DATASHEET

Trend Micro™

CONNECTED THREAT DEFENSE

Improve your protection from new threats

THE CHALLENGE TODAY

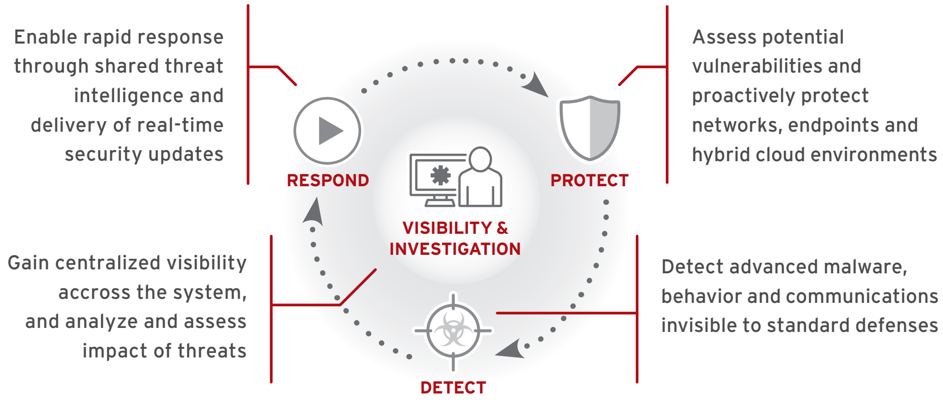
With the ever-changing threat landscape, organizations need to constantly review how they are managing the threats that are targeting them. In the past, threats were one-to-many. Today we know the majority of attacks target only a few, or even a single victim.

Another reality is that threats can start through a single entry point in your organization (with 94 percent of attacks coming through email[1]), and then laterally move to another, often with a dwell time of weeks, if not months. Many organizations struggle due to the complexity and volume of security solutions they deal with on a daily basis. In most cases the different layers or solutions do not integrate together, so identifying threats that have grown across your IT infrastructure may not be detected or identified as part of a single attack. Your organization needs to address these challenges with a different approach.

A MODERN APPROACH

Leveraging XGen™ security capabilities across multiple solutions, Trend Micro's Connected Threat Defense is a layered security approach that gives you a better way to quickly protect, detect, and respond to new threats, leveraging central visibility and investigation capabilities that span your complete IT infrastructure.

SEE ACROSS ALL SECURITY LAYERS FOR MAXIMUM VISIBILITY AND STREAMLINED INVESTIGATIONS



Enable rapid response through shared threat intelligence and delivery of real-time security updates

Assess potential vulnerabilities and proactively protect networks, endpoints and hybrid cloud environments

Gain centralized visibility accross the system, and analyze and assess impact of threats

Detect advanced malware, behavior and communications invisible to standard defenses

PROTECT YOUR ORGANIZATION

Protection is focused on proactively protecting your networks, endpoints, email, and hybrid cloud environments. No single technique can protect against all threats, which is why the XGen™ security approach of leveraging a cross-generational blend of threat defense techniques provides the broadest range of threat protection. Trend Micro solutions incorporate many protection techniques, including highly effective traditional approaches like anti-malware, intrusion prevention, whitelisting, encryption and data loss prevention. They also include new state-of-the-art techniques like high fidelity machine learning and behavior analysis to catch advanced threats like ransomware.

