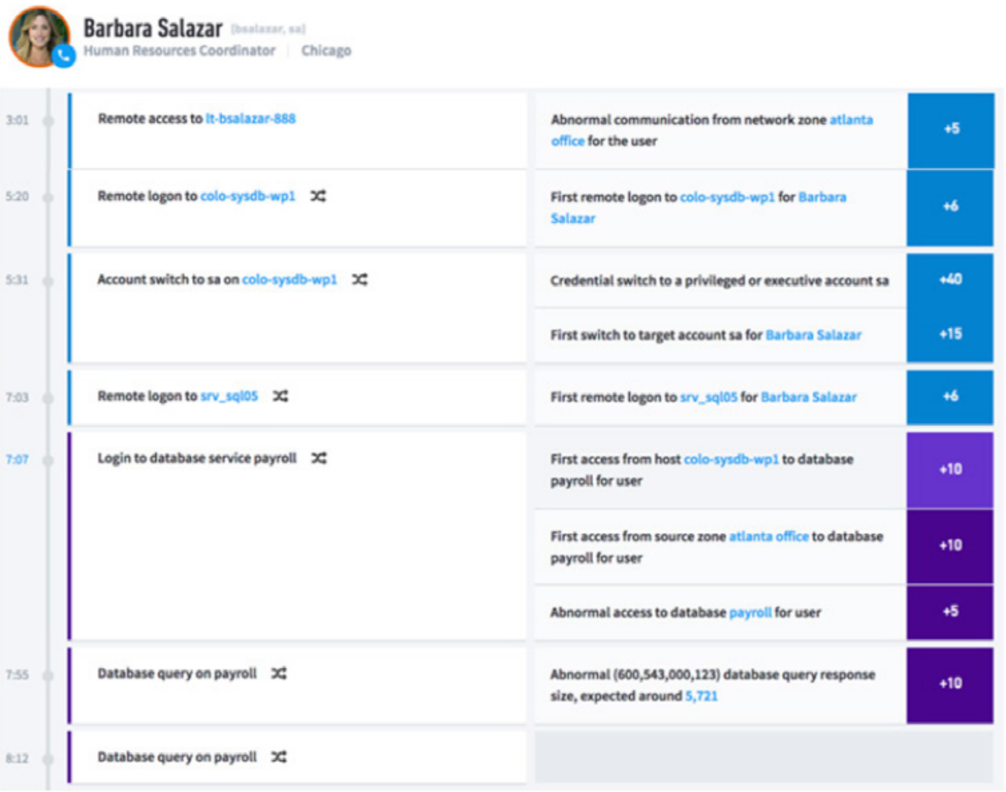
□ Security Alerts

□ VPN Activity

□ DNS Activity

Figure 01 Exabeam provides guidance on which logs are needed to ensure you have coverage where it matters most.

Your security team would view this analysis as an investigation attack chain or 'smart timeline,' as shown in Figure 2. Exabeam Smart Timelines provide all the information your analysts need to perform rapid investigations and responses. They include every action a user (or an attacker who has compromised a user's credentials) took during a specific session, including access to protected health information. Your team can see what preceded the security alert and what the employee did during their entire session. Each action is represented in the timeline with a risk score and includes surrounding context, such as if the alert maps to the MITRE ATT&CK framework.



Barbara Salazar [bsalazar, sa]
Human Resources Coordinator | Chicago

3:01	Remote access to lt-bsalazar-888	Abnormal communication from network zone atlanta office for the user	+5
5:20	Remote logon to colo-sysdb-wp1	First remote logon to colo-sysdb-wp1 for Barbara Salazar	+6
5:31	Account switch to sa on colo-sysdb-wp1	Credential switch to a privileged or executive account sa	+40
		First switch to target account sa for Barbara Salazar	+15
7:03	Remote logon to srv_sql05	First remote logon to srv_sql05 for Barbara Salazar	+6
7:07	Login to database service payroll	First access from host colo-sysdb-wp1 to database payroll for user	+10
		First access from source zone atlanta office to database payroll for user	+10
		Abnormal access to database payroll for user	+5
7:55	Database query on payroll	Abnormal (600,543,000,123) database query response size, expected around 5,721	+10
8:12	Database query on payroll		

Figure 02 Exabeam Smart Timelines show how each action taken by the user is attributed with a risk score, denoting how risky an individual's activity is to the organization.

Secure the Internet of Medical Things

With an estimated 30 billion[1] connected IoT and medical devices in the health sector, security professionals are working tirelessly to catalog, track, and secure IoMT devices connecting to the network and accessing, storing, and processing information. This includes legacy devices utilized beyond their shelf life and left to run on unsupported outdated operating systems. These devices can no longer be patched against vulnerabilities and often lack antivirus or personal firewall capabilities.

Depending on the sheer volume of medical devices within your organization, upgrading or replacing legacy devices can be time-consuming, prohibitively expensive, and ultimately impractical.

Exabeam monitors your medical devices and other high-risk assets for anomalous behavior, alerting your security team when the behavior patterns of a specific device falls outside a normal range and warrants further investigation.

With Exabeam, you can be assured that rules, alerts, and searches are performed against the complete dataset, regardless of modern network evolution. This provides your security team with full visibility across the ecosystem.

Addressing the skills shortage

SIEM solutions are renowned for being resource-intensive, requiring skilled analysts to run manual investigations, consuming huge amounts of time, and are prone to human error. Your ability to source, train, and retain proficient talent to run such solutions is expensive and hard to fulfill in a market already suffering from a significant skills gap.

Exabeam's modular solutions improve analyst productivity through natural language querying, context-enhanced parsing, and data presentation, providing security analysts the ability to quickly create new rules without the need for copious amounts of training.

[1] HIMSS Cyber Security Survey by Frost & Sullivan

Exabeam enables you to improve the operational efficiency of your team with automation throughout your workflow.

- Automated detection eliminates the need to maintain correlation rules.
- Automated triage identifies notable users and assigns a risk score to each action taken.
- Automated investigations, visualized through Smart Timelines, help analysts accurately detect insider threats faster.
- Automated response rounds out the workflow with pre-configured playbooks.

By automating the end-to-end workflow, Exabeam cuts the time spent on security tasks by 51%[2] and further supports your compliance requirements by removing the potential for human error borne out of historically manual processes.

Supporting a culture of regulatory compliance

Demonstrating the effectiveness of your compliance programs, including the prevention, detection, and resolution of instances of conduct violating government regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, local data privacy legislation laws, or health care program requirements, is challenging and time-consuming.

By harnessing hundreds of out-of-the-box compliance reports, which can be used to fulfill audit and regulatory requirements, and the ability to search and retrieve up to 10 years of historical logs in minutes, Exabeam significantly reduces the burden of compliance monitoring and the need for your security analysts to manually sift through disparate data sources for audit purposes.

[2] Ponemon Institute - Exabeam SIEM Productivity Study, July 2019

About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit exabeam.com.

exabeam™