exabeam

SOLUTION BRIEF

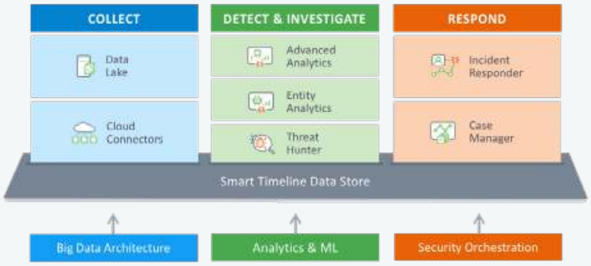
EXABEAM FOR CISCO SECURITY

Cisco offers a broad set of security solutions for protecting the network and enforcing control. These include leading products at the network, email, Web, DNS, identity, and other levels. Exabeam enhances these solutions through cross-product analytics and intelligent response. The resulting combination is a comprehensive and modern security fabric for protecting the corporate network, detecting modern threats, and responding effectively to prevent data and operational loss.

EXABEAM SECURITY MANAGEMENT PLATFORM

The Exabeam Security Management Platform provides organizations of all sizes with end-to-end detection, analytics, and response capabilities from a single security management and operations platform. It stores, indexes, and searches data via Exabeam, a modern log management system built on top of ElasticSearch to provide unlimited data ingestion at a predictable, cost effective price. The Exabeam SMP detects complex, multi-stage threats using the analytics capabilities of Exabeam Advanced Analytics; the world's most deployed User and Entity Behavior Analytics (UEBA) solution. Finally, The Exabeam SMP improves incident response efficiency with Exabeam Incident Responder, security orchestration and automation response (SOAR) solution.

These products with Cisco's market-leading security solutions to improve threat protection, detection and response within a corporate IT environment.



Integrations

Exabeam integrates with many Cisco security products, including:

- Advanced Malware Protection (AMP) for Endpoints
- Adaptive Security Appliance (ASA)
- AnyConnect
- Cloudlock
- Cloud Web Security
- Duo
- Email and Web Security Appliance (ESA, WSA)
- FirePower
- Identity Services Engine (ISE)
- Internetwork Operating System (IOS)
- Meraki
- Network Processing Engine (NPE)
- Threat Grid
- Umbrella
- Stealthwatch
- PxGrid

THREAT PROTECTION

Cisco solutions including Email and Web Security, Umbrella, ThreatGrid, ISE, Stealthwatch, and pxGrid all provide effective protection against threats entering the corporate environment.

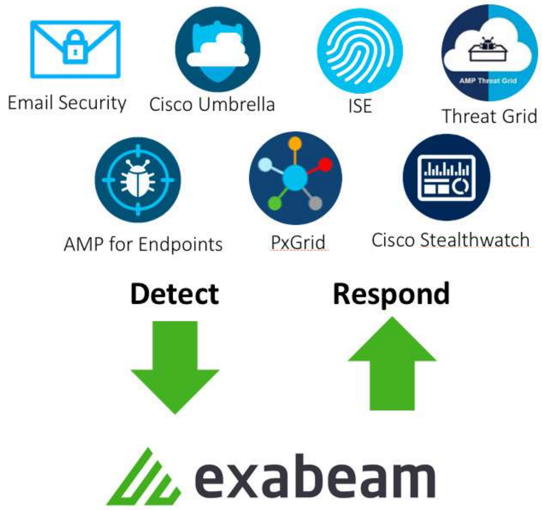
THREAT DETECTION

Exabeam provides advanced threat detection by integrating data from these Cisco solutions, as well as other security controls within a customer environment. Exabeam builds behavioral baselines for user and machine behavior using this integrated data and patented machine learning techniques. As a result, Exabeam can indicate user behavior that is both unusual and risky, quickly enough to take effective action.

For example, Exabeam can ingest log data from Cisco security products such as Cloudlock or Duo, and link that activity to other behavior, such as source code access in GitHub or customer data access in Salesforce. Exabeam can integrate network-level analytics data from Stealthwatch with user-level behavior to understand the full impact of a threat, leading to complete elimination of the attacker from the corporate network.

THREAT RESPONSE

Once an advanced threat, such as compromised account or malicious insider, is detected, Exabeam's automated investigation and response capabilities can enhance the control policies within Cisco products. For example, Exabeam can use data from Umbrella, CloudLock, Duo, AMP and more to automatically build an incident timeline, then adjust risk scores using reputation data from Cisco Umbrella Investigate.



An Exabeam playbook can send a suspected email attachment to Threat Grid for detonation and evaluation, then use the returned threat score to elevate response. The Exabeam playbook might then notify Cisco products directly to block an IP or domain, or a particular user or system. Integration to Cisco pxGrid enables Exabeam to take Rapid Threat Containment actions to investigate or mitigate threats utilizing the Cisco security and network infrastructure.

BETTER TOGETHER

The combination of Cisco's market-leading security enforcement and analytics products and Exabeam's most-deployed behavioral analytics solution brings a truly modern approach to cybersecurity. Together, the products increase perimeter and internal enforcement, detect new threats before they can cause damage, and provide automated response to shut down attacks and protect sensitive data, all while removing the alert fatigue that overwhelms hard-to-hire security analysts every day.

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