

SOLUTION BRIEF

Trellix® Ransomware Detection and Response

Put ransomware nightmares to sleep

The Trellix Advantage

Comprehensive Security.

Trellix's open, AI-powered platform is integrated across endpoint, email, network, data, cloud, and security operations, lowering overall ransomware risk.

AI-powered Event Correlation and Investigation.

Automatic multivector, multivendor correlation and contextualization reduce mean time to detect. AI-guided investigation and response reduce mean time to investigate and respond.

Embedded Threat Intelligence.

Embedded in the platform and available as a service, threat intelligence uncovers and prioritizes threats.

Increased Cost Effectiveness.

Simplified security operations, higher productivity, and faster time to value lower overall costs.

The Challenge

Ransomware is pervasive, it's expensive, and today's security solutions aren't helping. According to our recent "[Mind of the CISO](#)" study, 93% of CISOs surveyed agree that ransomware is a serious concern, with 90% stating it has increased over the past twelve months.

Even with a well-staffed security operations center (SOC), cyber professionals say ransomware keeps them up at night. To face ransomware with confidence, you need visibility across your entire security ecosystem, so that you can detect, investigate, and respond to ransomware at every stage of the kill chain.

The Solution

Ransomware attacks are sophisticated, multistage campaigns that require visibility and control across each stage to disrupt them and avoid impact. Trellix provides critical coverage for all stages of a sophisticated ransomware campaign—from reconnaissance to recovery—offering unmatched visibility and reduced time to detection and response.

The [Trellix Advanced Research Center](#) analyzed more than 9,000 real-world ransomware attacks across 97 ransomware groups over several years to develop a kill chain model specific to ransomware. The resulting model is designed to help you combat ransomware while reducing time to value, cost, complexity, and overall risk.

The AI-powered [Trellix Security Platform](#) addresses each step of the ransomware kill chain. Its industry-leading security controls and embedded threat intelligence, paired with Trellix Services—which range from proactive threat hunting to managed detection and response to incident response and forensics—enable you to strengthen your ransomware defense posture and reduce risk.

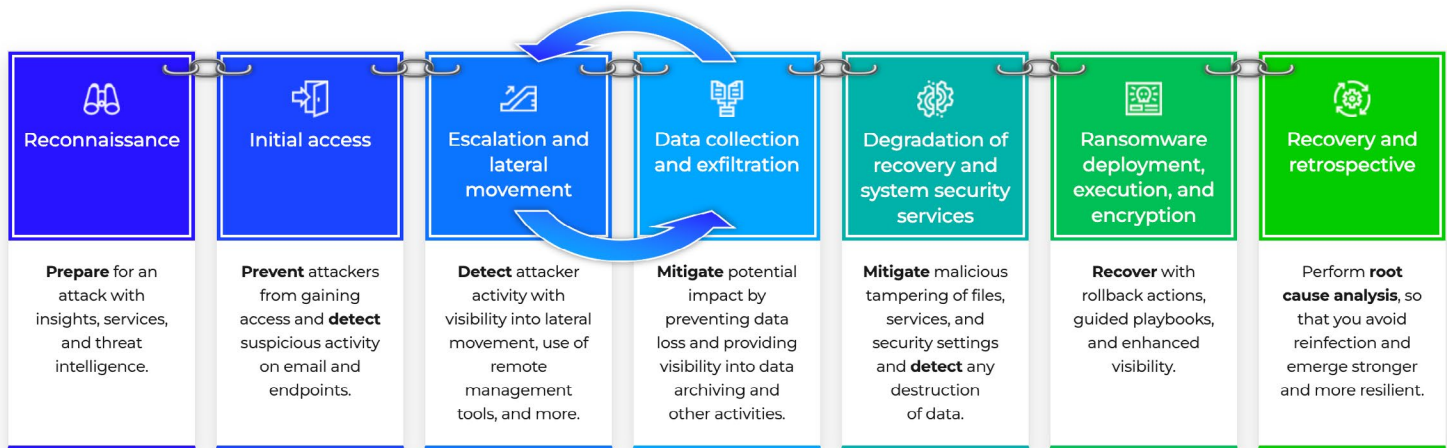


Figure 1. Trellix addresses each step of the ransomware kill chain.

