Trend Micro™

DEEP DISCOVERY™ FAMILY

Advanced threat protection against targeted attacks

INTRODUCTION

Targeted attacks and advanced threats are customized to evade your conventional security defenses. They remain hidden while stealing your corporate data, intellectual property, and communications, or encrypt critical data until ransom demands are met. To detect targeted attacks and advanced threats, analysts and security experts agree that organizations should use advanced detection technology as part of an expanded strategy to address today's evasive threats.

Trend Micro™ Deep Discovery™ is a family of advanced threat protection products that enables you to detect, analyze, and respond to today's stealthy, targeted attacks. Deep Discovery blends specialized detection engines, custom sandboxing, and global threat intelligence from the Trend Micro™ Smart Protection Network™, providing the highest detection rate possible against attacks that are invisible to standard security products. Deployed individually or as an integrated solution, Deep Discovery works with Trend Micro and third-party products to provide advanced threat protection across your organization.

Key Benefits

Protection against attacks

Unique threat detection technologies discover attacks before the damage is done.

Intelligence for a rapid response

Deep Discovery and global threat intelligence drive a rapid and effective response.

Integration of your defenses

Deep Discovery integrates with your Trend Micro and third-party security tools to help prevent successful targeted attacks.

Protection from integrated threats

Trend Micro Network Defense solutions provide a blend of cross-generational techniques that apply the right technology at the right time. Trend Micro™ TippingPoint™ IPS and Deep Discovery advanced threat protection work closely together to deliver integrated detection and prevention of known, unknown, and undisclosed threats.

Trend Micro™ Deep Discovery™ Inspector is a network appliance that monitors network traffic across all ports and more than 100 protocols and applications. Using specialized detection engines and custom sandboxing, it identifies the malware, command and control communications (C&C), and activities signaling an attempted attack. Detection intelligence aids your rapid response and is automatically shared with your other security products to block further attacks.

Trend Micro™ Deep Discovery™ Analyzer is an open custom sandbox analysis server that enhances the malware detection capabilities of all your security products. Analyzer supports out-of-the-box integration with many Trend Micro products, manual sample submission, and provides an open Web Services interface to allow any product or process to submit samples and obtain results. It also offers added sandboxing for other Deep Discovery products and extends the value of Trend Micro and other security products.

Trend Micro™ Deep Discovery™ Director is an on-premises orchestration that enables centralized deployment of product and sandbox updates, with smart threat investigation on top of an enterprise-ready deployment architecture. This virtual appliance can also be your central point for advanced threat sharing. Using standards-based formats (STIX and YARA) and transfers (TAXII) it will pull threat information from several sources and share the indicators of compromise (IoC) with Trend Micro and third-party products.

Trend Micro™ XDR for Networks provides prioritized visibility into an attack. Leveraging Deep Discovery Inspector detection and network metadata collection points, XDR for Networks utilizes expert rules to correlate and connect threat detection events against network access events, presenting threat investigators with a complete view of the attack life cycle.

Deep Discovery Analyzer as a Service is an add-on to the virtual Deep Discovery Inspector and Trend Micro Apex One™ as a Service to provide cloud sandboxing capabilities. For environments that require a virtual form factor and cloud-based sandboxing, this solution will provide protection from advanced threats and targeted attacks.

Managed Detection and Response

Let Trend Micro's security experts and industry-leading artificial intelligence help you monitor and prioritize threats with Trend Micro™ Managed XDR. Trend Micro analysts will monitor, investigate, and provide a response to advanced threats discovered by Deep Discovery Inspector on a 24/7 basis. Managed XDR doesn't stop at the network layer, it extends across email, endpoints, servers, and cloud workloads. By monitoring and correlating more threat vectors, it has broader context and can provide a better detection.

CAPABILITIES

Network content inspection. Deep Discovery Inspector monitors all traffic across physical and virtual network segments, all network ports, and more than 100 network protocols to identify targeted attacks, advanced threats, and ransomware. Our agnostic approach to network traffic enables Deep Discovery to detect targeted attacks, advanced threats, and ransomware from inbound and outbound network traffic, as well as lateral movement, C&C, and other attacker behavior across all phases of the attack life cycle.

