Trellix

Revolutionary Threat Detection and Response

Trellix at a Glance

53K customers

185 countries

3.5K employees

30+ years of experience

Trellix Customers on the Global Fortune 100

100% of telecom companies

100% of top motor vehicle companies

86% of top financial companies

80% of top healthcare companies

86% of top energy companies

75% of U.S. Department of Defense agencies

Our Story

Trellix®, the trusted CISO ally, is transforming security operations with AI, automation, and analytics to power a resilient, thriving world.

A combination of the highly skilled McAfee Enterprise and FireEye teams, Trellix is dedicated to transforming the way organizations think about security by delivering market-leading solutions and best-in-class technology and expertise to keep customers everywhere safe and secure.

Today's dynamic world demands a holistic, integrated, and unified security ecosystem. Trellix's AI-powered security platform enables organizations to stay one step ahead of adversaries and adapt to new threats with faster detection, investigation, and remediation. The platform's open architecture and broadest set of native security controls across endpoint, email, network, cloud, and data security integrate with 500 third-party tools to create multi-vector, multi-vendor event correlation and context to speed up investigations.

Trellix, along with an extensive partner ecosystem, empowers over 50,000 business and government customers with responsibly architected security.

Our Customers

Trellix customers range from government agencies to businesses in all industries, including midsize organizations to the largest global enterprises. In fact, Trellix customers represent 80% of the Fortune Global 100. Our integrated platform allows organizations to achieve optimized security daily, enabling business while helping to reduce risk, drive compliance, and realize operational efficiencies.

Trellix Leadership

Vishal Rao,
Chief Executive Officer

James Denena,
EVP, Chief Financial Officer

Joe Gonyea,
EVP, Chief Legal Officer

Kim Anstett,
Chief Information Officer

Michael Alicea,
Chief Human Resources Officer

Ash Parikh,
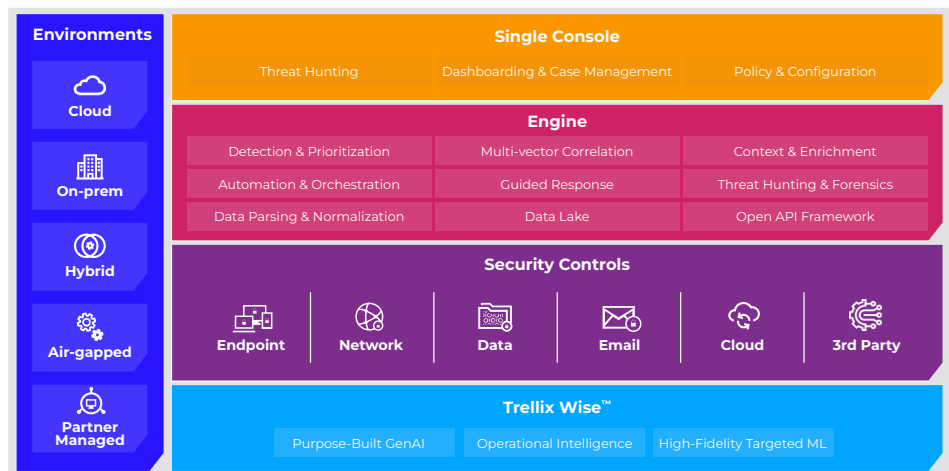Chief Marketing Officer

Gareth Maclachlan,
Chief Product Officer

Sean Morton,
SVP, Strategy and Services

The Trellix Platform

Comprehensive, open, and integrated, the Trellix AI-powered security platform strengthens an organization's security posture while streamlining security operations. The Trellix Platform integrates 500 third-party data sources as well as Trellix native endpoint, email, data, network, and cloud security controls. Multi-vector, multi-vendor detections accelerate detection, investigation, and response times with threat intelligence from over 53,000 Trellix customers, third parties, and data sources to contextualize and prioritize threats.

