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, and then laterally move to another, maintaining a presence for 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 network 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, while simultaneously improving visibility and streamlining investigation across your organization.

Key Benefits
- Better protection from advanced threats
- Improved visibility into attacks and threats across all networks, endpoints and hybrid cloud environments
- Automated identification of new threats detected using custom sandboxing and network analysis
- 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

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 real-time data sharing across all endpoint, server, and gateway 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.

PROTECT YOUR ORGANIZATION
Protection is focused on proactively protecting your networks, endpoints, 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.
DETECT THREATS ACROSS THE ENTERPRISE

Detection includes:

**Network Inspection**
360-degree monitoring of network traffic scans more than 100 protocols across the network to detect suspicious activity, C&C communications and lateral movement of inbound, outbound, and internal network communications, giving you insight as to what’s coming your way and a chance to stop it before it spreads and does damage.

**Custom Sandboxing**
When one of the protection techniques finds something that is suspicious, the item is automatically submitted to a customized virtual sandbox. With the ability to mirror your real system configurations, the sandbox is optimized to help ensure accurate analysis. When the suspicious content is safely executed, you will be able to determine its potential impact and if it is, in fact, malicious.

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 include the delivery of real-time updates to multiple security techniques to prevent future attacks, identify root cause, and speed up remediation.

Response is based on taking rapid action on detection events. If a threat is discovered through sandboxing, 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 gateway security 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.

Response includes:

**Immediate Action**
If an attack is detected, targeted intelligence covering malicious files, IP addresses, and C&C communications is shared with the multiple protection techniques for real-time protection. The next time these objects are encountered they can automatically be blocked, the benefit of Connected Threat Defense.

**Automated Remediation**
To maximize productivity, you need the ability to automatically clean computers of file-based and network viruses, as well as virus and worm remnants.

**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.

Integration allows the various security layers to share intelligence and gives you a consolidated view of what is happening. Central visibility across all security layers provides a comprehensive view of the security of your networks, endpoints, and hybrid cloud environments, and simplifies threat investigation and day-to-day management tasks.

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.