Retail
Secure the Omnichannel Experience, Protect Critical Data and Support a Culture of Regulatory Compliance

Rapid advancements in technology, increasingly high customer expectations and the rise of omnichannel commerce, trends that were already reshaping the retail sector prior to the COVID-19 pandemic are now firmly on the agenda as retailers look to streamline operations.

Acknowledging these trends, hackers have pivoted and are increasingly taking advantage of the opportunities digital retail channels provide. This has elevated the retail sector to the second most targeted industry1, as financially motivated threat actors continue to move away from POS attacks to targeting web application servers in their quest to obtain consumers personally identifiable information (PII), payment card data, financial data, loyalty program information and shopping history.

Your security team is facing an adversary who has ready access to compromised privileged credentials, often acquired through the dark web, and the ability to exploit web application vulnerabilities. Burdened with legacy tools and manual processes, your team’s investigations are time-consuming and often require specialist skills. The result is a lack of visibility into malicious activity, further exposing your organization in the event of an attack.

1 IBM X-Force Threat Intelligence Index 2020
Additionally it is challenging and time consuming to demonstrate the effectiveness of compliance programs, including the prevention, detection and resolution of instances of conduct that do not conform to government regulations such as GDPR, country specific data protection laws or industry regulations like the Payment Card Industry Data Security Standard (PCI DSS).

Exabeam helps retailers address these cybersecurity and compliance challenges.

**Exabeam solution for retail**

Exabeam ingests log files from all relevant sources. By analyzing the logs and applying behavioral analytics to detect adversaries’ techniques and malicious insider threats; Exabeam’s automated workflows help you to secure the omnichannel and multi-channel, protect critical data and support a culture of regulatory compliance.

**Mitigate Cyberattacks Targeting PII and Other Business Critical Data**

Exabeam solutions are designed to accurately detect high risk, anomalous user and entity activity across your network, including point of sale (POS) and cloud applications, through behavioral analytics.

By analyzing users’ day-to-day behavior for specific anomalies, your security team is directed, in near real time, to instances of a potentially malicious employee, or adversary behaviors such as early signs of a potential data exfiltration.

Your security team would view this analysis in a machine-built incident timeline as shown in figure 1. Exabeam Smart Timelines provide all the information your analysts need to perform rapid investigations. They include every action a user or an attacker, who has compromised a trusted user’s credentials took during a specific session, including access of PII, so your team can see what preceded the security alert and what the attacker 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.

![Smart Timeline](image)

**Figure 1** – This Smart Timeline event shows an instance of a potentially compromised insider, with the employees’ credentials seen remotely accessing a part of the network for the first time, before moving laterally across the network to access payroll data.
Secure the omnichannel and multi-channel

With Exabeam you can be assured that rules, alerts and searches are performed against the complete dataset, regardless of modern network evolution.

Exabeam monitors your mobile POS devices, in-store sensors, workstations, tablets on the corporate network, and other connected devices for anomalous behavior. Alerting your security team when the behavior patterns of a specific device fall outside a normal range and warrant further investigation, presenting this information via the same Smart Timelines as shown in Figure 1.

Support a culture of regulatory compliance

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.

Exabeam further supports your compliance requirements by automating workflows, removing the potential for human error borne out of historically manual processes tied to security incidents.

- Automated detection eliminates the need to manually 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.

Key points

- Gain visibility into insider threats and indicators of compromise
- Monitor devices for unusual behavior
- Secure Personally Identifiable Information (PII)
- Meet PCI DSS and GDPR data regulatory requirements
- Reduce time spent on security tasks by 51%

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Management platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit www.exabeam.com.

To learn more about how Exabeam can help you visit exabeam.com today.