Trellix

SOLUTION BRIEF

Trellix Ransomware Detection and Response

Put ransomware nightmares to sleep

The Challenge

Ransomware is pervasive, it's expensive, and today's security solutions aren't helping.

Our recent Mind of the CISO survey found that more than half of all organizations use more than 20 security solutions. Yet only 34% of CISOs say they have what they need for their organizations to be cyber resilient.

Even with all these tools, ransomware keeps many cyber professionals 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, multi-stage 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.

Addressing each step of the ransomware kill chain, Trellix enables you to strengthen your ransomware defense posture and reduce risk with Trellix's AI-powered platform, XDR, industry-leading security controls, threat intelligence, and services.

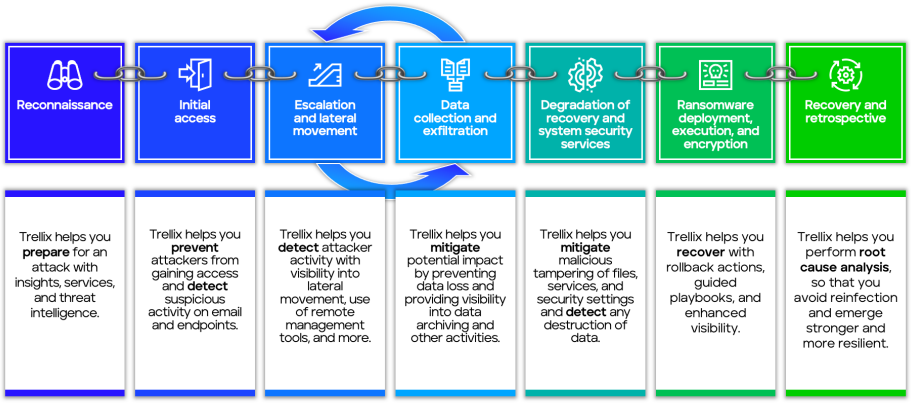

Figure 1. Trellix addresses each step of the ransomware kill chain.

The Trellix Advantage

Strengthen Posture
Reduce ransomware risk with the most comprehensive, integrated, and open, AI-powered platform leveraging over 1000+ integrations.

Minimize Time to Detect
Automatic correlation across multiple vectors ousts attackers in the earliest stages of a ransomware campaign reducing Mean Time to Detect (MTTD).

Reduce Time to Investigate and Respond
Reduce cost and increase productivity with AI-guided investigation, playbooks, and response. Cutting down Mean Time to Investigate (MTTI) and Mean Time to Respond (MTTR).

Empower Talent
Proactively shore up defenses by augmenting your team with Trellix Professional Services. Recover faster and ensure no attacker foothold is left behind with Trellix Incident Response.

Reduce Costs
Decreased MTTD, MTTI, and MTTR reduces cost in the Security Operations Center (SOC). Vendor consolidation decreases operational and technical expenses across the organization.

Enrich with Threat Intelligence
Threat intelligence is Infused across the Trellix portfolio and available as a service to uncover novel attacks and prioritize high-impact threats.

With Trellix, you're able to:

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

Why Trellix

40,000 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 Platform.

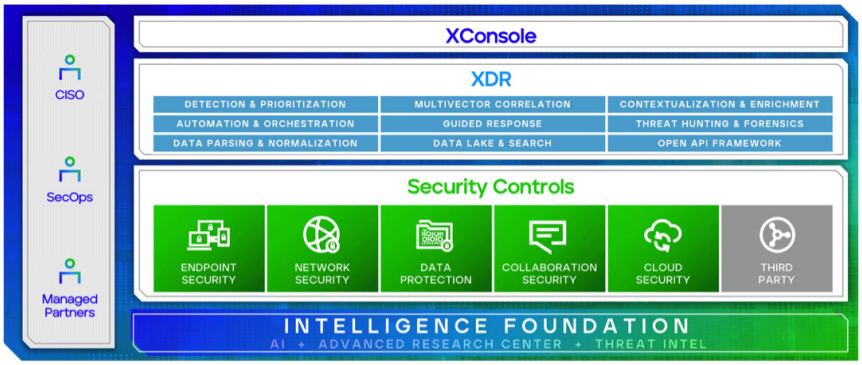

Figure 2. The Trellix Platform.

The Trellix Platform integrates over 1,000 third-party data sources as well as Trellix native endpoint, email, data, network, and cloud security controls. Multi-vector, multi-vendor detections accelerate your detection, investigation, and response times with threat intelligence from over 40,000 Trellix customers, third parties, and data sources that contextualizes and prioritizes threats. Trellix XDR (Extended Detection and Response) powers the entire platform, providing faster, more insightful visibility and analysis to create automation and empower analysts with intelligent attack mitigation.

To learn more, visit the Trellix Ransomware Detection and Response web page and schedule a demo.

Visit Trellix.com to learn more.

Trellix