AI-Powered Trellix Platform

Environments	Single Console		
Cloud	Threat Hunting	Dashboarding & Case Management	Policy & Configuration
On-prem	**Engine**		
	Detection & Prioritization	Multi-vector Correlation	Context & Enrichment
	Automation & Orchestration	Guided Response	Threat Hunting & Forensics
Hybrid	Data Parsing & Normalization	Data Lake	Open API Framework
Air-gapped	**Security Controls**		
	Endpoint Network Data Email Cloud 3rd Party		
Partner Managed	**Trellix Wise™**		
	Purpose-Built GenAI Operational Intelligence High-Fidelity Targeted ML		

Trellix Wise™

Trellix Wise™ is a powerful set of traditional and Generative AI (GenAI) tools extending across the Trellix portfolio to deliver increased analyst efficiencies and improved threat prevention, detection, investigation, and remediation. The open Trellix Platform applies GenAI defenses to more of the environment and finds advanced threats with complex kill chains. Trellix Wise™ is built on the foundation of decades of AI modeling, analytics, and machine learning infused with continuous threat intelligence to provide customers with the leading GenAI powered security platform.

With Trellix Wise™, automatic alert investigation ensures alerts are quickly triaged, scoped, and assessed. It connects hundreds of security tools and can be implemented in on-premises and cloud environments.

Trellix Wise™ benefits include:

- **Increased threat detection and prevention** with AI-powered anomoly detection, predictive intelligence, and automated threat hunting.

- **Improved incident response** with automated incident containment, streamlined investigations, and summaries of events with risk scores and recommendations.

- **Enhanced security operations** with automated and accelerated workflows, security content creation, identifying attacks in real-time, and interacting with tools in natural language to reduce complexity and training requirements.

- **More detection and reduced risk** with the richest set of security telemetry powered by the modern XDR Platform while putting the human in the loop to receive AI-guided insights from the world's best practitioners.

Why Trellix?

Trellix is uniquely positioned to solve all your cybersecurity needs:

- **Open** - Seamless integration of 500 third-party sources out of the box with native security controls.

- **Comprehensive** - Broadest set of tightly integrated, best-of-breed security controls, threat intelligence, and XDR.

- **Hybrid** - Security for all your workloads across your organization, whether on-premises, cloud, or hybrid.

- **Data Analytics** - Data models are built on a foundation of decades of machine learning, artificial intelligence modeling and analytics infused with continuous threat intelligence.

- **Operational Threat Intelligence** - Insights gleaned from global customers combined with expert analysis from the Trellix Advanced Research Center, strategic intelligence partnerships, third parties, and open-source intelligence. With multiple petabytes of telemetry data, Trellix delivers real-time operational threat intelligence leveraging 68 billion queries a day on malicious activity from more than 100 million endpoints.

- **Multi-Vector -** Correlated, prioritized threat detection and data protection across multiple security controls and tools.

Trellix Advantages

Reduced time to value
Minimize time to detection and resolution from days and weeks to hours and minutes.

Reduced cost and complexity
Uplevel SOC resources, consolidate tools, and accelerate decision-making.

Reduced risk
Prioritizing threats and automated actions ensures accurate remediation.

The Trellix difference

Security vendors hold great responsibility, occupying a privileged position with access to the kernel, the heart of customers' systems. Trellix adheres to standard best practices to ensure all code deployed in the kernel is certified by Microsoft and not changed without the customer's approval and knowledge.

At Trellix, we employ a conservative approach anchored by three imperatives: **Transparency**, **Choice**, and **Responsibility**.

Transparency

Trellix customers have visibility into the way we package our code.

- Code sitting at the kernel level should be minimized to limit the potential for a cascading catastrophic system outage.

- We follow kernel driver best practices: separating content from executable code, ensuring all kernel drivers are certified and signed by Microsoft.

- This separation of security content and code ensures if there is ever a crash caused by an erroneous file, our program terminates independent of the operating system, and permits remote recovery.

Choice

Trellix customers have control over kernel-level changes.

- At Trellix, the choice of updates to kernel drivers is always in the hands of the customer.

- Trellix customers can determine if, when, and how to roll out updates to kernel drivers. Trellix will not override a customer's update distribution preferences or controls.

Responsibility

Trellix customers should be protected against people and process errors.

- Trellix follows rigorous processes to validate the quality and stability of both agent and security content updates before they are released, and has multiple controls to limit the impact if an error ever does occur.

- Trellix follows a phased rollout to prevent wide-scale impact, even for our daily security content.

- Trellix customers require us to provide high-quality releases across cloud, on-premises, air-gapped, and embedded environments at scale.

The Official Sponsor of the CISO

Trellix, the trusted CISO ally, is transforming security operations with AI, automation, and analytics.