WHITE PAPER

The Importance of Analyzing and Detecting Threats from End Users

Connection®
we solve IT®

CISCO
Partner
Gold Certified

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

Public Sector Solutions
1.800.800.0019

www.connection.com/cisco

Executive Summary

Today's news is full of stories of companies having to pay ransom to regain control of their operations from hackers, who have wreaked havoc on their systems by "crypto locking" their files. With all the information about cyber security out there, how do these attacks keep happening and why are they successful?

They keep happening because they have a high reward potential vs. a minimum investment. A "crypto locker" kit can be purchased on the Internet, complete with a Dark Web site to collect ransom—all with instructions on how to carry out the attack and reap the reward. Ransom is usually around $8,000 or more per computer to recover data and $30,000 per server—if you're lucky. For most companies, it's simpler to cough up the ransom and restore normal operations than it is to try to fight back. And on top of all that money they had to pay out, all their systems are now potentially compromised, and everything must be rebuilt from scratch.

These attacks are successful because most companies do not have full-time security staff or a security command center. Most IT resources are dedicated to fixing issues as they arise, rather than anticipating threats and ensuring the right tools and mechanisms are in place before attacks occur. Misguided technology decision makers often put most of their faith in a strong firewall, but that strategy has serious flaws. Depending on the firewall is the equivalent of putting up a fence with a door in it and watching over said fence to see what is coming on the horizon. The problem is that you also must watch behind you—your worst enemies are your end users.

You're Only as Strong as Your Weakest Password

Your end users are points of entry to your network that must be constantly defended. They have credentials and privileges to all your data already, so they're the simplest point of entry for a hacker—even if they don't know they're being hacked. If we take the fence analogy again, while you watch over the horizon, your end user is propping open the gate to let people in and telling you everything is fine.

Examples of threats are:

- **Phishing attempts**
- **Malware directly delivered**
- **Command-and-control attacks (C&C)**

Therefore, user threat is at the access layer of your network all the way to the edge (fence). Since the users cannot be blocked from accessing the resources that they need to perform their duties, we must constantly watch them. In this white paper, we will discuss the tools you can use to analyze and detect threats coming from within your organization.

How to Select the Right Tools

This conversation is always very interesting. Fifteen years ago, most tools were signature based, meaning they could only detect threats that had already been identified. Those were the days of anti-virus software, and while the technology was sufficient at the time, most anti-virus tools are not able to keep up with the velocity of threats and variants being created and deployed today.

Most anti-virus tools are not able to keep up with the velocity of threats and variants being created and deployed today.

The old strategy of using different vendors for endpoint security so that if product A fails to detect a threat, product B might catch it no longer makes sense in today's world of diversified threats. What is helpful today is to have products deployed in different areas that communicate with each other. Product A would never be able to learn from what product B has detected and update its response accordingly. With Cisco's stack of security products, you get tools that communicate and coordinate a response. Let's dive deeper into how they work together to keep your data safe behind the fence.

Cisco Endpoint Security

This product is formerly known as AMP or Advanced Malware Protection, and it's not an anti-virus application, but rather a full endpoint security tool. As a matter of fact, it can coexist with an anti-virus if you choose to use both on the same endpoints. It's also perfectly capable of working by itself in case you want to keep CPU cycles on the endpoint low.

The product uses different layers to protect the endpoint, such as:

- **Malicious file detection**
- **Abnormal network activity**
- **Behavioral indicators**

Malicious File Detection

Let's talk about malicious file detection first. When a new file is created, the file gets "fingerprinted" in an SHA-256 value and compared against known malware using signatures. If the threat does not match any of the known signatures, the process moves to stage two. Talos, an online real-time threat research center, scans the file. With its access to millions of endpoints worldwide, Talos can see if the suspect file has been seen elsewhere in the world. If this file is new, the third stage of the process will send your file to a virtual machine in the cloud and see what comes back. If the virtual machine sees things like unknown connections to the Internet, registry entries being created, etc., it will let you know the file is a threat. Since the process is not instantaneous, the verdict will be retroactive, but this does not necessarily mean you are infected, depending on how the file was detected and whether it was quarantined.

Abnormal Network Activity

Another key indicator of malware is abnormal network activity. If you see an endpoint starting to initiate suspicious connections to the Internet or even starting to connect to internal hosts on random ports, this is a red flag. In most command-and-control attacks (C&C), it's not malware that is delivered to end users, but rather an instruction. The instruction is to start calling into the mothership at a chosen time and to download (or upload) data. This can be done easily in an embedded command within a PDF or Word Document.

If you see an endpoint starting to initiate suspicious connections to the Internet or even starting to connect to internal hosts on random ports, this is a red flag.

