WHY YOU NEED NETWORK SECURITY
The network must be at the foundation of a cybersecurity strategy, as it touches all aspects of the business. Despite more people working from home or outside the office, they are still connecting to the network, which is a fundamental attack vector for hackers. The vast majority of attacks that begin at the endpoint are just the first step in an effort to access the network through stolen and/or escalated credentials.

WHAT IS NETWORK DETECTION AND RESPONSE?
Network detection and response (NDR) is an industry category that is growing in appreciation and importance by cybersecurity professionals and the analyst community. NDR enables organizations to monitor network traffic moving inbound, outbound, and laterally across the network for malicious activity and suspicious behavior. After the threat is detected, it can be responded to at the network layer and beyond. Response measures can be automated or manual for threat hunting or increased control.

STEP ONE: STOP THE BREACH BEFORE IT CAN OCCUR
Prevention should still be a priority. As the saying goes: “An ounce of prevention is worth a pound of cure.” Stopping threats before they reach your network is critical, and a key to a Zero Trust philosophy. However, being 100% secure is unrealistic—that’s why layered security is always a requirement. Once the network has been breached, how quickly can it be detected and how prepared are you to respond?
Trend Micro expands upon traditional NDR, delivering detection and response capabilities combined with a powerful layer of protection. Our industry-leading threat protection system (TPS) blocks threats before they reach the network and can provide proactive protection against undisclosed vulnerabilities, protecting customers an average of 81 days before the release of a vendor patch.

WHAT IS TREND MICRO NETWORK ONE?
Trend Micro goes beyond traditional NDR by adding a layer of protection to detection and response. The Trend Micro Network One is a family of solutions that brings together our TPS and advanced threat protection (ATP) methods. This provides customers with inline protection at wire speeds with very low latency, and allows them to monitor out-of-band traffic and analyze slow-moving or time-delayed attacks. Together, they provide protection from known, unknown, and undisclosed threats. By leveraging Trend Micro™ Zero Day Initiative™ (ZDI), the world’s largest bug bounty program, machine learning, heuristics, sandboxing, and other detection and blocking techniques, Trend Micro Network One keeps bad actors at bay and quickly identifies breaches.

While prevention should be the first step to any network security strategy, bad actors just need to be right once to get in. In the event malware or a hacker does slip into the network, quick and accurate detection is critical. You need to know what was the first point of entry, who in the environment is impacted, and to where is the threat calling out. Once this is understood, response measures can be taken, including updating the protection devices to block future attacks and stop call-outs to command and control (C&C) servers.
KNOWN, UNKNOWN, AND UNDISCLOSED VULNERABILITIES

Every security vendor will say they can protect you from known and unknown threats. This is a good starting point, but what about the undiscovered vulnerabilities? Undisclosed vulnerabilities are a hybrid between known and unknown. These vulnerabilities are usually known by some security researchers and the impacted software vendors. Until the software is patched, enterprises are at risk of threat actors exploiting it to gain access or launch attacks. ZDI, the world’s largest vendor agnostic bug bounty program and global leader in vulnerability disclosure and research, enables Trend Micro TPS to provide virtual patches to vulnerabilities before the bad guys know they exist. This gives our customers an average of 81 days of extra protection before the vulnerabilities are publicly disclosed.

PROTECTION FROM THREE TYPES OF ZERO-DAYS

The use of “zero-day” has become a blanket term to describe any type of threat that has not yet been disclosed but is being used by malicious operators. However, painting in such broad strokes leaves enterprises vulnerable. There are actually three different types of zero-day threats enterprises need to know about:

