Trellix

DATA SHEET

Trellix Enterprise Security Manager

Prioritize, investigate, respond

Key benefits

- **Intelligent**: Advanced analytics and rich context help you detect and prioritize threats.
- **Actionable**: Dynamic views of data give you the option to investigate, contain, remediate, and adapt to important alerts and patterns.
- **Integrated**: The solution monitors and analyzes data from a broad heterogeneous security infrastructure, offers two-way integration via open interfaces, and allows many first response actions to be automated.
- **Flexible deployment**: Supports hardware or virtual machine deployments to accommodate customers' requirements, preferences, and needs.

Overview

The most effective security starts with visibility into all activity on systems, networks, databases, applications, and the cloud. Security information and event management (SIEM) is the foundation of an effective security framework. Trellix Enterprise Security Manager, a core Trellix SIEM solution, delivers performance, actionable intelligence, and solution integration at the speed and scale required for your security organization. It allows your organization to quickly prioritize, investigate, and respond to hidden threats and meet compliance requirements.

Enterprise Security Manager delivers a real-time understanding of the world outside—threat data and reputation feeds—as well as a view of the systems, data, risks, and activities inside your enterprise. It offers your security team complete and correlated access to the content and context needed for fast, risk-based decisions, so you can optimize investments in a dynamic threat and operational landscape. This is critical for investigating "low-and-slow" attacks, searching for indicators of compromise (IoCs), or remediating audit findings.

To make threat and compliance management a core part of security operations, Enterprise Security Manager also provides integrated tools for configuration and change management, case management, and centralized policy management. You get everything you need to improve workflow and security operations team efficiency. Additionally, content packs offer prebuilt configurations for advanced security use cases that help simplify security operations.

Receive critical facts in minutes, not hours

Rapid access to long-term storage of event data is critical for investigating incidents, searching for evidence of advanced attacks, or attempting to remediate a failed compliance audit. All these activities require visibility into historical data and full access to the complete details of each specific event.

Enterprise Security Manager is a highly tuned solution that can collect, process, and correlate log events from multiple years with other data streams—including STIX-based threat intelligence feeds—at the speed you require. It can store billions of events and flows, keeping all information available for immediate ad hoc queries while retaining data for the long term for forensics, rules validation, and compliance. You can replicate data to multiple storage locations immediately to maintain business continuity.

Scale to your enterprise

Security operations teams require greater efficiency as they collect and explore increasingly large volumes of raw and parsed data from dynamic and distributed enterprise architectures. To overcome this challenge, Enterprise Security Manager uses an open and scalable data bus that was built specifically for high-volume data processing.

In addition, a highly scalable data architecture supports ingestion, management, and analysis to prevent compromises to data collection, searching, and retention. Such compromises can jeopardize investigations when critical data is not available later, when query response slows analysis, or when only partial searching is possible due to performance.

> Get flexible deployment options: Enterprise Security Manager is available for deployment within your data center as a hardware-based or VM-based solution.

Get context and content awareness

When contextual information is available—including threat data and reputation feeds, identity and access management systems, privacy solutions, or other supported systems—each event is enriched with that context. This enrichment delivers better understanding and accurate triage based on how network and security events correlate to asset attributes and real business processes and policies.

The scalability and performance of Enterprise Security Manager enable you to collect more information from more sources, including application content such as documents, transactions, and communications, providing deep forensic value. This information is heavily indexed, normalized, and correlated to help you detect a wide range of risks and threats.

Enhance threat interpretation

Whether it's network traffic, user activity, or application use, any variation from normal activity could indicate that a threat is imminent and that your data or infrastructure is at risk. Enterprise Security Manager calculates baseline activity for all collected information and provides prioritized alerts with the goal of discovering potential threats before they occur. At the same time, it analyzes that data for patterns that may indicate a larger threat. The solution also leverages contextual information and enriches each event with that context for a better understanding of how security events can impact real business processes.

Cyberthreat management dashboards offer enhanced real-time monitoring and understanding of emerging threats. Aggregate suspicious or confirmed threat information reported via STIX/TAXII, Trellix Advanced Threat Defense, and third-party web URLs and correlate it in near real time or historically (using the Backtrace feature) against event data. This provides your security team with a deeper understanding of threat propagation within your environment. This intelligence also enables your organization to align the right data with the right people to take action quickly and make smarter decisions.