Extensive detection techniques use file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior.

Custom sandbox analysis uses virtual images tuned to precisely match an organization's system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats and ransomware designed to evade standard virtual images.

Flexible deployment. Deep Discovery Analyzer can be deployed as a standalone sandbox or in parallel with a larger Deep Discovery Inspector deployment to add additional sandbox capacity. It is scalable to support up to 60 sandboxes in a single appliance. Multiple appliances can be clustered for high availability or configured for a hot or cold backup.

Deep Discovery Inspector is available as both a hardware appliance or as a virtual appliance to help meet your deployment objectives and needs.

Advanced detection. Methods such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation, ensure threats are discovered quickly. Deep Discovery also detects multi-stage malicious files, outbound connections, and repeated C&C from suspicious files.

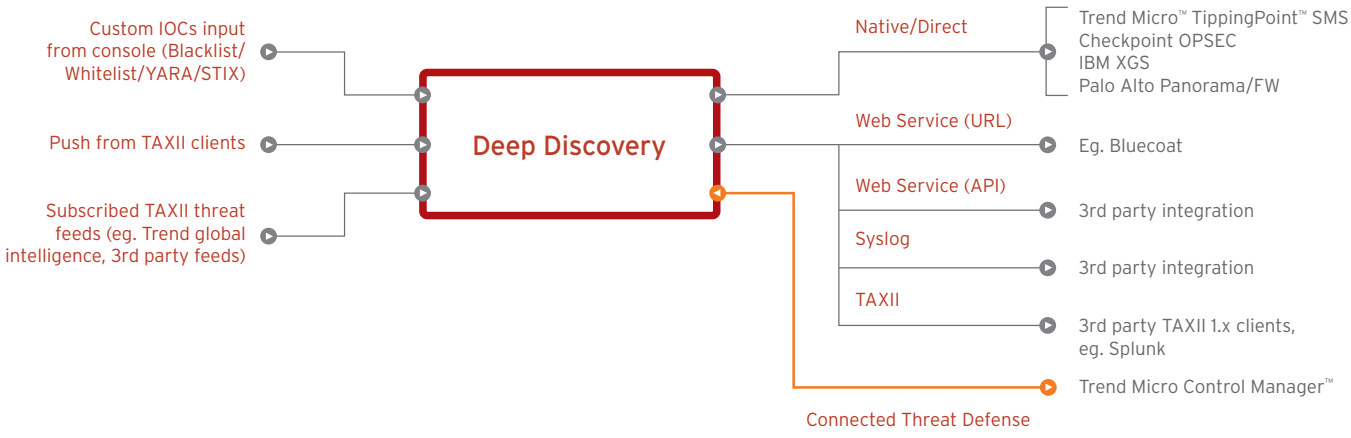
Threat intelligence. Deep Discovery will correlate and share advanced threat intelligence using standards-based formats and transports like STIX/TAXII and YARA. This enables organizations to stay ahead of unknown threats that may breach the network.

Threat Analytics will give you greater visibility into an attack, helping you prioritize the threats and show how the threat breached the network, where it went from there, and who else has been impacted by the attack. Press play and watch the entire attack play out step by step.

Integration. Deep Discovery is built to work with Trend Micro products, as well as third-party products. With native integration and a multitude of APIs, Deep Discovery will help automate security response, IoC sharing, and prevention of advanced threats and targeted attacks.

