Trend Micro™

XDR FOR USERS

Detection and response capabilities across email and endpoints

Organizations today face an onslaught of new and stealthy threats that are constantly evolving to bypass existing security measures. Having advanced detection and response capabilities, in addition to advanced protection, is essential to eliminate or minimize the impact of threats that do make it through defenses. Endpoint detection and response (EDR) is a great tool to detect threats that have landed on an endpoint, investigate the root cause, and mitigate the impact–but with its targeted focus on endpoints, EDR can't see or influence important parts of the attack path. For example, while EDR can identify that a threat came into the organization via email, it can't offer key details on the scope of compromised accounts and hence can't remove or stop the spread of the threat. Given that 90% of malware incidents come from email , combining email with endpoint detection and response is a powerful capability.

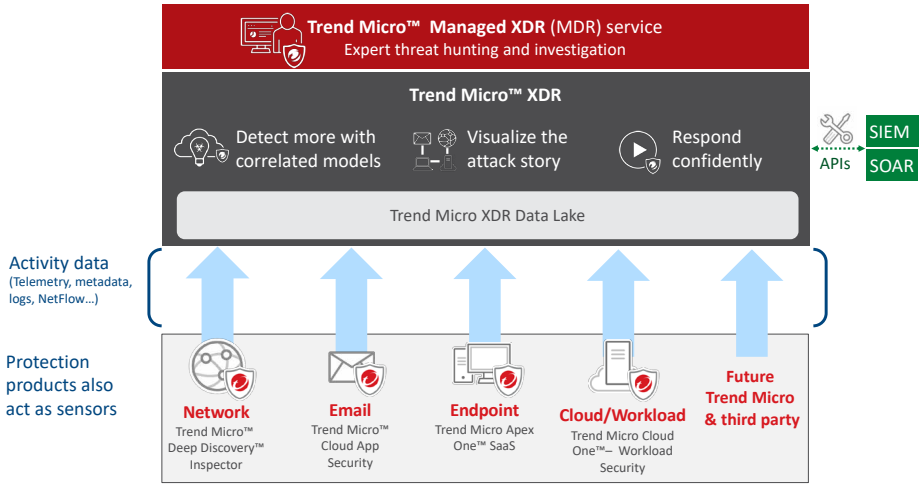
TREND MICRO™ XDR FOR USERS

Trend Micro™ XDR for Users is a complete software-as-a-service (SaaS) offering that includes protection, detection, and response across email and endpoints and through Trend Micro Apex One™ and Trend Micro™ Cloud App Security solutions. It also includes Trend Micro™ XDR for correlated email and endpoint detection using security analytics, automatic sweeping for Indicators of Compromise (IoC) using Trend Micro threat intelligence, central investigation and response, and proactive threat hunting. With XDR for Users, customers can respond more effectively to threats, minimizing the severity and scope of a potential breach.

Protection Points

- Microsoft® Windows®
- Mac
- Microsoft 365® (email, Microsoft® OneDrive® for Business, Microsoft® SharePoint® Online, Microsoft® Teams®)
- Google G Suite™ (email, Google Drive™)

FORRESTER®
WAVE LEADER 2020
Enterprise Detection And Response



[1] 2019 Data Breach Investigations Report, Verizon 2020

ADVANCED THREAT PROTECTION

- Apex One leverages a blend of modern threat techniques to provide the broadest protection against all types of threats. It offers highly-tuned endpoint security that maximizes performance and effectiveness.
- Cloud App Security catches millions of threats not found by upstream protection from Microsoft 365, G Suite or third-party email gateway services. Using APIs, it integrates in minutes with cloud email and file sharing platforms to add advance malware and phishing detection—including specialized protection against credential phishing and BEC impersonation attacks.
- Strong endpoint and email threat protection reduces the number of threats that get through in the first place, resulting in less events in which to investigate and respond.