Optimize security operations

The analyst-centric user experience of Enterprise Security Manager offers increased flexibility, ease of customization, and faster response to investigations. Streamlined workflows allow for timely and effective incident management. With fast and smart access to threat information, analysts with any level of expertise—from beginner to expert—will find it easier to prioritize, investigate, and respond to evolving threats.

Your security team will experience the difference right out of the box, with hundreds of reports, views, rules, and alerts ready to use immediately—and all easily customizable. Whether setting up baselining for understanding typical network usage or simply customizing alerts, the Enterprise Security Manager dashboard enables easy visualization, investigation, and reporting on the most relevant security information. Now, your organization can have comprehensive and correlated access to the data and context it needs to guide your business with confidence.

You can use Enterprise Security Manager content packs to simplify security operations with ready-to-go security use cases that offer fast access to advanced threat or compliance management capabilities. Content packs are prebuilt configurations for common security use cases thatprovide sets of rules, alarms, views, reports, variables, and watchlists. Many content packs provide prepackaged triggers for behaviors that may warrant additional scrutiny or automatic remediation.

Simplify compliance

By centralizing and automating compliance monitoring and reporting with Enterprise Security Manager, you eliminate time-consuming manual processes.

Additionally, integration with the Unified Compliance Framework (UCF) enables a "collect once, comply with many" methodology to meet compliance requirements and minimize audit efforts and expense. Support for the UCF brings efficiencies to compliance by normalizing the specifics of each regulation. This enables the single set of collected events to be easily mapped to individual regulations.

We also make compliance management easy and fast by including hundreds of prebuilt dashboards, comprehensive audit trails, and reports for more than 240 global regulations and control frameworks, including PCI DSS, HIPAA, NERC CIP, FISMA, GLBA, GPG13, J-SOX, and SOX. Beyond the extensive out-of-the-box support, all Enterprise Security Manager compliance reports, rules, and dashboards are fully customizable.

Connect your IT infrastructure

Integration across your security infrastructure delivers an unprecedented level of real-time visibility into your organization's security posture. Enterprise Security Manager can collect valuable data from hundreds of third-party security vendor devices, as well as threat intelligence feeds. Integration with Trellix Global Threat Intelligence brings in data from more than 100 million Trellix Labs global threat sensors, offering a constantly updated feed of known malicious IP addresses. The solution can also ingest threat information reported via STIX/ TAXII and third-party web URLs and take action based on analysis.

Enterprise Security Manager offers active integrations with dozens of complementary incident management and analytics solutions, including Trellix solutions and Trellix Security Innovation Alliance partner solutions.

For example, Trellix Threat Intelligence Exchange, based on endpoint monitoring, aggregates low-prevalence attacks leveraging global, third-party, and local threat intelligence. Threat Intelligence Exchange can also utilize other integrated products, such as Trellix Advanced Threat Defense, to further analyze and convict files.

Analysts also benefit from integration with Behavioral Analytics. This dedicated user and entity behavior analytics solution distills billions of security events down to hundreds of anomalies to produce a handful of prioritized threat leads. It allows analysts to discover unusual and high-risk security threats, often unidentifiable by other solutions. Similarly, Enterprise Security Manager integrates with Trellix EDR to help transform analysts into expert investigators and allow them to close more cases faster with higher confidence that they've determined the root cause.

Incident response teams and administrators can use Trellix Active Response to look for malicious zero-day files that lay dormant on systems, as well as active processes in memory. Active Response uses persistent collectors to continuously monitor your endpoints for specific IoCs, automatically alerting you if an IoC appears somewhere in your environment. Unlike standard security approaches, this combination provides your organization with a detailed, closed-loop workflow from discovery to containment and remediation.

Trellix delivers an integrated security system that empowers you to prevent and respond to emerging threats. We help you resolve more threats faster and with fewer resources. Our connected architecture and centralized management reduce complexity and improve operational efficiency across your entire security infrastructure. Trellix is committed to being your number one security partner, providing you with a complete set of integrated security capabilities.

To learn more about Trellix, visit trellix.com.

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

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.