Trellix

SOLUTION BRIEF

Analytics through Trellix Helix

Identify threats faster using robust security analytics

Key benefits

- **Identify threats faster.** Shorten the time it takes your analysts to find threats by helping them identify abnormal patterns.
- **Detect advanced, non-malware-based attacks.** Identify complex attacks that leverage stolen credentials or misconfiguration vulnerabilities with user, entity, and behavioral analytics (UEBA) and configuration monitoring.
- **Prevent insider threats and lateral network movement.** Track user behavior and network traffic patterns to identify attackers before they can exfiltrate data.

Making sense of security data has never been more challenging. Malicious users, compromised accounts, and cloud infrastructure vulnerabilities add complexity to the challenge of finding threats and remediating compromises. Organizations need automated, machine learning-driven detection that empowers security teams to find threats faster.

Trellix Helix integrates your security tools and augments them with next generation security information and event management (SIEM), orchestration, and threat intelligence capabilities to capture the untapped potential of security investments. The security analytics built into Helix enable security operations teams to prevent, detect, and respond to threats faster.

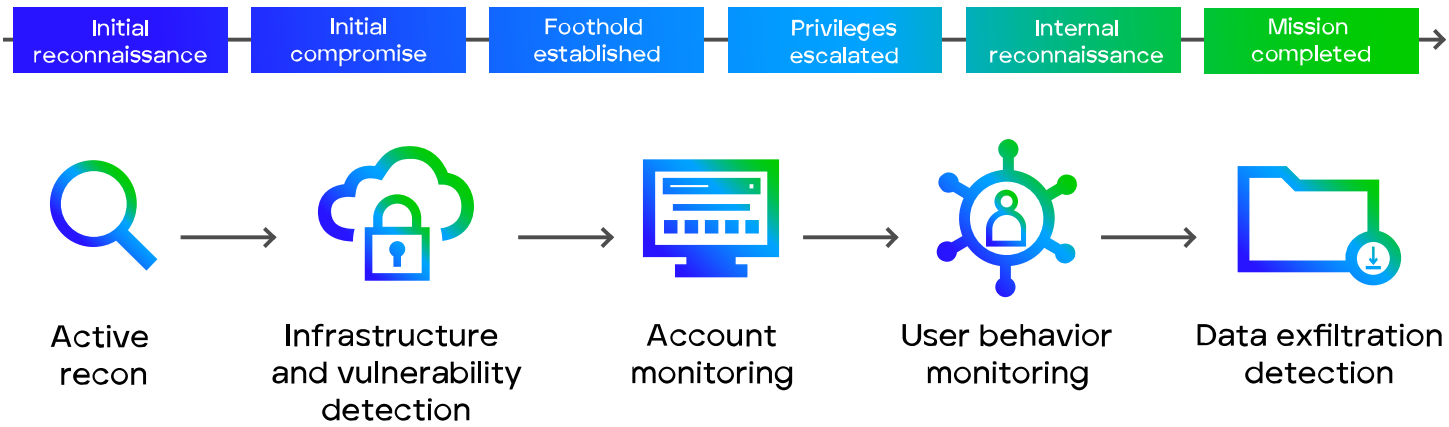

Figure 1. Operational interface for immediate situational awareness

Additional capabilities

User, entity, and behavioral analytics

Track users accessing data across your environment, detect behavioral anomalies, and identify insider threats.

Cloud analytics

Proactively identify and automatically prevent AWS and Azure cloud misconfigurations.

Machine learning

Build detection rules to identify threats unique to your environment using machine learning and dynamic modelling.

Credential abuse and compromised account detection

Monitor all your connected devices and networks. Detect abnormal access behavior or prevent covert attacker access.

Lateral network movement detection

Analyze inbound and outbound network traffic patterns, port scanning attempts, and VPN access.

Security augmentation

Enhance your native cloud security products and get greater access control and visibility with an integrated interface.

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