Trend Micro™

LAYERING SECURITY FOR THE MOST EFFECTIVE DETECTION AND RESPONSE

Lower exposure time and respond faster

INTRODUCTION

Cybersecurity professionals understand that in today’s threat landscape it’s no longer a case of “if” your organization gets attacked online, but “when”. If attacks are inevitable, it’s more important than ever to improve your detection and response to help minimize their impact. Most analysts can agree that organizations must move away from the unrealistic “prevention only” mindset.

Fortunately, Trend Micro offers tools that can integrate and share threat information automatically, aiding in detection and response to advanced malware inside your organization. This will help you to lower your exposure time and respond faster to today’s advanced threats.

When faced with known threats, organizations must do their best to block them outright. But when that’s not possible, there should be tools in place to minimize the length of time key systems and data are exposed. Current estimates suggest the “dwell time”—the time attackers go undetected inside systems—is just over 100 days. Given that one of these attacks could cause your organization to incur major financial losses, reputational damage, and possible customer attrition, you need to have the right threat detection techniques in place.

Key benefits:

• Protection from suspicious URLs and files
• Definitive answers on potential threats
• Automation of threat intelligence sharing
• A reduction in exposure to hidden threats
BENEFITS OF A LAYERED APPROACH

Despite what some vendors might tell you, there’s no such thing as a silver bullet. Instead, what’s needed is a blend of threat detection techniques, optimized so the right technique is used at the right time to deal with a particular threat.

Here are four ways layered security can improve detection and response:

1. **Rapid automated sharing**: From endpoint to email to network security, our individual security products become more than the sum of their parts through strong application programming interface (API)-driven integration. Potential threats detected by these tools are automatically submitted to the Trend Micro™ Deep Discovery™ Analyzer sandbox. If rated malicious, the update is automatically shared with all other connected security solutions. Through automation you can be protected faster.

2. **Reduces false positives**: Nothing is 100% effective every time, which is why a layered approach is best. When benign files or URLs are mistaken for threats and then blocked, it can cause significant decrease in user productivity. Trend Micro minimizes false positives by ensuring any potential threat can be offloaded to Deep Discovery Analyzer for a definitive answer. This improves protection and keeps employees productive.

3. **Improves visibility**: Trend Micro will help correlate threat intelligence, allowing the customer to connect the dots between network, endpoint, server, and network security products. This provides better visibility to threats as they are detected, and lets you look back at how they spread.

4. **Extends value**: Deep Discovery Analyzer supports both Trend Micro and third-party security products. That means you can extend the value of existing security investments and even split the cost across multiple departments.

Modern organizations are threatened by the complexity of today’s threat landscape, and can struggle to drive value from using multiple point solutions. That’s why we offer Trend Micro™ Connected Threat Defense, 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.

---

Potential threat submissions by any product, in this case Trend Micro™ Apex One™ (Trend Micro™ OfficeScan™) are sent to Deep Discovery Analyzer for further investigation.

If the submission is determined malicious, the verified threat information is sent not only to the submitting product but also to the rest of the security ecosystem for layered protection. Threat intelligence is also sent to the Trend Micro™ Smart Protection Network™ so users around the world can be protected from the once unknown threat.