Why a Network-based Security Solution is Better than Using Point Solutions Architectures

In This Paper

- Many threats today rely on newly discovered vulnerabilities or exploits
- CPE-based solutions alone often are strained when dealing with today’s threat environment
- Network-based security offers threat intelligence to complement CPE solutions
Introduction

As security requirements and cyber threats keep evolving, network-based security that relies on monitoring command and control servers, suspect sites and IP addresses, and Netflow sessions, as well as looking for unusual activity, brings many benefits. In particular, network-based security offers enhanced protection against the growing number of unknown threats that are hard to block when using customer premises equipment (CPE) point solutions. Such solutions have the added disadvantage of being labor-intensive to manage, thus adding to operational costs.

Changing threat environment

Companies today are subject to evolving and ever-more sophisticated cyber threats. Many of the new forms of attack, such as blended attacks that combine multiple types of attacks, advanced persistent threats, and botnet-based attacks that deliver spam or overwhelm a site via a distributed denial of service (DDoS) attack, are harder to detect, prevent, or parry than attacks of old.

In most cases, today’s threats are more complex and rely on newly discovered vulnerabilities or exploits. Additionally, in several recently discovered large breaches such as the ones at Target, Home Depot, and Sony, criminals and political activists have shown their persistence and determination by using multiple levels of attacks over a long time period. In those cases and others, one or a handful of corporate or business partner machines or user accounts were compromised. Those systems or accounts were then used to carry out additional infections or data collection efforts over time. In many instances, data collected was subsequently used to socially engineer even more sophisticated attacks.

A good example of the methods and patience being employed today can be seen in a recent discovery of an attack where, for more than a year, a group of cybercriminals pilfered email correspondence from more than 100 organizations (most of them publicly traded healthcare or pharmaceutical companies) in pursuit of information significant enough to affect global financial markets.

With today’s complex attacks, traditional approaches to defending against cyber threats are often ineffective. Signature-based solutions do not recognize attacks based on zero-day exploits. And point solutions frequently miss multi-pronged attacks.

Recent large-scale breaches illustrate the challenges companies face when battling today’s cyber thieves. For instance, they frequently use socially

“Many threats today rely on newly discovered vulnerabilities or exploits.”
engineered phishing attacks, which are highly effective compared to traditional spam\textsuperscript{2}. Email recipients deem these poisoned messages safe (or at least from a legitimate source), let their guard down, and open an attachment or click on a link they otherwise would avoid. This gives the thieves a foot in the door, which is then used to collect data or launch additional and different types of attacks.

With some compound attacks, hackers infiltrate a third party (a supply chain partner, insurance processor, or credit card clearing service, for example) and then bide their time posing as an authorized user, all the while collecting information that can be used either in a more targeted attack or to steal information.

Compounding the impact of today’s more effective socially engineered attacks is the fact that hackers are resorting to zero-day exploits more than in the past. In 2014 there was an uptick in zero-day attacks due in part to the availability of the Elderwood platform, which is a set of exploits packaged so they can be used by non-technical crooks.\textsuperscript{3}

These factors are making it harder to protect an organization’s systems and data.

### Issues to consider with CPE point solutions

This changing threat environment has great implications when using traditional security solutions.

To start, signature-based approaches to fighting malware require frequent updates, but even worse they detect only known viruses, Trojans, keyloggers, and other malicious software. The rise in attacks using zero-day exploits makes this a serious problem since most antivirus products will miss nine out of 10 zero-day malware threats.\textsuperscript{4}

Likely avenues for malware to compromise an organization’s system have not changed much, but the techniques used to deliver the malware have. That carries implications for CPE solutions. In particular, a major entry point for malware is still an employee opening an infected e-mail attachment and unwittingly clicking on an infected URL while surfing the Web. Unfortunately, hackers now have the upper hand by using socially-engineered phishing attacks and shortened URLs on social media sites.

Such methods make it harder to protect systems. Most organizations seem to realize this is a critical issue. One recent survey found that 62 percent of respondents said their endpoint security software was not effective for detecting zero-day or polymorphic malware delivered in this manner.\textsuperscript{5}

Certainly, most companies use more than just anti-malware software. In fact, it is quite common to use a combination of CPE equipment like next-gen firewalls, IDS/IPS, and email and URL filtering systems.

“Traditional approaches to defending against cyber threats are often ineffective.”
“Most antivirus products will miss nine out of 10 zero-day malware threats.”

However, there are several problems with using multiple CPE point solutions.

First, such solutions are labor-intensive to manage, requiring frequent updates. This has driven the cost of security to new levels. A 1,000 person organization typically spends between $500,000 and $800,000 on security.