- **Zero-day vulnerabilities**: These are the vulnerabilities that are not yet discovered or disclosed to most of the world. For the 13th consecutive year, the ZDI has been the world leader in discovering and disclosing zero-day vulnerabilities. In 2020, ZDI disclosed 60.5% of reported vulnerabilities, more than all other vendors combined.
- **Zero-day exploits**: An exploit is code written specifically to take advantage of a vulnerability. A single vulnerability could have hundreds of exploits targeting it, each using a variation of a common technique. When an attacker comes up with an entirely new way to leverage a known vulnerability, that’s called a zero-day exploit. Trend Micro uses a combination of technologies to detect zero-day exploits and targeted attacks including machine learning, heuristics, anomaly detection, and sandboxing.
- **Zero-day malware**: The vast majority of malware targets and exploits known software vulnerabilities to gain elevated access privileges and infect the host system. If the malware is known to security vendors, its hash signature can be detected in transport, allowing their solutions to filter and block the malware. But by changing just one piece of the code, the entire signature can be changed—creating a new, unknown malware that’s never been seen. If that new zero-day malware takes advantage of zero-day exploits or zero-day vulnerabilities (or even both), it becomes nearly undetectable by conventional means. Integration of our TPS with the sandbox can block the malware and automatically send suspicious objects to the sandbox for further analysis. If it’s found to be malicious, the TPS will block all future attacks.

ELIMINATE BLIND SPOTS IN THE NETWORK

Endpoint protection (EPP) and endpoint detection and response (EDR) tools provide security operations center (SOC) analysts and security professionals great insights into attacks at the endpoint. However, they are still missing critical pieces of information about the attacks, such as bring-your-own-device (BYOD) and third-party devices, industrial internet of things (IIoT) and internet of things (IoT) systems, printers, and forgotten or misconfigured systems.

These systems don’t have an agent or can’t have an agent installed on them. Focused on a single area—the traditional endpoint—EDR solutions are blind to all of these devices, leaving visibility gaps across the network. NDR shines a light and provides visibility to all devices connecting to the network, eliminating the blind spots so you can see the managed and unmanaged devices that make up the attack landscape.

Analyst groups recognize that EDR solutions provide host-level telemetry as well as information for forensic investigation. They are also seeing more SOCs implementing NDR solutions to investigate alerts and obtain additional context about suspicious activity in the network.

CORRELATION AND ANALYSIS

Trend Micro Network One is a key part of Trend Micro Vision One™, delivering critical network visibility to the XDR cyber defense center. It provides critical logs and visibility into unmanaged systems, such as contractor/third-party systems, IoT and IIoT devices, printers, and BYOD systems. By correlating the network data, the attack lifecycle becomes visible, showing what was the first point of entry, who else is part of the attack (managed and unmanaged systems), and where they are reaching out.

VISIBILITY OF NORTH/SOUTH AND EAST/WEST TRAFFIC

Traffic moves in all directions through the network. Perimeter protection is an essential part of network security, however, if it is only watching the perimeter, it can give you a false sense of security. In an instant, a threat can zip past the perimeter defenses undetected and wreak havoc from within. An essential part of a successful detection and response strategy is visibility of traffic moving laterally across the network. Unlike other vendors in this category, which require a device at the perimeter and a separate device to watch lateral movement, Trend Micro gives users visibility to traffic moving north/south and east/west with a single device, saving you time, money, and minimizing complexity.

VISIBILITY INTO ENCRYPTED TRAFFIC

With as much as **90% of internet traffic encrypted** these days, if you don’t have visibility into the encrypted workflows, you are running blind. The cost of this visibility often comes at a high price in performance. TLS/SSL decryption can have a **90% performance degradation** on your network security tools. Even if TLS inspection is included in the price of the solution, the performance impact can drive organizations to purchase devices well above their current throughput requirements just to have TLS inspection at their required rate. Trend Micro offers cloud, server, and client TLS inspection using the inline proxy method, essentially presenting itself as a connecting client, as if it were a server or client. Through this method, the appliance maintains end-to-end encryption protection, completing decryption-inspection-reencryption while maintaining perfect forward secrecy (PFS). Further, Trend Micro solutions utilize hardware and software acceleration to increase performance, reducing the need for over provisioned appliances in many cases.