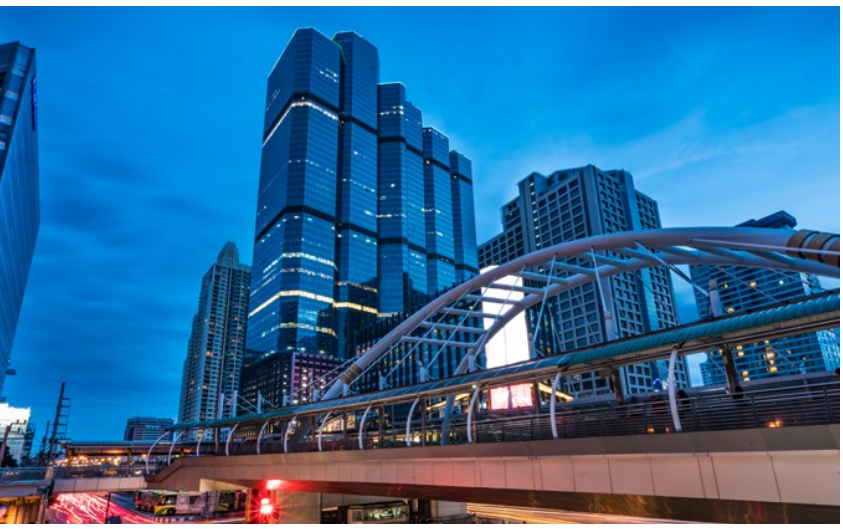
Trellix

DATA SHEET



Trellix Central Management System

Centralize device and intelligence management to correlate data across attack vectors

Key Benefits

- Offers integrated controls for multiple platform deployments
- Enables blended threat prevention through multivector correlation
- Provides a purpose-built platform that can be deployed quickly without requiring rules, policies, or tuning
- Displays an at-a-glance security dashboard that provides advanced targeted attack protection status
- Speeds reports and audits through a consolidated security event storehouse
- Streamlines management of multiple Trellix solutions and reduces time spent managing configurations, threat updates, and software upgrades

Overview

Trellix Central Management System consolidates the administration, reporting, and data sharing of Trellix products in one easy-to-deploy, network-based solution. Central Management enables real-time sharing of auto-generated threat intelligence to identify and block advanced attacks targeting your organization. It also provides centralized configuration, management, and reporting for several Trellix solutions.

Real-time sharing of local threat intelligence

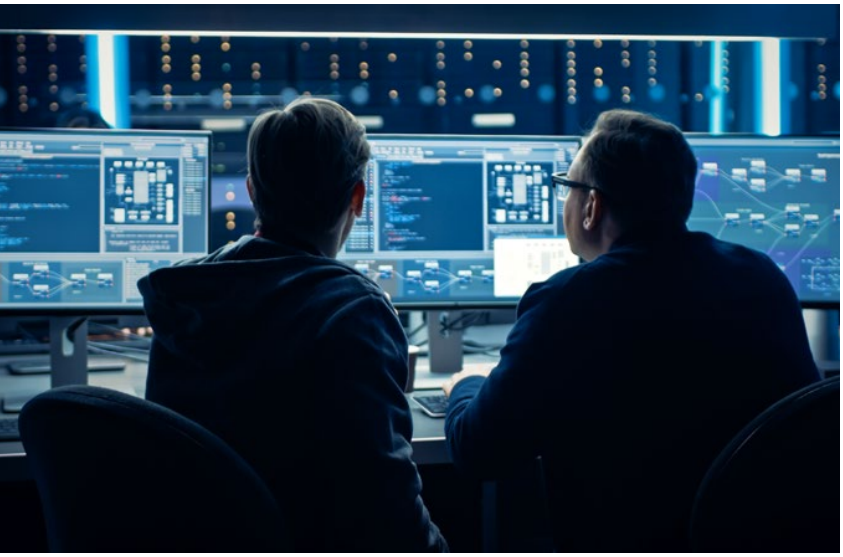
Trellix solutions generate real-time threat intelligence using the Trellix Multi-Vector Virtual Execution (MVX) engine. Central Management distributes that threat intelligence to multiple Trellix deployments, ensuring that each solution has the same dynamic protections against advanced attacks. Subscribers to the Trellix Dynamic Threat Intelligence (DTI) Cloud can use Central Management to centralize the sending and receiving of anonymized threat intelligence across Trellix solutions deployed at customers, technology partners, and service providers around the world.

At-a-glance security dashboard, plus drilldowns

Central Management consolidates activities and improves situational awareness with a unified security dashboard. The dashboard gives administrators a real-time view of the number of infected systems and lets them drill directly down to infection details to determine next steps.

Unified analysis of advanced targeted attacks

The analysis of blended threats, such as pinpointing a spear-phishing email used to distribute malicious URLs and correlating a perimeter alert to the endpoint, becomes possible. Security analysts can connect the dots of a blended attack to get the actionable intelligence they need to protect their organization against advanced targeted attacks.



Enterprise-class console and alerting

Central Management provides a web-based GUI console where administrators can view, search, and filter events and send real-time alert notifications via SMTP, SNMP, syslog, or HTTP POST. Administrators can filter by events, dates, or IP ranges and results are displayed to only show data based on the administrator's IT operational role. Notifications can also be sent to third-party SIEM tools. Administrators can click on an event link and connect seamlessly to specific Trellix solutions to view the network segment being protected.

Central configuration and platform upgrades

For efficient enterprise deployments, Central Management features dynamic configurations that can be determined centrally and then distributed across an organization accordingly. Administrators can remotely configure and view settings for one or more Trellix security solutions. Plus, all upgrades can be simultaneously deployed to all managed solutions, ensuring that they have the latest security capabilities.

Consolidated storehouse and detailed reporting

Larger and regulated organizations can use Central Management for efficient, consolidated reporting of security data. You can collect and store audit-relevant security events to meet long-term data retention requirements.

Trellix Central Management System offers convenient ways to search for and report on threats by name or type. Organizations can also view summaries such as the top infected hosts and malware and callback events, including geolocation details. Trending views can help show progress toward reducing the number of compromised systems.