BOLSTERING THE SOC

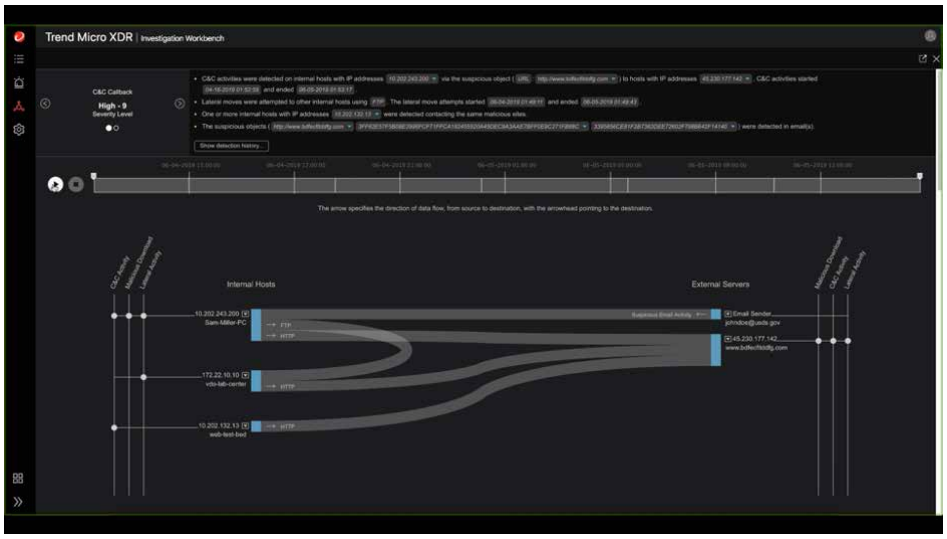
Security professionals need to understand the threat landscape. They need to know when threats are breaking and how to stop them. A thankless job, but one that is incredibly valuable. To help members of the SOC and other security professionals stay ahead of the latest threats, Deep Discovery will ingest the latest advanced threat intelligence or IoCs, using standards-based formats and transfers (STIX/TAXII and YARA) from threat feeds and custom inputs. It will then share the IoCs with Trend Micro and third-party solutions within the network. By creating this IoC exchange, you will be able to improve your time to detect advanced threats, as all of the connected products will be able to detect and block the previously unknown threats.



Deep Discovery Analyzer, more commonly known as a pure sandbox, will automatically take IoCs from other security products, detonate, and analyze the threat; and automatically send the results back for further action. Deep Discovery Analyzer can also help security analysts or threat hunters by accepting manual submissions of potential threats. This simplifies the analysis by providing a definitive answer to potential threats and suspicious objects.

PRIORITIZATION AND SIMPLIFICATION

Security products are great at detecting, alerting, and blocking threats trying to attack the organization. The downside is they produce a lot of data, some of it relevant, some of it not. It is up to the security professional in the organization to comb through the potential thousands of alerts or logs each day to determine what is actually a threat and if they need to respond.



On the easy-to-read Sankey diagram (see above), you will be able to see every step of the attack play out, dating back six months. XDR for Networks sequentially extracts metadata from the network traffic and correlates the events in a graph database for real-time visibility. This provides faster resolution with fewer people involved, and gives you a bigger picture of the full attack. In some cases, you may think the attack started today, but in fact, the initial breach happened weeks ago. XDR for Networks will correlate the data and map out every step of the attack, giving you a better idea of how to respond and how to prevent future attacks.

A KEY PART OF TREND MICRO XDR

Trend Micro defines XDR as cross layer detection and response, breaking down the silos between email, endpoints, servers, cloud workloads, and networks. It offers broader visibility and expert security analytics, leading to fewer alerts and higher-confidence detections for an earlier, faster response. With XDR, you can identify and respond more effectively and efficiently to threats, minimizing the severity and scope of an attack on the organization. Deep Discovery Inspector and XDR for Networks are valuable parts of the XDR solution, providing critical logs and visibility into unmanaged systems, such as contractor/third-party systems, Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices, printers, and bring-your-own-device (BYOD) systems.

Trend Micro Deep Discovery Family is powered by XGen™, a smart, optimized, and connected security approach.

To help prioritize and simplify the attack data, XDR for Networks will show you:

What was the first point of entry of the attack?

Who else in the organization has been impacted by the attack?

Where was the threat calling out to? (C&C communication)

TREND MICRO™

Securing Your Connected World

© 2020 Trend Micro Incorporated and/or its affiliates. All rights reserved. Trend Micro and the t-ball logo are trademarks or registered trademarks of Trend Micro and/or its affiliates in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.

[SB02_DD_Family_200616US]