Trellix

DATA SHEET

Trellix XDR

Comprehensive threat intelligence, powering stronger attack prevention

See more threats. Stop more attacks.

The constant barrage of incoming alerts continually challenges Security Operations Center (SOC) teams, tasked with identifying and prioritizing actual threats versus what is just noise. As a result, SOCs get overloaded and miss critical alerts. With fragmented security tools that don't work together, constrained security budgets and varying levels of security expertise, it is difficult for SOC teams to respond effectively. The overall impact is increased risk to the entire organization.

But what if you had a platform that provided a simplified yet comprehensive security operations experience that improved clarity across endpoints, cloud, network, email, and application-specific data? And what if that same platform delivered fast, accurate threat detection to stop attacks sooner, along with directed, automated responses for attack mitigation?

Welcome to Trellix XDR!

Key Benefits

- Reduces cyber risks:
  By providing improved visibility across the threat landscapes coupled with industry-leading threat detection technology, Trellix XDR stops cyberattacks before they happen.
- Optimizes SOC resources:
  Addressing today's scrutinized security budgets and the scarcity of experienced security talent, Trellix XDR identifies and prioritizes critical alerts and provides automated guidance and responses for mitigating attacks, reducing the manual strain on SOC teams.
- Simplifies SOC operations:
  Detect and prioritize emerging high-impact threats leveraging real-time, automation security analytics and accelerate threat investigations with an intuitive, directed solution built for security analysts by security analysts.
- Reduces SOC costs:
  SOC costs have exploded with the proliferation of disconnected, ineffective security tools, each with its acquisition, operations, and maintenance costs, not to mention staff.

Stay ahead of threats with a living security ecosystem

Trellix XDR (eXtended Detection and Response) streamlines the security operations experience and delivers effective extended threat detection and response to keep organizations safe. CISOs and security operations teams rely on Trellix XDR for insightful visibility and analysis, fast and accurate detection, immediate automated responses, and attack mitigation. The platform eliminates blind spots using native and open APIs to integrate with existing security controls seamlessly, detects and prioritizes emerging high-impact threats leveraging real-time, ML and AI-driven security analytics and modernizes threat investigations with a guided solution built for security analysts by security analysts.

The EDR to XDR evolution

As attack frameworks become more sophisticated, threat mitigation tools need to evolve to keep pace. XDR builds on Endpoint Detection and Response (EDR) threat prevention functionality by adding exponentially incremental telemetry for expanded detection and response. By synthesizing information from an expanded array of threat vectors beyond the endpoint, including email, identity, network, applications, data lakes and the cloud, Trellix delivers faster, more accurate threat identification and recovery.

Insightful Visibility and Simplified Analysis

Trellix XDR provides real-time adversarial insights leveraging threat intelligence from 40,000 organizations worldwide and the proven expertise of Trellix Advanced Research Center. It also eliminates blind spots across your security infrastructure by correlating attack alerts and telemetry from over 1,000 data sources in the proven flexible and native XDR ecosystem. In addition, existing security controls can seamlessly integrate with Trellix and 3rd party providers.

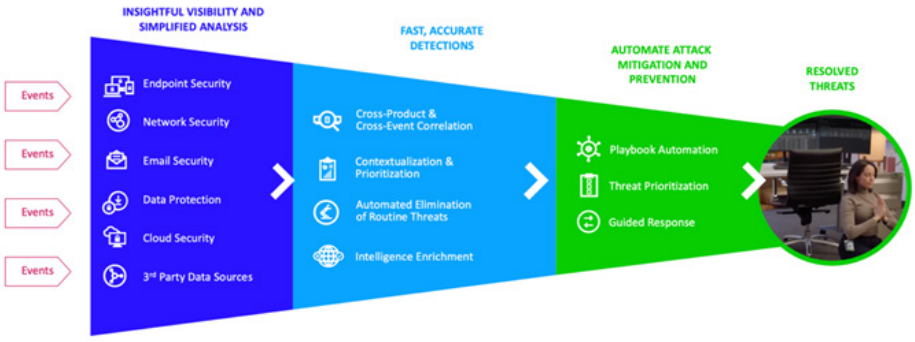

Figure 1: The Trellix XDR solution delivers a simplified and insightful SecOps experience to rapidly stop attacks

Fast, Accurate Threat Detection

Trellix XDR detects and prioritizes high-impact threats in real-time using machine learning (ML) and artificial intelligence-driven security analytics. Users also get actionable intelligence that adjusts for high-probability threats and responds to existing attacks. As a result, Trellix learns and adapts at the speed of threat actors with immediate, meaningful intelligence.

Automated Attack Mitigation and Prevention

The platform also streamlines threat investigations with an intuitive, directed solution built for security analysts by security analysts. Incident response is enriched with automated, guided, and contextual answers in continuous near real-time. And threat responses are accelerated using a library of pre-built and customizable automated response playbooks.

To learn more about Trellix, visit trellix.com.