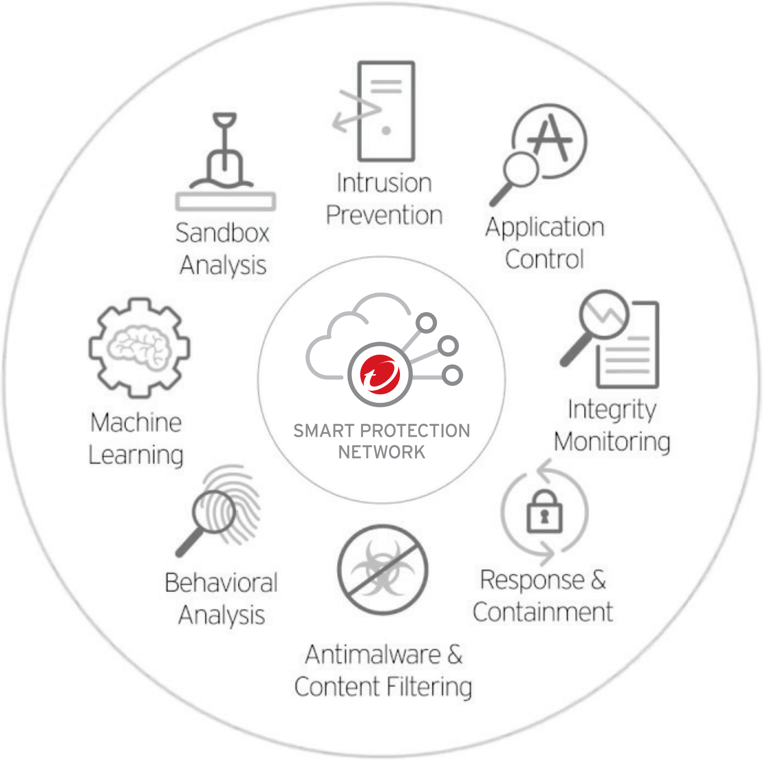
Despite the strength of multiple techniques, you will not be able to protect your organizations from 100 percent of malware or attacks. That is why being able to detect advanced malware, malicious behavior, and communications that are invisible to standard defenses is so critical. Detection is particularly important to detect zero-day attacks, command and control (C&C) communications, and advanced persistent threats.

Key Benefits

Better protection from advanced threats

- Improved visibility into attacks and threats across all emails, endpoints, hybrid cloud environments, and networks
- Automated identification of new threats detected using artificial intelligence and correlation rules
- Rapid response and deployment of new threat security techniques across multiple layers of defense
- Powered by XGen™ security, which applies the right technique at the right time

[1] 2019 Verizon Data Breach Report



DETECT THREATS ACROSS THE ENTERPRISE

With intelligent sensors across email, endpoint, server, cloud workloads, and networks gathering extensive activity data, you have the ability to quickly understand the big picture of what is happening. For example, network inspection gives you 360-degree monitoring of network traffic and scans more than 100 protocols to detect suspicious activity, command-and-control (C&C) communications, and lateral movement of inbound, outbound, and internal network communications, giving you insights about the threats coming your way and a chance to thwart them.

Trend Micro™ XDR brings it all together. This cross-layer detection and response solution applies the most effective AI and expert analytics to the activity data, producing fewer, higher-fidelity alerts. Global threat intelligence from the Trend Micro™ Smart Protection Network™, combined with expert detection rules continually updated from our threat experts, maximize the power of AI and analytical models.

RESPOND TO THREATS FASTER

When a threat is detected, either in real-time with protection techniques or an existing threat with detection techniques, you need to be able to respond quickly. As a part of a Connected Threat Defense, response capabilities delivered through XDR include:

- Prioritized alerts based on one expert alert schema to interpret data in a standard and meaningful way
- A consolidated view to uncover events and the attack path across security layers
- Guided investigations to understand the impact and identify the path to resolution

Response is also based on taking rapid action on detection events. If a threat is discovered, a file is found to be malicious, or C&C traffic is detected, then your security needs to create and share real-time information about that file or C&C server and immediately share it with all endpoint, server, and network components. This ensures that the next time the attack or threat is encountered, it will be blocked automatically—even as it attempts to laterally move through your organization.

