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 eliminating or minimizing 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 of these threats, and mitigate their 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 recognize 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 94% of malware incidents come from email , combining email with endpoint detection and response is a powerful capability.

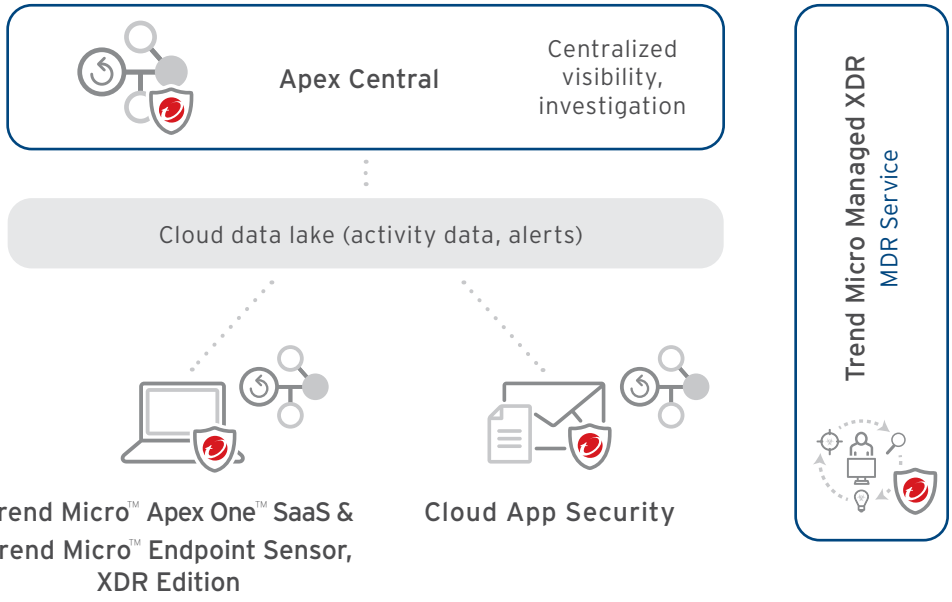
Protection Points

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

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 endpoints and email through Trend Micro Apex One™ and Trend Micro™ Cloud App Security solutions. It also includes Trend Micro Apex Central™, a centralized management console where users can view all available detection and threat information, and perform investigation tasks like indicators of compromise (IoC) sweeping, root cause analysis, and threat hunting. With XDR for Users, customers can respond more effectively to threats, minimizing the severity and scope of a breach.

FORRESTER®
WAVE LEADER 2020
Enterprise Detection And Response



[1] 2018 Data Breach Investigations Report, Verizon 2019

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 provides advanced threat protection for email and cloud file sharing. It is an API-integrated solution that works with Microsoft or Google security or third-party email gateways to add malware detection, credential phishing detection, business email compromise (BEC) impersonation detection, and internal email and file sharing protection (Microsoft® OneDrive® for Business, Microsoft® SharePoint® Online, Box, Dropbox™, Google Drive™).
- Strong and integrated 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.
- Leveraging integration into endpoint and email solutions native to Trend Micro results in more effective analytics and threat prioritization compared to what is achievable with third-party integrations.

CONSOLIDATED DETECTION, INVESTIGATION, AND RESPONSE

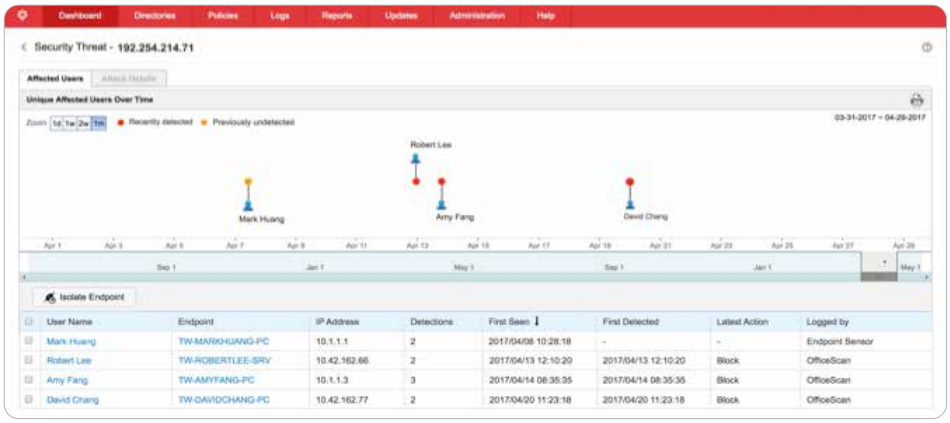
- By connecting endpoint detection information and Microsoft® Office 365® email, XDR for Users provides more insightful investigations, connecting the dots across security layers and taking into account email, which is the #1 attack source for organizations today.
- XDR for Users enables an integrated root cause analysis so a security analyst can identify which attacks started with an email and can automatically search inboxes to find other facets of the attack (e.g. who else received the malicious email and if the malicious attachment or URL is in other users' inboxes). By proactively identifying and addressing these undetonated threats, organizations can prevent any additional spread and damage.

