Trellix

DATA SHEET

Trellix Helix Enterprise

Highlights

- Detect advanced threats: Integrate over 600 Trellix and third-party security tools, and overlay contextual threat intelligence and behavioral analytics to deliver unparalleled situational awareness
- Minimize the impact of an incident: Accelerate response with security orchestration and workflow automation informed by frontline experience
- Gain visibility across all threat vectors and deployment types: Whether on premises or in the cloud, centralize security data and infrastructure with next-generation SIEM for complete visibility into threats and vulnerabilities
- Experience living security with Helix: Adapt and learn with a smart and unified security operations solution

Introduction

With new cyberthreats exposing vulnerabilities and forcing businesses to purchase more products and hire more talent, cybersecurity has never been so challenging. But instead of being reactive and operating in silos, which leads to more complexity, your business can take a comprehensive, proactive approach.

With the Trellix Helix SaaS security operations platform, your security operations—whether big or small—can build a holistic foundation that empowers your organization to take control of any incident, from detection to response.

Trellix Helix Enterprise 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. Designed by security experts for security experts, it empowers security teams to efficiently conduct primary functions, such as alert management, search, analysis, investigations, and reporting.

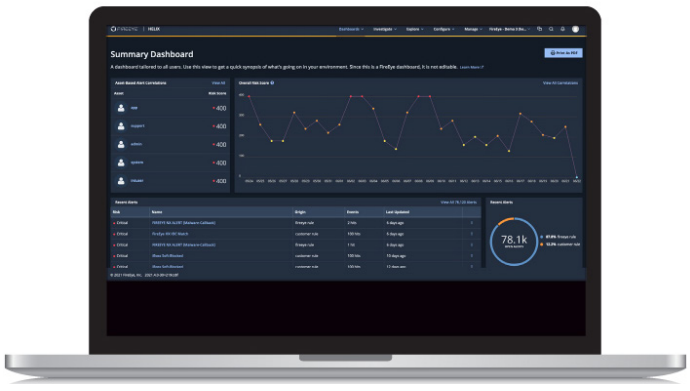

Figure 1. Operational interface for immediate situational awareness

What Helix Enterprise helps you do

Detect security incidents by correlating data from multiple tools

Make informed and efficient decisions with contextual threat intelligence

Centralize security data and infrastructure

Helix Enterprise add-on retention options

- **Quick search**
  Helix Enterprise allows for 7-day quick search. For security analysts that need additional days for monitoring and hunting, Helix Enterprise customers can upgrade to 16, 30, 60, or 90 days.
- **Long-term storage**
  Due to compliance reasons or incident response requirements, sometimes data must be stored longer than the 13 months provided by Helix Enterprise. We offer Helix Enterprise customers options for cold storage in 2-, 3-, 5-, or 7-year increments.

Threat intelligence

Detect, enrich, explore, and learn about the latest intelligence threats

Security orchestration and automation (SOAR)

Automate response with prebuilt playbooks created by frontline practitioners

Workflow management

Organize, assign, collaborate, and action steps through the investigative process with automated and manual workflows

Next-generation SIEM

Improve threat hunting and detection with advanced user behavior analytics and quick search capabilities

User and entity behavior analytics (UEBA)

Correlate alerts with machine learning to identify activities that suggest a high risk of insider threats, lateral movement, or final-stage attacks

Dashboards and reporting

Use built-in reports, including compliance visibility, and customize dashboards and widgets to visually aggregate, present, and explore the most important information

How to get Helix Enterprise

Helix Enterprise and add-ons are available for purchase through Trellix channels. It works across all Trellix technologies and integrates your installed base of third-party security products. As your organization grows and changes, Trellix solutions can be reconfigured, added, or upgraded without disrupting organizational operations.

Helix Detect is part of Trellix XDR. Learn more at trellix.com.

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