Connected Threat Defense in Action

Here's what could happen with a Connected Threat Defense approach:

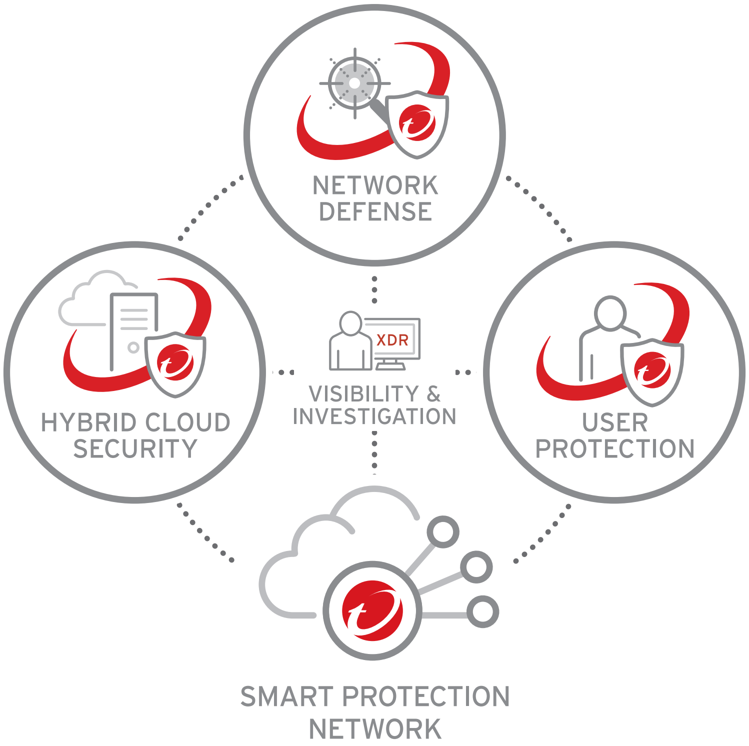
- The attack begins with the arrival of an email in a user's inbox, complete with an attachment containing a zero-day information-stealing threat. It could be stopped at the **Protection** stage by any of the numerous advanced security techniques.
- However, this zero-day threat has been designed to bypass traditional techniques, which makes the **Detection** stage vital. The messaging layer submits the attachment to the sandbox which identifies the file as malicious, but also identifies C&C communication data.
- After analysis of a sophisticated threat must come the **Response** via prioritized analysis of all environments for additional potential related threats. In addition, response should include real-time data sharing across all endpoint, server, and network security components. Failure to do this means the threat won't be blocked automatically the next time it's encountered – multiplying risk. Response also includes remediation steps like automatically cleaning computers of any malware and in doing so, maximizing user productivity. With **Central Visibility**, organizations can quickly see who else got that email or threat and respond before the threat spreads laterally through the network.

CENTRALIZED VISIBILITY AND INVESTIGATION

It is important to have techniques that cover the entire threat life cycle. However, it is also a key requirement to have those techniques integrated and coordinated into a single solution where all components work together with central visibility and the ability to easily investigate security incidents.

Unlike endpoint detection and response (EDR), Trend Micro XDR collects and correlates data across email, endpoint, servers, cloud workloads, and networks, enabling visibility and analysis that is difficult or impossible to achieve otherwise. With more context, events that seem benign on their own suddenly become meaningful indicators of compromise, and you can quickly contain the impact, minimizing the severity and scope.

While most organizations are resource and skillset constrained, XDR offers a single platform to alleviate the time and dedicated expert resources required to sift through alerts. In addition, Trend Micro™ Managed XDR helps augment understaffed security teams with 24/7 detection, investigation, and response services.



POWERED BY XGEN™ SECURITY

The one constant is the need to regularly assess the threat landscape and model your security controls based on the latest tactics, techniques, and procedures (TTPs) utilized by your adversaries. Powered by XGen™ security, the need for a Connected Threat Defense has emerged because the traditional model is no longer adequate to defend against today's attacks and threats. This approach allows an organization to take advantage of a range of cross-generational threat defense techniques that are coordinated and integrated across your networks, endpoints, and hybrid cloud environments, and gives you the visibility you need to quickly identify and remediate these attacks.

Trend Micro Connected Threat Defense works across Trend Micro **User Protection**, **Network Defense**, and **Hybrid Cloud Security** solutions, and is underpinned by **Trend Micro XDR**. Including our global threat intelligence network, all Trend Micro offerings are powered by **XGen™ security**.

Contact your Trend Micro representative or channel partner for more information, or visit **www.trendmicro.com**.

Securing Your Connected World

www.trendmicro.com

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