With Trellix, you're able to:

- Minimize mean time to detect (MTTD) and respond (MTTR) to ransomware threats by uncovering subtle malicious activity through AI-powered curation and correlation of events across your ecosystem.
- Leverage rich threat intelligence from the Trellix Advanced Research Center to decrease false positives and ensure your SOC spends time fighting attackers instead of chasing alerts.
- Reduce costs and increase SOC analyst productivity with automatic prioritization, guided response, and rollback actions to detect and respond quickly.

Why Trellix

More than 50,000 organizations around the world trust Trellix to effectively detect and respond to threats.

Trellix's revolutionary threat detection and response is delivered by the Trellix Security Platform.

The Trellix Security Platform integrates over 1,000 third-party data sources, as well as Trellix native endpoint, email, data, network, and cloud security controls. Multivector, multivendor detections accelerate your detection, investigation, and response times with threat intelligence from over 50,000 Trellix customers, third parties, and data sources that contextualizes and prioritizes threats.

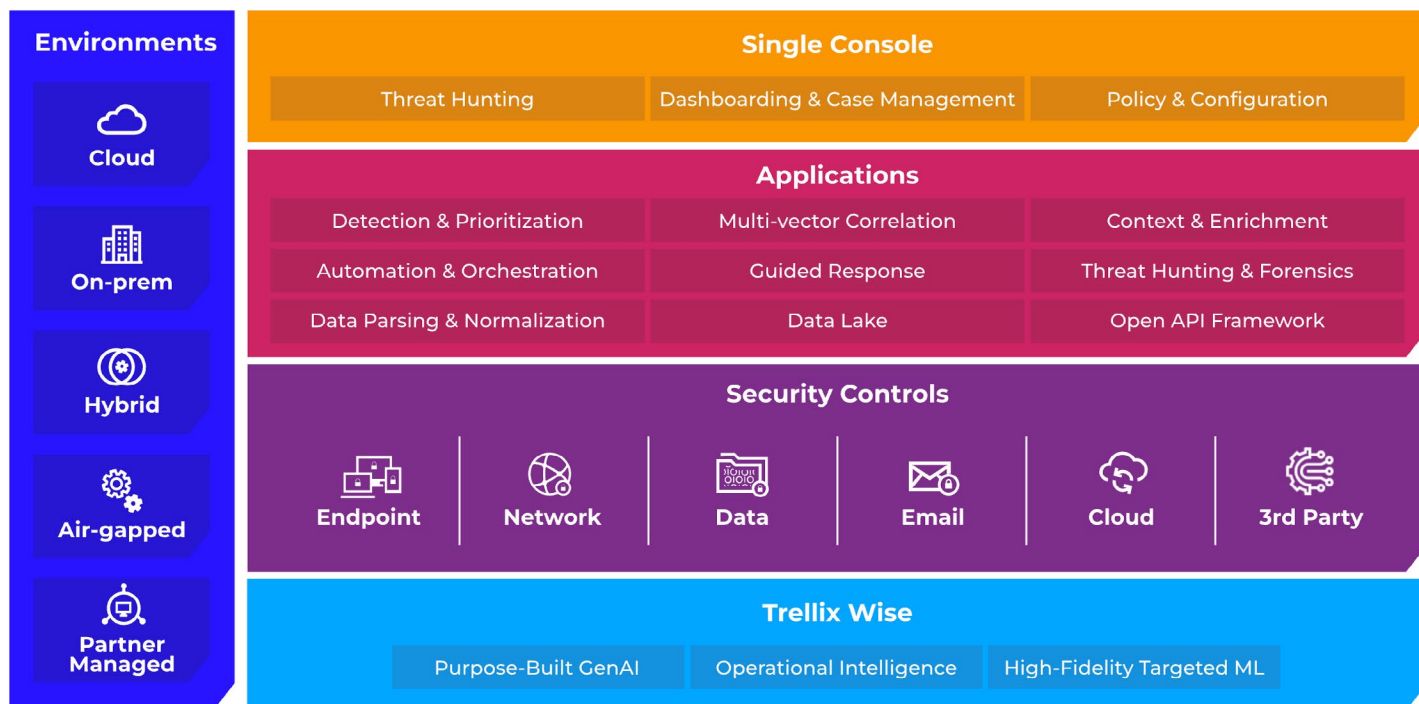


Figure 2. The Trellix Security Platform.

The Trellix Security Platform leverages AI and automation to provide faster, more insightful visibility and analysis, empowering analysts with intelligent attack mitigation.

[Request a demo.](#)

To learn more, visit trellix.com.