exabeam

SOLUTION BRIEF

EXABEAM AND FORESCOUT

Detect Suspicious Network Access Attempts with Exabeam and Forescout

Unprecedented growth in "bring your own" (BYOD) and "internet of things" (IoT) devices accompanied by the adoption of SaaS applications and cloud services has resulted in tremendous pressure for today's IT teams. They must provide employees, vendors, and guests with reliable network access and address the increased security risk presented by numerous devices accessing the corporate network. Not only do they need the ability to discover and identify unknown devices on the network and their corresponding levels of compliance with access policies - they must also protect the business from damaging malware and targeted attacks that could be introduced by infected or non-compliant devices.

Network access control (NAC) solutions, like Forescout, are beneficial to security teams because they able to identify devices that attempt to connect to the network, enabling monitoring that does not require software agents or previous device knowledge. While NAC solutions use analytics to alert teams to suspicious network access attempts, evaluating network data anomalies in the context of other

FORESCOUT

solutions' security data and users' behavior allows your security team can appropriately evaluate and prioritize risks.

Exabeam's user and entity behavior analytics (UEBA) solution uses behavioral modelling of users, peer groups, and devices to automatically baseline normal activity. It then assigns a risk score to suspicious events and intelligently prioritize them for further evaluation – across all your security solutions of choice. The powerful combination of Exabeam and Forescout uses behavioral analysis to bridge the gap between NAC data and the data generated by other security point products so joint customers can more effectively detect, investigate, and respond to potential threats.

GET REAL-TIME VISIBILITY INTO MANAGED AND UNMANAGED DEVICES

The Exabeam-Forescout integration improves monitoring and real-time visibility over managed and unmanaged devices across the enterprise by collecting unlimited network access activity data such as device type, location, time of day, user identity and level of compliance and analyzing it in the context of baseline user and device behavior. Security teams can quickly and accurately identify anomalous behavior such as suspicious authentication attempts, unusual device access activity, or atypical network access that may denote a compromised insider or lateral network movement.

Exabeam collects NAC data from Forescout and automatically combines it with user and device activity data from other security solutions such as endpoint detection and response. By bringing together normal and abnormal behaviors for users and devices with their surrounding context, Exabeam's machine-built incident timelines automate the manual process of gathering evidence and assembling a timeline, resulting in significant time savings for incident investigation and threat hunting. And, incident response playbooks ensure timely and consistent action that reduces human error and further increases security team productivity.

INTEGRATION BENEFITS

COLLECT

Collect unlimited Forescout network access control activity data—such as device type, location, time of day, user identity and level of compliance —and eliminate unpredictable volume-based expenses with Exabeam's flat pricing model.

TOP USE CASES

- Identify compromised insider
- Detect lateral movement
- Monitor IoT and BYOD

DETECT

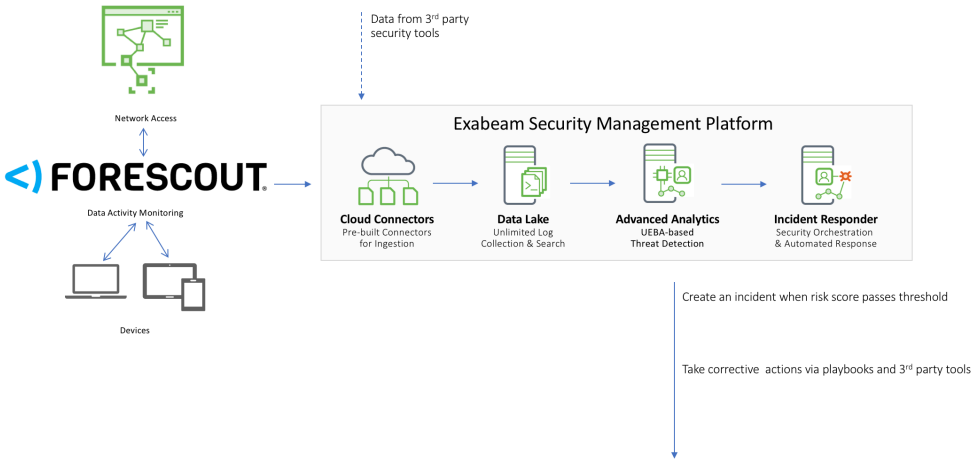
Exabeam's UEBA detects risks, such as a compromised insider, by analyzing anomalous NAC activity in the context of "normal" baseline behavior from a wide assortment of third-party security and infrastructure tools, such as endpoint detection and response solutions, even for attacks that have never been seen before. Anomalous activity is assigned a risk score; the more anomalous the activity, the higher the score, which aids security teams in rapidly detecting critical threats.

INVESTIGATE

Exabeam integrates Forescout data along with user and device information from other solutions, such as endpoint detection and response (EDR), to create machine-built timelines that allow security teams to accurately track lateral movement throughout the network. This dramatically reduces the time analysts spend investigating incidents by going from point solution to point solution to track. No longer does an analyst need to go between their NAC, EDR, and other security solutions to collect information on a suspicious device that accessed the network from an unexpected location at an unusual time of day - it is all presented in Exabeam Smart Timelines.

RESPOND

Reduce human error and response times with pre-built, out-of-the-box playbooks. Playbooks automate and standardize incident response "control" actions via third-party tools including enabling or disabling devices and quarantining endpoints or restricting user access based on anomalous activity.



EXABEAM AND FORESCOUT ENHANCE SECURITY PROFESSIONALS' DETECTION, INVESTIGATION AND RESPONSE TO SUSPICIOUS NETWORK ACCESS EVENTS.

HOW IT WORKS

- Forescout monitors endpoint attempts to connect to your network and informs Exabeam of the endpoint's status.
- Exabeam ingests the event, log, and real-time endpoint access and profile data from Forescout's API. Exabeam then parses, normalizes, and enriches the data with context from your environment.
- Exabeam baselines normal user activity using UEBA and then automatically detects deviations from those behavioral baselines such as an approved user introducing a new device to the network. This anomalous activity is assigned a risk score and added to the relevant user or device for each incident detected.
- Concurrently, Exabeam stitches together Forescout data with third-party security solutions' data to create machine-built incident timelines for rapid threat investigation.
- When user risk scores surpass a pre-defined risk threshold, your security team can use Exabeam's response playbooks to automatically enable or disable devices and quarantine or restrict user access using third-party tools.

> "The workforce revolution means that employees can work anytime, anywhere, and from any device or location. Exabeam and Forescout help companies meet the demands of the modern workforce with protected network access and enhanced threat detection."
>
> **CHRIS STEWART, SR. DIRECTOR OF BUSINESS DEVELOPMENT, EXABEAM**

exabeam

ABOUT FORESCOUT

Forescout Technologies, Inc. provides security at first sight. Forescout delivers device visibility and control to enable enterprises and government agencies to gain complete situational awareness of their environment and orchestrate action.

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 https://www.exabeam.com.

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