Trellix

SOLUTION BRIEF

The Trellix XDR Platform

Create visibility, context, and insights to outpace attackers

If you are like most organizations today you have a collection of security controls for threat detection, investigation, and remediation. These tools, while useful, usually operate in silos allowing attackers to move more easily across your environment undetected. They also force security analysts to manually collect and comb through data, causing delays to threat investigations and remediation.

To reduce risk, detect sophisticated attacks across threat vectors and simplify processes for SOC teams, your organization needs Extended Detection and Response (XDR). XDR unites data from multiple tools, creating multi-vector detections, prioritized alerts for your SOC and opportunities for automation to boost efficiency.

Evaluating XDR solutions can be difficult as vendors vary in their capabilities, making it hard to understand whether a particular solution is a fit for your requirements. In this solution brief we will look at the unique capabilities of Trellix XDR and the challenges we can help you address.

Key Benefits

Minimize time to detection and resolution
Multi-vector, multi-vendor detections and real-time global insights reduce MTTD and MTTR from days to minutes, speeding time to value.

Uplevel SOC resources and consolidate tools
Provide fewer integration and pivot points for the SOC team, leverage flexible deployments, and integrate data from 1000 data sources to centralize visibility, reducing cost and complexity.

Prioritize threats and automate actions
Advanced analytics, guided investigation, and prioritized alerts allow analysts to build, manage, and track cases and automate responses with pre-built playbooks, reducing overall risk.

Why Choose the Trellix XDR Platform?

The Trellix XDR Platform is designed to deliver value rapidly for your unique environment:

1. **Data ingestion from Trellix best-of-breed native security controls -** Trellix native security controls include endpoint security, network security, data protection, email security, cloud security, and threat intelligence. Our technology stack helps reduce your vendor footprint and optimize the efficiency of your Security Operations with integrated, cross-environment correlations.
2. **Native and open integrations deliver faster time to value -** Hundreds of integrations, data from 1,000+ third-party sources, and over 2,000 rules are ready out of the box to plug into your current environment. Quickly create detection and event correlation, get context for investigations, trigger responses, and streamline SecOps workflows. Our commitment to an open ecosystem means the Trellix XDR Platform will grow with your business as your environment changes.
3. **Multi-vector, multi-vendor analysis -** The Trellix XDR Platform enables multi-vector (across different security controls), multi-vendor (across vendors) detections that help teams better prioritize threats.
4. **Unique Threat Intelligence extends contextualization from native and third-party sources -** Intelligence from over 40,000 customers is leveraged to inform and drive accurate detections. An elite team of Trellix security researchers regularly engage with law enforcement to take down dark web criminals and leverage their findings to inform Trellix detection capabilities.
5. **Built-in playbooks for SaaS-based and on-premises response and orchestration -** Bridge the skillset gap of various levels of analysts, standardize responses, and automate responses to save time for higher-priority triage tasks. The Trellix XDR Platform works with on-premises, cloud, and hybrid environments so you can improve visibility and create contextual insights no matter which model your organization prefers.

How does The Trellix XDR Platform work?

Everyone's XDR journey is different, but the main goal is the same - to grow your SecOps maturity. That's one reason why the analyst experience is at the heart of The Trellix XDR Platform. Visibility is made simple, and analysis streamlined by ingesting data from Trellix native security controls across endpoint, network, data, and cloud security. You can also leverage non-Trellix security controls using open integrations to collect data from over 1,000 third-party sources so your team can unlock and get more from the data you already own.

Detections are surfaced using correlation across vendors and multiple threat vectors to create context. Known and routine threats are eliminated with out-of-the-box automated responses. Actionable threat Intelligence for less common or new threats is created using insights from our Advanced Research Center and network of over 1 billion global sensors. Emerging, high-impact threats are detected and prioritized using AI-driven analytics that help teams stay ahead of the evolving threat landscape.

Attack mitigation is performed by several automation tools built specifically for security analysts—by security analysts. A library of pre-built, automated, and orchestrated response playbooks designed by experienced security researchers help teams accelerate threat response. Contextual answers

The Trellix Advantage

The Trellix XDR Platform helps you optimize security analyst efficiency with real-time threat detection, investigation, response, and hunting with the most effective, open and native platform. Implement XDR that is designed for your journey to the cloud, correlate across all your vectors and tools, detect threats in minutes, and respond lightning-fast with AI-guided intelligence.

Take the guesswork out of SecOps processes. Detect, respond, and remediate threats with confidence.

Visit www.trellix.com to learn more or to schedule a demonstration.

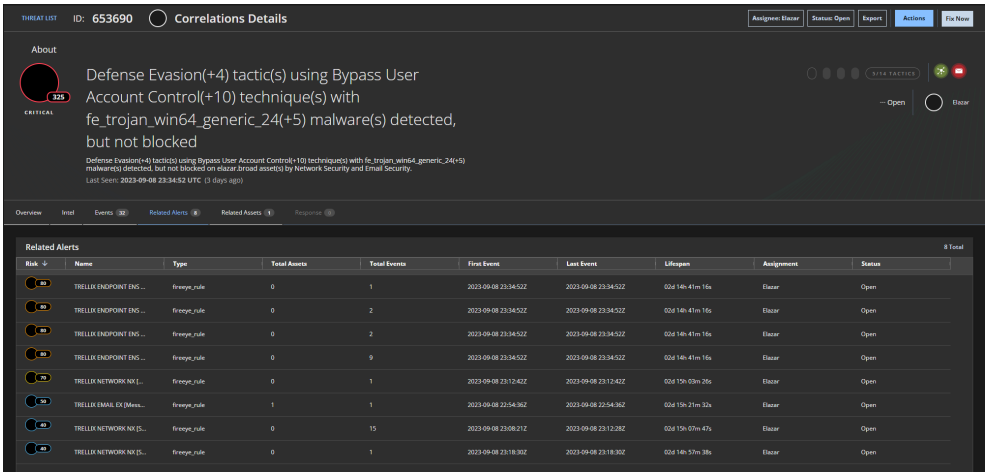

Figure 1. The Trellix XDR Platform creates correlations across multiple data sources.

Visit Trellix.com to learn more.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. 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, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.