exabeam

INDUSTRY SOLUTION BRIEF

# HEALTHCARE

## Mitigate your cyber security risks, support a culture of regulatory compliance, and overcome the cyber security skills shortage

**THE HEALTHCARE SECTOR, ALREADY A PRIME TARGET OF HACKERS AND ROGUE INSIDERS LOOKING TO ACCESS ELECTRONIC MEDICAL RECORDS (EMR) IS EVOLVING.**

Healthcare providers are embracing emerging technologies such as IoT, digital therapeutics, cloud hosting and AI, and in doing so, significantly increasing the complexity of safeguarding protected health information (PHI). While a growing reliance on sharing critical patient data across providers via electronic health records (EHR) is making the sector an attractive target for ransomware attacks.

Exabeam helps healthcare organizations address today's cyber security challenges.

Exabeam ingests log files from your security and IT applications, analyzes the logs, and applies behavioral analytics to detect early indicators of compromise and malicious insider threats. Exabeam helps you to mitigate your cyber security risks, secure the Internet of Medical Things (IoMT), overcome the cyber security skills shortage by improving operational efficiency with automation, and support 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 off of 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**

## MITIGATING CYBER SECURITY RISK

Many healthcare 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 resulting in cumbersome investigations that are 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.

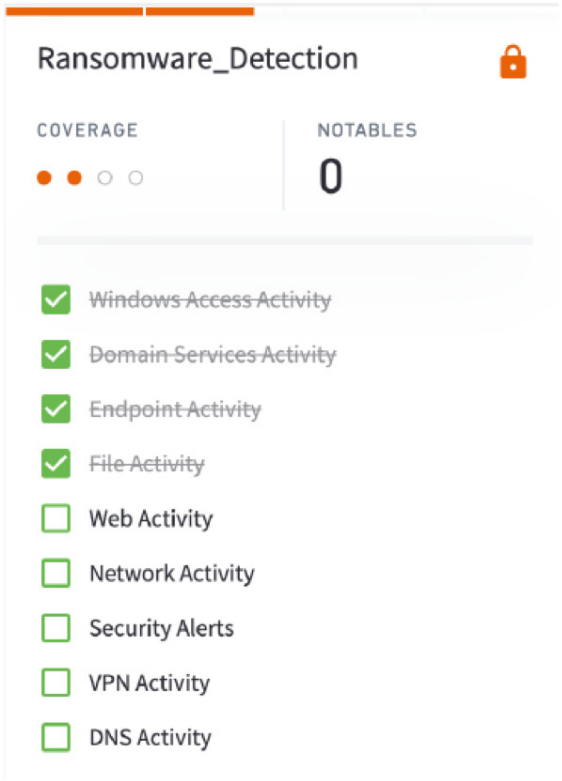


**FIGURE 1: EXABEAM PROVIDES GUIDANCE ON WHICH LOGS ARE NEEDED TO ENSURE YOU HAVE COVERAGE WHERE IT MATTERS MOST.**

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.

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 response. 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 next from the time they logged on to the time they logged off. 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.

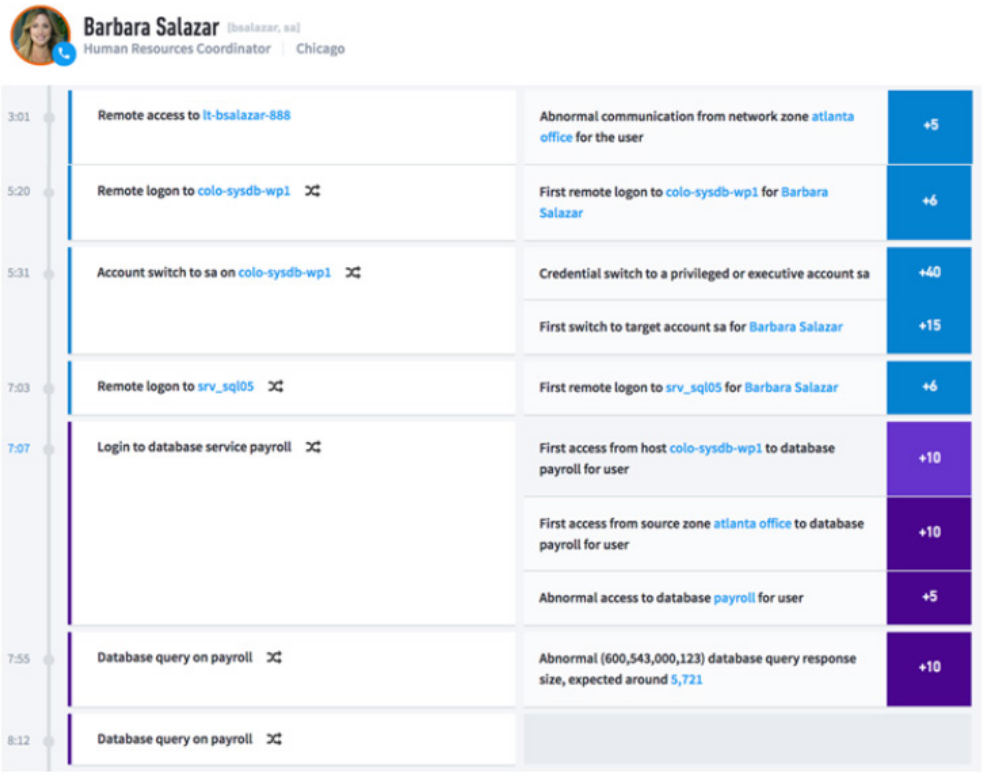


**FIGURE 2: EXABEAM SMART TIMELINE SHOWS HOW EACH ACTION TAKEN BY THE USER IS ATTRIBUTED WITH A RISK SCORE, DENOTING HOW RISKY AN INDIVIDUAL'S ACTIVITY IS TO THE ORGANIZATION.**

## SECURING 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 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. Your security team will have full visibility across the ecosystem.

[1] HIMSS CYBER SECURITY SURVEY BY FROST & SULLIVAN

## ADDRESSING THE SKILLS SHORTAGE

SIEM solutions are renowned for being resource intensive, requiring skilled analysts to run manual investigations that consume 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 that already suffers 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.

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 effectiveness of your compliance programs, including the prevention, detection and resolution of instances of conduct that do not conform to 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 to have your security analysts manually sifting through disparate data sources for audit purposes.

## 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 HIPPA and data regulatory requirements
- Reduce time spent on security tasks by 51%

[2] PONEMON INSTITUTE - EXABEAM SIEM PRODUCTIVITY STUDY, JULY 2019

exabeam

## ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with missed distributed attacks and unknown threats, manual investigations and remediation, or excessive storage fees. With the modular Exabeam Security Management Platform, analysts can use behavioral analytics to detect attacks, automate investigation and incident response, and reduce storage costs. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures. For more information, visit www.exabeam.com.



**TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.**