SINGLE CONSOLE

- Apex Central console provides a single view across endpoint and email security layers, eliminating data silos and giving IT teams wider visibility to clearly and quickly identify threats and to action the appropriate response.
- A single console for visibility and investigation collapses the time it takes to detect, contain, and respond to threats, minimizing the severity and scope of impact.

HOW IT WORKS

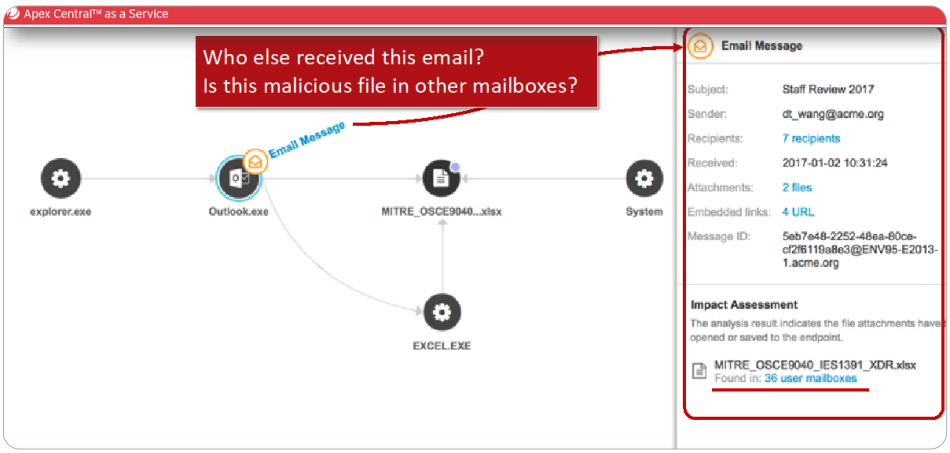
1. Endpoints with Apex One Endpoint Sensor SaaS, XDR Edition enabled, and Office 365 or Google G Suite™ emails with Cloud App Security, will record system behaviors, user behaviors, and communications.
2. Activity data (e.g. endpoint telemetry, email metadata, etc.) and detection data from these endpoints and emails are sent to the Trend Micro XDR data lake.
3. When a detection is made, investigators can search through the data to analyze the impact of the detection to understand how far it has spread and who else has been compromised.



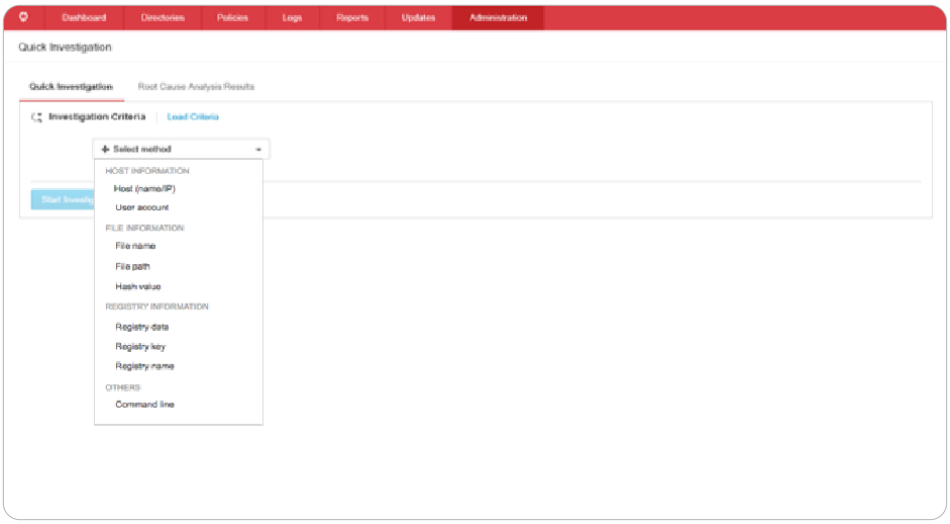
Key Protection Capabilities

- 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 detection with writing style analysis

4. A full root cause analysis allows investigators to understand the cause of the detection and immediately implement a response that includes remediating affected systems and updating Apex One and Cloud App Security to block similar attacks in the future.



5. Alternately, before a detection, investigators can search for indicators of attack (IoAs) by searching using various parameters or with IoCs and YARA rules.



TREND MICRO™ MANAGED XDR SERVICE

Alleviate constraints on security operations teams

- 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