Trellix

SOLUTION BRIEF

User and entity behavior analytics through Trellix Helix

Manage risk with entity-based alert correlation

Key benefits

- **Prevent data loss and insider threats.** Monitor user data access and prevent sensitive data from leaving your organization.
- **Investigate faster.** Triage alerts with aggregated risk scores that are calculated per entity and based on alerts from rules, intel, and analytics.
- **Detect late-stage attacks.** Find the most critical threats by monitoring connected device behaviors.

Monitoring user and account behavior helps you detect internal and external threats. These might include insiders using privileged access to exfiltrate data, or external adversaries trying to gain a foothold in your environment with stolen credentials. More and more, companies are relying on security information and event management products that use machine learning to build detections customized to user behavior within their environment.

Trellix Helix offers alert-to-fix capabilities that use robust analytics and a deep understanding of user and adversary behavior. It's a native security detection and analytics module that uses machine learning to identify normal behavior and alert you to risky deviations that suggest insider threats, lateral movement, or attacks at the end stages of the cyberattack kill chain.

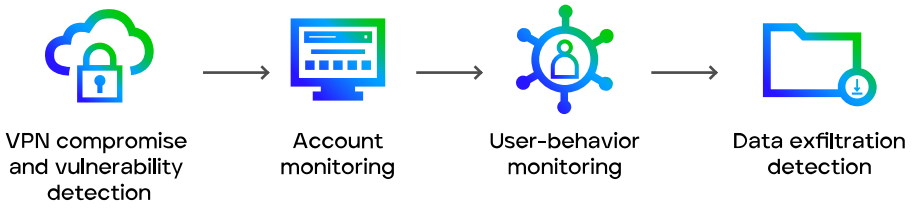

Figure 1. Operational interface for immediate situational awareness

Additional capabilities

Data theft detection

Detect late-stage attacks by identifying when data is being exfiltrated to suspicious destinations using advanced machine learning and statistical anomaly detection.

Compromised VPN account detection

Detect compromised behavior using models of login times and locations as well as login hostnames for users within a network.

User behavior monitoring

Detect insider threats and automatically generate reports to meet data compliance standards, including PCI and HIPAA.

Entity analytics and IoT monitoring

Monitor all devices across your network. Use behavioral baselining to detect unusual data flow destinations and login behaviors.

Credential abuse

Identify abnormal user account creations, privilege escalations, and geographically infeasible logins, which may indicate account abuse.

Misconfiguration detection

Automatically notify your analysts when security devices go silent. Detect third-party cloud misconfigurations that can be exploited by adversaries.

How to get Helix

Helix is available standalone or with the purchase of Trellix's subscription-based solutions. It works across all Trellix technologies and helps integrate your installed base of non-Trellix security products. As your organization grows and changes, Trellix solutions can be reconfigured, added, or upgraded without disrupting organizational operations.

To learn more, visit trellix.com.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com