CrowdStrike Store

exabeam

CROWDSTRIKE

Data Sheet

EXABEAM: SECURITY MANAGEMENT PLATFORM

Detecting and investigating advanced attacks and insider threats with user and entity behavior analytics (UEBA)

CHALLENGE

Attackers are targeting endpoints more than ever, due to the proliferation of multiple devices, users and entities across the enterprise. While security teams can leverage endpoint telemetry as a rich data source to detect advanced attacks, they often lack the ability to link this activity to a user. Techniques such as lateral movement, credential compromise and privilege abuse are difficult to detect using endpoint data alone when access appears legitimate. And even after a threat is detected, analysts must spend precious time investigating an incident to understand the scope and severity before being able to confidently and completely take steps toward remediating the detected threat.

SOLUTION

Exabeam utilizes CrowdStrike® endpoint telemetry data, powered by the CrowdStrike Security Cloud and world-class AI, to attribute endpoint activity to a user and establish a behavioral baseline for normal activity. With user and entity behavior analytics (UEBA), Exabeam's modular Security Management Platform identifies anomalies to enable security teams to more efficiently detect, prioritize and investigate endpoint threats. Analysts can then use Exabeam's machine-built Smart Timelines to investigate user activity before, during and after an alert, drastically reducing the mean time to respond (MTTR).

KEY BENEFITS

Secures your enterprise against modern attacks by detecting advanced and insider threats with user and entity behavior analytics (UEBA)

Enables a more effective and efficient security operations center (SOC) by automatically prioritizing alerts based on risk to help guide analyst investigations

Enhances analyst productivity by automating investigations using machine-built timelines

BUSINESS VALUE

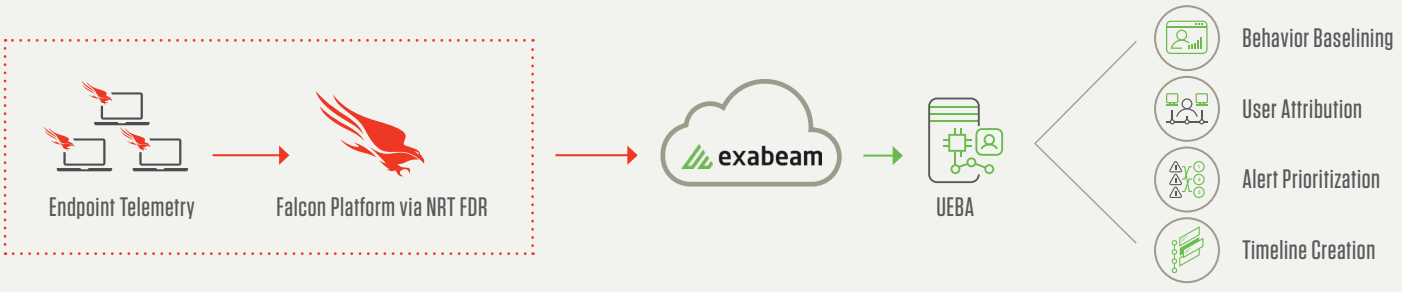
Use Case	Solution	Benefits
Advanced threat detection: Endpoint telemetry is unable to provide visibility into user behavior across all systems, making it difficult to detect advanced and insider threats.	Exabeam's UEBA uses machine learning to distinguish between normal and abnormal behavior for a user, helping to identify risky activity — like that associated with credential compromise, insider threats and privilege abuse — even if it has never been seen before.	By augmenting CrowdStrike's endpoint detection and response (EDR) capabilities with Exabeam's UEBA, organizations can improve their security posture and better detect modern threats.
Lateral movement detection: When threats use lateral movement, changes in IP addresses, devices or credentials become difficult to detect.	Patented host-to-IP mapping allows Exabeam to automatically follow attacks and attribute endpoint activity back to the related user, regardless of how an attacker moves through the network.	Exabeam ensures that sophisticated attacks involving lateral movement don't go undetected.
Alert prioritization: Analysts deal with an overwhelming volume of alerts from numerous attacks on endpoints.	Exabeam's UEBA aggregates alerts and activity by user and prioritizes them by risk score to help analysts focus on the highest-risk threats.	Exabeam increases SOC efficiency and effectiveness by quantifying threats to focus analyst efforts on those that are highest risk, based on user behavior.
Incident investigation: Analysts must spend too much time investigating an attack to ensure effective post-incident remediation.	Exabeam's Smart Timelines enable analysts to dramatically reduce time spent on incident investigations by automatically stitching together events before and after an alert to provide the full picture of an attack.	Exabeam enhances analyst productivity by automating tedious investigations with machine-built timelines, based on user sessions.

"CrowdStrike and Exabeam are uniquely positioned to jointly deliver an integrated, fully SaaS offering. This provides customers with the flexibility to solve complex security management problems while also adhering to cloud-first and cloud-only procurement mandates."

Trevor Daugney
VP of Product Marketing, Exabeam

TECHNICAL SOLUTION

How It Works



1. Collect endpoint telemetry data via a CrowdStrike agent
2. Send enriched telemetry data to Exabeam
3. Apply UEBA to detect, prioritize and investigate threats

KEY CAPABILITIES

- Behavioral baselining and anomaly detection with UEBA
- Risk-based alert prioritization
- Machine-built timelines showing user sessions with the complete attack chain of events

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. It helps security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51% 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.

For more information, visit **https://www.exabeam.com**

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**