In order to thwart this, Cisco Endpoint Security installs a proxy driver on the network connection and can then see what the endpoint is doing. Typically, it can see calls to numerous low reputation URLs via Talos queries—and many of these connections won't even complete because most of these domains get shut off by law enforcement. But if the C&C is calling out to 1,000 domains, chances are one may still be active. The attack is not necessarily succeeding at this point, but it has made it past the fence, and now you have a trusted endpoint trying to reach out to a bad actor mothership, and that is certainly a danger.

Typically, once discovered, this type of "dormant" attack can be pinpointed to a file or script, which can be turned into an indicator of compromise (IOC). This can help you investigate the rest of your endpoints to see if they are hosting the same IOC and mitigate. IOCs are fantastic because you can search for anything like registry entries, files, directories, etc.

Behavioral Indicators

A good way to defend yourself against threats is to understand what things do, how they do it, and when they do it. If you know what normal behaviors look like, it will be easier to spot abnormal processes. Most binary decisions are made based on true or false tests but lack context. It is very important to understand context in order to be as accurate as possible when we try to detect and flag threats.

IOCs are a fantastic tool, because you can search for anything like registry entries, files, directories, etc.

For example, you have two servers and five workstations to protect, and the same agent is deployed to all endpoints. Agent 1 is calling headquarters to report many random files are being created on its protected endpoint. Agent 2 is calling in several registry changes. Both are valid alerts, but if Agent 1 is on a server, where files are often being created, it is a false positive. The same applies to Agent 2 if it's installed on a workstation where software is currently being installed. But if you flip the roles, the alarms become relevant.

Agents in Cisco Endpoint protection can be deployed based on profiles and understand a certain baseline of activities at install time. As time goes by, "normal" behaviors are learned via machine learning mechanisms, and the behavior patterns become more accurate. When deviations occur, the Cisco Secure Desktop tool will start flagging them.

Secure Network Analytics

Endpoint protection is where security starts, and to be able to tell a good security story, we must understand network connections at large. Secure Network Analytics, formerly known as Stealthwatch, will give you that story based on traffic movements. With a distributed sensor deployment, switches, routers, and firewalls will send NetFlow data to a collector, which will compile and assemble flows. With this information, Network Analytics can tell what is connected to what, as well as how and if any suspicious behaviors were detected, which results in a CI (confidence indicator) value that will trigger an alarm after a certain threshold is crossed.

Endpoint protection is where security starts, and to be able to tell a good security story, we must understand network connections at large.

The following are examples of the value of Secure Network Analytics:

1. **The scanner:** Numerous connection requests sent from a host ended in RST. This is an indicator a host is trying to connect to a service that isn't available or is trying to scan other hosts to see what is open.
2. **Data exfiltration:** A host that baselines to 10GB of data a day is now communicating to an external host with 250GB of data in one day.
3. **Application misuse:** A host has several long-lived flows to a DNS server on UDP port 53.

Secure Network Analytics is a fantastic tool that looks at actual flows on the network that other security tools could miss. Pure flow information is a very powerful element in a security investigation, and being able to have that visibility is well worth the time it takes to set up. There is a cloud version of Secure Network Analytics available if installing appliances is not feasible in your environment, but it does have some limitations.

Identity Services Engine

The Gatekeeper

The Cisco Identity Services Engine (ISE) should be the first mechanism encountered by a device that needs to connect to the network, either via wired connection or Wi-Fi, and is one of the pillars of any zero-trust initiative.

ISE closes all points of entry, allowing endpoints to attempt to connect to a physical switch port or associate to an SSID and evaluate their admissibility of doing so by issuing a challenge. ISE uses the standard 802.1x protocol to issue such challenges and has another mechanism for devices that may not be able to converse on that level, the Mac Address Bypass (MAB) protocol.

Admins get to set up a policy that can identify the endpoint and allow specific access to that endpoint. Policies, for example, can evaluate if an endpoint is a company-owned asset vs. a BYOD device and if a corporate active directory user is authenticating on it.

The policies leading to access authorization could be built like this:

a. **Corporate Device + Corporate User = Corporate Network at Large**

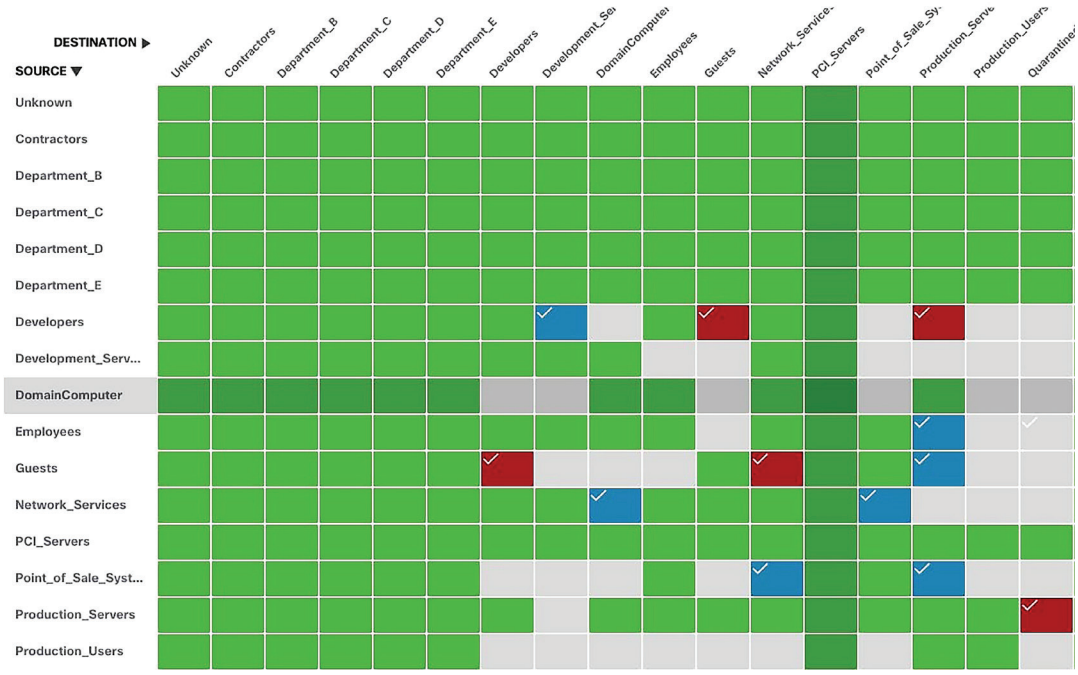
b. **BYOD + Corporate User = Intranet Websites Only**

c. **BYOD + Guest = Internet Only**

All of this is possible by using the same network with different access, and ISE can do much more than this. Profiling devices to help onboarding as well as posture assessment are just the tip of the "ISE-berg."

Profiling devices to help onboarding as well as posture assessment are just the tip of the "ISE-berg."

A newer way to segment traffic, the scalable group tag (SGT) is also driven by ISE. The process involves creating a matrix of access dos and don'ts, and after ISE identifies and allocates a tag to your connection, the matrix is followed:

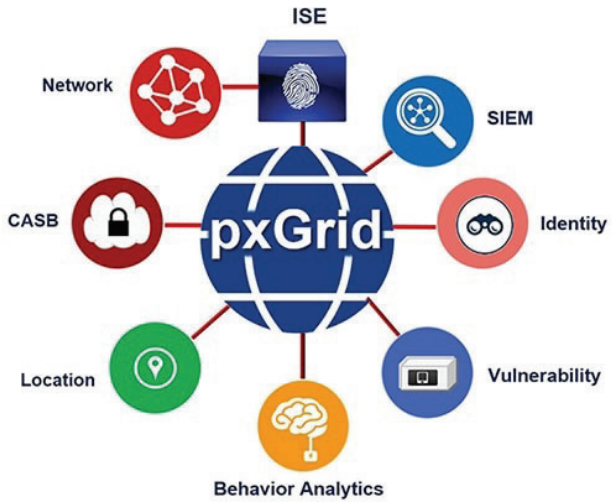


The beauty of using tags is that you are no longer using IPs to base your security rules (access lists). This makes your security portable to any segment of the network.

The Enforcer

Zero-trust is great when applied correctly to the correct endpoints for the correct reasons. What makes a great defense is not only to allow only approved traffic, but also to keep an eye on that traffic to ensure nothing changes. The biggest attack vector is usually the end user, because you already allowed the end user in. They will be the first point of compromise, and we know attackers can use them as a launchpad to get the rest of your resources, possibly elevate their user privileges, and really inflict some damage to your data.

ISE not only allows things on your network based on profiles and policies—it can also be notified by your other tools of changes in behavior. The magic link between the Cisco tools is called the PxGrid. PxGrid allows tools such as Secure Network Analytics, Secure Endpoint, and others to let ISE know something is not right.



From such intel, ISE can issue a change of authorization (CoA), essentially immediately revoking access to the network and placing the endpoint in a different state (quarantine or offline). A holistic approach to security always has an enforcement mechanism and, from a Cisco technology perspective, ISE is the enforcer.

Conclusion

Security begins at the edge. Understanding your devices, what they do, and how they are being used is key for your security strategy. Having the correct tools in place to automate a lot of that decision-making process, as well as understanding anomalies and taking action make a difference in saving your data from compromise.

If you're ready to revise your security processes and learn more about the Cisco security stack, contact an Account Manager today.

Connection® we solve IT®

Cisco Partner Gold Certified

Contact us today to learn how to get started.

Business Solutions	Enterprise Solutions	Public Sector Solutions
1.800.800.0014	1.800.369.1047	1.800.800.0019

www.connection.com/cisco