exabeam

SOLUTION BRIEF

# EXABEAM AND ARMIS

## Extend SIEM visibility into Internet of Things (IoT) devices to unify IoT and IT device defense

## THE IT AND IOT SECURITY CHALLENGE:

Organizations are seeing an increasing number of attacks on unmanaged and Internet of Things (IoT) devices: smart TVs, security cameras, digital assistants, medical devices, manufacturing devices and more. At the same time, every year the number of unmanaged devices that make their way into the enterprise grows by nearly 31%. Although these connected devices help achieve greater productivity, they also create greater risk for organizations.

IoT devices are often innately vulnerable to attacks. This is because the vast majority of IoT devices lack built-in security, have default passwords, are hard or impossible to update, and businesses have little visibility or management processes for them. As a result, IoT devices are frequently seen as easy targets for attackers looking to access the corporate network. Attackers often use IoT devices as a foothold to access corporate data—an attacker might exploit a vulnerability or default password in an IoT device, like

ARMIS

"Exabeam recognizes the importance of expanding SIEM to IoT devices, and integrating with a leading IoT security vendor will provide significant value for organizations that manage infrastructure, industrial facilities, manufacturing and smart cities," commented Trevor Daughney, VP, Product Marketing, Exabeam. "By partnering with Armis, we help security teams improve their operational efficiency by automating the detection and investigation of attacks using IoT devices."

**TREVOR DAUGHNEY, VP, PRODUCT MARKETING, EXABEAM**

a camera, to then move laterally and gain access to the corporate network. As such, failing to monitor IoT devices, exposes organizations to increased risk of an attack.

With the interconnectedness of IoT, IT devices and corporate data, and the increase in targeted attacks on IoT devices, it is imperative for security teams to maintain an enterprise-wide security strategy that provides visibility across all devices accessing the corporate network.

## THE EXABEAM AND ARMIS SOLUTION

The Exabeam Security Management Platform and Armis® integration, allows for a single platform to monitor and identify malicious activity on IT and IoT devices. Leveraging the comprehensive asset inventory from Armis, Exabeam extends its visibility into managed and unmanaged IoT devices to help identify anomalies and enable security teams to more efficiently detect, prioritize and investigate threats across a larger breadth of endpoints.

Exabeam's behavior analysis solutions detect threats by identifying high risk, anomalous activity. This happens by using machine learning to baseline normal activity for all users and entities in an environment. Once a baseline is available, Exabeam can automatically detect deviations compared to that baseline and assign that activity a risk score. For all anomalies detected, Exabeam's machine-built incident timelines (Smart Timelines), stitch together both the normal and abnormal behavior for users and machines. These timelines include all information an analyst needs to perform a rapid investigation, including: normal and abnormal behavior, as well as the surrounding context, like what happened before and after an alert, or whether the alert maps to a MITRE tactic, technique, or procedure. With this joint solution, security analysts can easily follow attacks as they move between IoT devices and users, helping security analysts identify attacks before they continue to spread across the corporate network.

Key Integration Benefits:

- Enhance visibility across IT and IoT devices through monitoring and identifying malicious activity on managed and unmanaged devices from a single platform
- Prioritize alerts confidently by associating security alerts to users and entities
- Expedite investigations with automated, machine-built timelines and follow attacks as they move between users and devices


**ARMIS DATA IS INGESTED INTO EXABEAM FOR UEBA-BASED THREAT DETECTION, PRIORITIZATION, AND RAPID INVESTIGATION.**

## HOW IT WORKS

- Armis discovers and classifies all devices like smart TVs, security cameras, digital assistants, medical devices, manufacturing devices and more in your environment, on or off your network.
- Armis device data is sent to Exabeam to be aggregated and analyzed alongside data from other security products
- Exabeam baselines normal user and device activity using UEBA and then automatically detects deviations from those behavioral baselines.
- Risk is added to the relevant user or entity for each anomalous activity detected
- Threats are automatically prioritized by risk score to focus analyst efforts on high risk anomalies
- Exabeam stitches together Armis data with third party security solutions' data to create machine-built incident timelines, for rapid threat investigation

## TOP USE CASES

| USE CASE / CHALLENGES | SOLUTION DESCRIPTION | BENEFITS |
|---|---|---|
| Asset identification - Many organizations are unaware of unmanaged assets connecting to their network. | Armis discovers and classifies managed and unmanaged devices, whether they are on or off a corporate network. Exabeam then consolidates device data from Armis with security information events and logs from all security, identity, and contextual data sources in an environment. | Extend visibility into IoT and IT devices connecting to a corporate network. |
| User attribution - Without the ability to discover and classify assets in an environment, security analysts are unable to easily associate an asset to users and can miss a key part of an attack. | Exabeam ingests the device context from Armis to automatically identify users associated with devices and device type. | Better detection and visibility of advanced threats as security analysts can follow attacks that span between devices and users. |
| Alert prioritization - Analysts deal with an overwhelming volume of alerts from the numerous attacks happening across all devices. | Exabeam aggregates alerts and activity by user and entity, prioritizes them by risk score, and focuses analysts in the highest risk threats. | Increase SOC efficiency and effectiveness by focusing analyst efforts on the highest risk threats. |
| Advanced threat detection - Limiting visibility of entity behavior to a single security vendor for all systems, makes it difficult to detect advanced threats. | Exabeam uses machine learning to distinguish normal and abnormal behavior for a user, helping to identify risky activity—like that associated with credential compromise, insider threats, and privilege abuse— even if it has never been seen before. | Improve security posture and detect modern threats by augmenting IoT security with UEBA. |
| Lateral movement detection - Threats using lateral movement become difficult to detect due to changes in IP address, device, or credentials. | Patented host-to-IP-to-user mapping allows Exabeam to automatically follow attacks and attribute device activity back to the related user, regardless of how an attacker moves through the network. | Ensure sophisticated attacks involving lateral movement don't go undetected. |
| Incident investigation - Analysts must spend too much time investigating an attack to ensure effective post-incident remediation. | Exabeam Smart Timelines enable analysts to dramatically reduce time spent on incident investigations by automatically stitching together events before and after an alert to give the full picture of an attack. | Enhance analyst productivity by automating tedious investigations with machine-built timelines. |

exabeam

## ABOUT ARMIS

Armis® is the leading agentless, enterprise-class device security platform, designed to protect organizations from cyberthreats created by the onslaught of unmanaged and IoT devices. Fortune 1000 companies trust our real-time and continuous protection to see and control all managed, unmanaged, un-agentable and IoT devices – from traditional devices like laptops and smartphones to new smart devices like smart TVs, webcams, printers, HVAC systems, industrial control systems and PLCs, medical devices and more. Armis provides passive and unparalleled asset inventory, risk management, and detection & response. Core to our platform is the Armis Device Knowledgebase. It is the world's largest cloud-based, crowd-source device behavior knowledgebase tracking 230 millions devices, and growing. Armis tracks device behavior, connections, and history, letting us compare real-time device behavior to "known-good" baseline, identifying policy violations, misconfigurations, or abnormal behavior. When a device acts suspiciously or maliciously, Armis can disconnect or quarantine the device.

## 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 excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. 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.

Exabeam is continuously adding new integrations with best of breed security vendors to its offering. These integrations are included as part of the solution at no additional cost, supporting organizations as they expand their security ecosystem, and providing peace of mind that Exabeam integrations will support your unique environment as it evolves over time. For more information, visit www.exabeam.com.

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