Exabeam and Trend Micro

Unified Endpoint and Network Security

The Insider Threat Challenge

Insider threats account for an average of 60% of all data breaches, as reported by multiple industry threat reports. With increasing corporate layoffs and challenging financial conditions, there is a heightened risk of disgruntled employees exfiltrating intellectual property (IP) and financial data. Detecting threats from negligent or malicious employees with valid credentials, or external attackers who have obtained valid credentials, is one of the most challenging tasks. To effectively detect, investigate, and respond to suspicious activities, it is essential to contextualize endpoint data with information from servers, identity management and directory tools, and cloud services.

Comprehensive Threat Detection and Response

The Exabeam Security Operations Platform integrates with Trend Micro Vision One™, using log data to attribute endpoint activity to users and establish a baseline for normal behavior. Anomalous activity is identified through user and entity behavior analytics (UEBA), which analyzes endpoint, IT, and security data and assesses risk. By stitching strong and weak signals together, Exabeam creates machine-built incident timelines, accelerating threat investigation and response to ensure successful security outcomes.

Integration Benefits

Accelerated Malware Detection

The AI-driven Exabeam Security Operations Platform, combined with Trend Vision One™, accelerates malware detection by consolidating alert data and detecting risks across endpoints, email, servers, cloud infrastructure, IT networking, and other security vendors. Security Analytics correlates events and uses machine learning (ML) to create threat timelines across users and devices, allowing analysts to trace the source of malware, monitor lateral movement and privilege escalation, and identify other exploits within the organization.

Increased Visibility of Credential-Based Attacks

Exabeam provides a comprehensive view of network activities by collecting endpoint telemetry for users and devices, establishing a behavioral baseline for normal activity. This baseline enables security analysts to quickly identify credential-based threats and detect potential data exfiltration, which may not be visible through pure endpoint detection alone. Legacy SIEM technology and security operations processes might take days or weeks of manual investigation to achieve similar results.

Lateral movement detection

Threats involving lateral movement are challenging to detect due to changes in IP addresses, devices, and credentials. Exabeam-patented host-to-IP mapping automatically follows attacks and attributes endpoint activity back to the related user, regardless of how the attacker moves through the network. Incorporating logs from physical IT sources, such as door access systems, helps solve insider threat cases by providing step-by-step chronological events in a timeline.

Top Use Cases

- Insider threat detection
- Credential-based attack identification
- Malware detection and response
- Lateral movement tracking

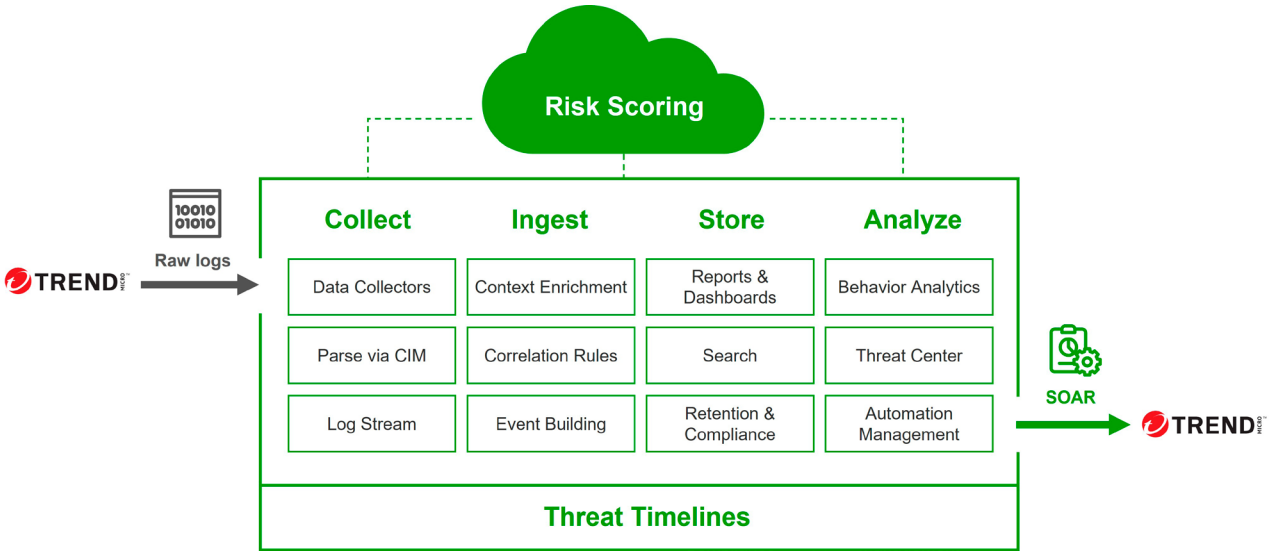

Figure 1.

Trend Micro data is ingested into Exabeam and enriched with context for combined UEBA and correlation-based incident detection and prioritization. Automation Management allows custom notification and webhooks back into Trend Micro and ITSM systems.

How It Works

Device monitoring: Trend Vision One identifies and monitors network-connected devices.

Data sharing: Log data is shared with Exabeam through a dedicated cloud collector.

Data normalization: The Common Information Model (CIM) transforms raw logs into normalized security events for easier parsing, storage, and reporting.

Behavioral baselines: Exabeam establishes normal user and endpoint activity baselines using UEBA and correlation rules, detecting deviations from these baselines as well as key detection events from Trend Micro.

Risk scoring: Risk is assigned to relevant users or entities for each detected anomaly, and cases are automatically created and prioritized by risk score.

Threat timelines: Exabeam integrates Trend Vision One data with other third-party security logs to create machine-built threat timelines for rapid investigation.

Case summaries: Exabeam Copilot provides simple case summaries for cross-team communication and interactive queries for detailed analysis.

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. www.TrendMicro.com.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation, and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.

exabeam

Detect
Defend
Defeat™

Get a demo →

Speak with an Expert →

Join a CTF →