Exabeam Ingester for CrowdStrike
Detect and investigate advanced attacks and insider threats with UEBA

Extending visibility: endpoint data and beyond
With threats constantly targeting end users, entities, and devices, endpoint detection and response (EDR) solutions are valuable tools for proactive threat detection, investigation, and protection. And, while endpoint data provides essential information about your security posture, it does not offer a complete picture for teams tasked with assessing all attack vectors. To understand the scope of an attack, security teams also must collect and contextually analyze information from a broad array of inputs, including servers, badge readers, and cloud-based services, to collect, detect, investigate, and respond to suspicious activity.

Exabeam user and entity behavior analytics (UEBA) solution uses behavioral modeling to automatically baseline normal activity and detect anomalous behaviors indicative of a threat — across all your security solutions of choice. The powerful combination of Exabeam and CrowdStrike uses endpoint visibility and behavioral analytics to bridge the gap between endpoint activity and other security and IT infrastructure tools, as part of a modern security management strategy.

“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.”

Chris Stewart, Sr. Director of Business Development, Exabeam
Accelerate incident analysis and response

Exabeam utilizes CrowdStrike EDR data from Falcon Data Replicator (FDR) to attribute endpoint activity to a user and establish a behavioral baseline for normal activity. With user and entity behavior analytics (UEBA), Exabeam identifies anomalies to enable security teams to more efficiently detect, prioritize and investigate endpoint threats. Analysts can then use machine-built Smart Timelines to investigate user activity before, during, and after an alert, drastically reducing mean time to respond (MTTR).

Key integration benefits:

- Secure the enterprise against modern attacks by accurately detecting advanced attacks and insider threats using user and entity behavior analytics (UEBA).
- Run a more effective and efficient SOC by automatically prioritizing alerts based on risk, to guide analyst investigations.
- Enhance analyst productivity by automating investigations using machine-built timelines.

How it works

- CrowdStrike monitors endpoint activity using its EDR solution and endpoint agents.
- Data is sent to CrowdStrike Falcon Data Replicator (FDR) in real-time.
- Exabeam ingests data from FDR via the Exabeam Ingestor for CrowdStrike connector.
- Exabeam baselines normal user and endpoint 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.
- Concurrently, Exabeam stitches together CrowdStrike data with third party security solutions’ data to create machine-built incident timelines, for rapid threat investigation.

Figure 01  CrowdStrike FDR Data is ingested into Exabeam UEBA-based threat detection, prioritization, and rapid investigation.
## Top use cases

<table>
<thead>
<tr>
<th>Use case / challenges</th>
<th>Solution Description</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced threat detection</strong></td>
<td>Endpoint telemetry is unable to provide visibility into user behavior across all systems, making it difficult to detect advanced and insider threats.</td>
<td>UEBA 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 EDR with UEBA.</td>
</tr>
<tr>
<td><strong>Lateral movement detection</strong></td>
<td>Threats using lateral movement become difficult to detect due to changes in IP address, device, or credentials.</td>
<td>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. Ensure sophisticated attacks involving lateral movement don’t go undetected.</td>
</tr>
<tr>
<td><strong>Alert prioritization</strong></td>
<td>Analysts deal with an overwhelming volume of alerts from the numerous attacks on endpoints.</td>
<td>Exabeam UEBA aggregates alerts and activity by user, prioritizes them by risk score, and focuses analysts in the highest risk threats. Increase SOC efficiency and effectiveness by quantifying focusing analyst efforts on the highest risk threats.</td>
</tr>
<tr>
<td><strong>Incident investigation</strong></td>
<td>Analysts spend too much time investigating an attack to ensure effective post-incident remediation.</td>
<td>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.</td>
</tr>
</tbody>
</table>
About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in Next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit exabeam.com.

About CrowdStrike

CrowdStrike (NASDAQ: CRWD) is a global cybersecurity leader that has redefined modern security with the world's most advanced cloud-native platform 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, the Falcon platform enables partners to rapidly build best-in-class integrations to deliver customer-focused solutions that provide scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

For more information, visit crowdstrike.com.