CONSOLIDATED DETECTION, INVESTIGATION, AND RESPONSE

- XDR for Users connects the dots across security layers to provide more insightful investigations and quicker response to endpoint and phishing incidents.
- Endpoint and email activity data (i.e. endpoint telemetry, email metadata, etc.) and detection logs are sent to the Trend Micro XDR data lake for attack discovery and analysis in the Trend Micro XDR platform.

CORRELATED DETECTION

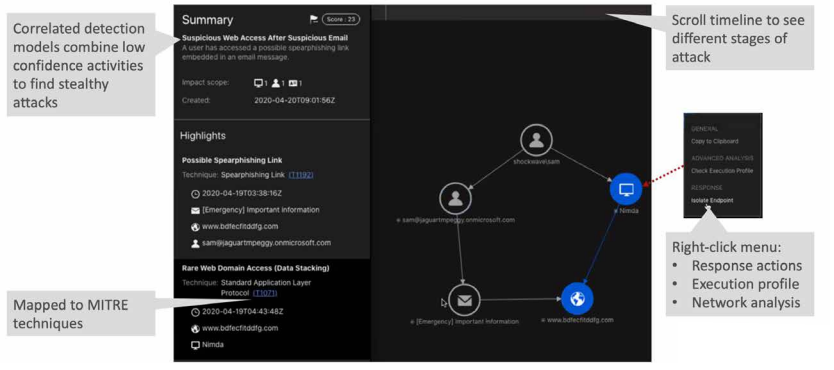
Built-in security analytics combined with global threat intelligence to detect more:

- XDR analytics can automatically tie together a series of lower-confidence activities into a higher-confidence event, surfacing fewer, prioritized alerts for action (i.e. a suspected phishing email is followed by an endpoint accessing a rare web domain).
- Correlate threat and detection data from your environment with Trend Micro's global threat intelligence in the Trend Micro™ Smart Protection Network™ for richer, more meaningful alerts.
- More context with mapping to the MITRE ATT&CK framework means faster detection and higher fidelity alerts.

INTEGRATED INVESTIGATION AND RESPONSE

One platform to respond faster with less resources:

- One place for investigations to quickly visualize the entire chain of events across security layers or to drill down into an execution profile.
- In seconds, determine the impact of a phishing attack as XDR automatically sweeps mailboxes to find other affected users.
- One location to respond using containment actions for both email and endpoint.



Trend Micro XDR: One place for attack discovery, investigation, and response

Key Protection Capabilities

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- Vulnerability protection
- Application control
- Data loss prevention (DLP)
- Device control
- Sandbox and breach detection integration
- Inbound and internal phishing protection
- Credential phishing detection with computer vision
- Business Email Compromise (BEC) impersonation detection with writing style

TREND MICRO XDR PLATFORM

XDR for Users includes the Trend Micro XDR platform for detection and response. XDR collects and automatically correlates data across multiple security layers; email, endpoints, servers, cloud workloads, and networks. Using advanced security analytics, it detects and tracks attackers across these layers so security teams can quickly visualize the story of an attack and respond more quickly and confidently.

TREND MICRO™ MANAGED XDR SERVICE

Threat hunting and investigations by Trend Micro threat experts

- With Managed XDR, customers can get the advantages of XDR; leveraging the resources and knowledge of Trend Micro security experts who are skilled in investigating advanced threats.
- Provides 24/7 alert monitoring, alert prioritization, investigation, and threat hunting services to Trend Micro customers as a managed service.
- Depending on the Trend Micro products in the environment, the Managed XDR service can collect data—from not only endpoints and email, but also network, server, and cloud—to correlate and prioritize alerts and system information and determine a full root cause analysis.
- Threat investigators take the burden of investigations and provide a full incident report and remediation plan so your internal teams can more easily and quickly know what has happened, along with the impact and the necessary remediation steps.

Key Detection and Response Features

- IoC sweeping
- IoA hunting
- Root cause analysis
- Impact analysis
- Automated response
- Open APIs and custom intelligence

For details about what personal information we collect and why, please see our Privacy Notice on our website at:
https://www.trendmicro.com/privacy

TREND MICRO™

Securing Your Connected World