Trend Micro™

CONNECTED THREAT DEFENSE

Improve your protection from new threats

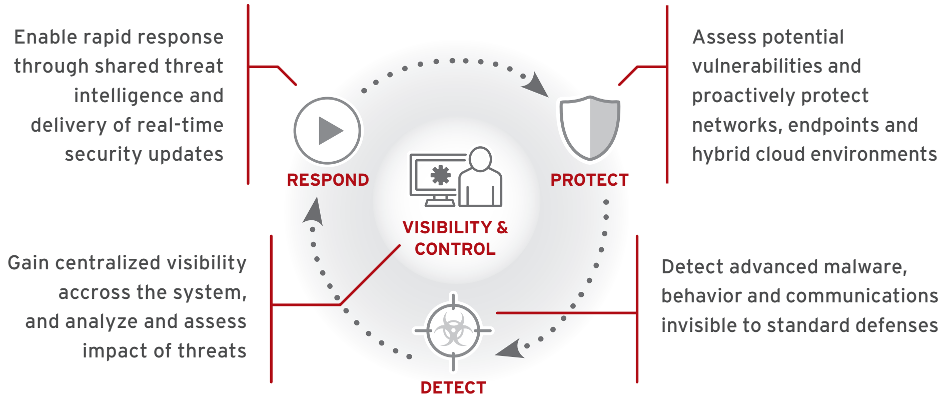
THE CHALLENGE TODAY

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 malware targets only a few, or even a single victim.

Another reality is that threats can enter your organization in one area, laterally move to another, and maintain 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 NEW APPROACH

Trend Micro Connected Threat Defense is a layered approach to security that gives you a better way to quickly protect, detect, and respond to new threats that are targeting you, while improving your visibility and control across your organization at the same time.



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

PROTECTION QUADRANT

The Protection quadrant proactively protects your networks, endpoints, and hybrid cloud environments. No single technique can protect all threats, so incorporating multiple techniques ensures the broadest range of threat protection. Trend Micro solutions incorporate many protection technologies such as anti-malware, behavior monitoring, intrusion prevention, whitelisting, application control, encryption and data loss prevention.

Despite the strength of its techniques, the Protection quadrant will not block 100 percent of malware or attacks. That is why the Detection quadrant employs techniques that will help you to detect advanced malware, malicious behavior, and communications that are invisible to standard defenses. This quadrant is particularly strong at detecting 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 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 protections across multiple layers of defense

Connected Threat Defense in Action

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

- Our 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 scanning techniques.
- However, our 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 signatures created and immediately shared with all endpoints and gateway security components. Failure to do this, means the threat won't be blocked automatically the next time it's encountered – multiplying risk. This stage also includes remediation to automatically clean computers of any malware and in doing so, maximizes user productivity.

DETECTION QUADRANT

The Detection quadrant 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 in its path.

CUSTOM SANDBOXING

When one of the techniques from the Protection quadrant finds something that is suspicious, the item is automatically submitted to a customized virtual sandbox. You can optimize detection as the sandbox mirrors your own system configurations, ensuring 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.

RESPONSE QUADRANT

Once you have protected and/or detected a threat, you need to be able to respond quickly. The Response phase delivers real-time signatures and security updates to the other quadrants to prevent future attacks, identify root cause and speed up remediation.

This quadrant relies on rapid response based on the findings in the detection quadrant. 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 a real-time signature for that file or C&C server and immediately share it with all endpoints and gateway security components. Next time the attack or threat is encountered, it will be blocked automatically.

The Response quadrant includes:

RAPID RESPONSE

If an attack is detected in this quadrant, targeted intelligence covering malicious files, IP addresses, and C&C communications is shared with the Protection quadrant to deliver real-time protection. The next time these objects are encountered they can automatically be blocked, delivering on the benefit of Connected Threat Defense.

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 CONTROL

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 management and reporting.

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.

User-centric visibility allows you to understand how threats are spreading for particular users across multiple threat vectors, devices, and applications. A visual dashboard provides a real-time display of key performance metrics and prioritization indicators for simpler, more effective security management.

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. Connected Threat Defense has emerged because the traditional model is no longer adequate to defend against today's attacks and threats. This new approach allows an organization to take advantage of the latest advanced threat protections that are coordinated and integrated across your networks, endpoints and hybrid cloud environments, and gives you the control and visibility you need to quickly identify and remediate these attacks.

AVAILABILITY

Trend Micro Connected Threat Defense is currently supported by all three Trend Micro solutions and the following products: Control Manager, Deep Discovery™, Deep Security™, OfficeScan™, ScanMail™ Exchange, and InterScan™ Messaging solutions, with support for future products coming.

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

Securing Your Journey to the Cloud

www.trendmicro.com