A second issue with using multiple CPE point solutions is that many of the solutions do not share information and thus do not provide the needed synergistic level of threat analysis insight that could help reduce exposure to many of today’s blended and compound threats.

Furthermore, a CPE-based approach does not provide information about the source of new threats nor does it spot abnormal activities that would indicate malicious activity in the making. For example, a company would not necessarily know that spoofed email was being delivered from an IP address in North Korea. Nor would a company be able to detect a command-and-control session originating from outside the company but interacting with a server behind the firewall.

Simply put, tried and true CPE-based security solutions are strained when dealing with today’s threat environment.

How network-based security helps: Capabilities that a network-based security solution can offer

Increasingly, organizations are looking to network-based security solutions to not only provide advanced protection, but also to deliver threat intelligence to complement the security offered by CPE solutions.

For example, companies for years have relied on network-based services to reduce threats reaching their facilities. Services included malware protection, spam filtering, and the blocking of URLs from known malicious sites.

These services offer several advantages. First, they are managed by the provider and thus offload the work of updating new malware signatures and managing firewalls and intrusion detection/prevention systems. Second, providers typically have security expertise and knowledge of new threats that companies may simply lack. Specifically, while IT staff in a company might not have the time to keep current on the latest types of attacks and methods to parry them, a provider would be expected to have such capabilities. And third, these services block known threats from reaching a company in the first place.

Moreover, network-based security solutions can provide an additional layer of security, enhancing the effectiveness of installed CPE solutions. For example, a network-based malware detection and email filtering solution could reduce the volume of spam reaching a company, allowing for a more modest investment in CPE equipment.

In many cases, newer network-based security services can help identify threats earlier in their lifecycle, and in some cases prevent the consequences of unknown threats. However, to do this requires much more information. An ideal service would need to collect threat intelligence gleaned from extensive monitoring of packets, infected machines, network traffic, and sessions. Analysis of this information could then be used to help identify potential malicious activity such as data theft indicated by data flow to a suspect IP address or a large amount of spam or network traffic coming from out-of-country IP addresses and servers, for example.
“CPE-based security solutions often are strained when dealing with today’s threat environment.”

Additionally, a network-based approach offered by a suitable provider brings threat intelligence AND the expertise, resources, and capabilities to minimize the impact of an attack. For example, a company fighting a DDoS attack would find its firewall is easily overwhelmed with traffic to its facility. However, a provider could scrutinize inbound traffic and divert the DDoS packets before they can hit a company’s firewall.

**Level 3 as your technology partner**

Organizations continue to build a patchwork of point solutions that are difficult to manage, create vulnerabilities, and reduce security.

Level 3 offers an alternative. Level 3 network-based security relies on extensive global monitoring of network traffic and rogue systems.

In particular, the Level 3 Security Operations Center monitors 1,000 command and control servers, more than 1 million packets per day, 350,000 alerts per day, more than 1.7 million infected machines, and more than 36 billion Netflow sessions per day.

Level 3 applies analytics to this information to develop threat intelligence upon which to act. This approach helps prevent attacks in general and is especially valuable for those based on new vulnerabilities. In particular, 40 percent of the threats detected by Level 3 were previously unknown. A CPE solution based on signatures and built to block known malicious sites would miss all of those new threats.

The threat intelligence Level 3 derives helps fight today’s newer types of attacks. For example, with advanced persistent threats, the activities of the hackers are stealthy and hard to detect. The command and control network traffic associated with these attacks can only be detected at the network layer level. What is required is deep log analyses and log correlation from various sources to detect the malicious activities.

The high-level threat intelligence complements other Level 3 network-based security offerings. Such offerings include:

- **Network Based Security:** Level 3’s cloud-based firewall and unified threat management (UTM) solution offers secure Internet access globally. Compared to backhauling traffic back to one or a few centralized datacenters for filtering, deploying a firewall and UTM service in the cloud can offer lower latency and reduced costs without the need for significant capital investment to deploy dedicated hardware at each site or continually update devices.

- **Email and Web security:** Level 3 Email and Web Defense services provide comprehensive email and Web security from the cloud for companies of any size. The services block threats at the network’s edge before they impact a business. The services help companies reduce capital expenditures and effectively balance IT and security resources while providing a platform to support a growing number of users and traffic as a business expands.
• **DDoS mitigation:** Only network-based DDoS protection solutions can provide realistic protection to company resources by quickly identifying and mitigating an attack. Level 3 DDoS mitigation services cost effectively mitigate risk posed by highly sophisticated, massive DDoS attacks through the application of proven anomaly detection technology. Available as an “on-demand” or “always-on” solution and backed by proven SLAs, Level 3 DDoS Mitigation service protects against most forms of attacks.

Taken together, Level 3 offers a layered defense approach to predict, detect, alert, and respond to threats against a company’s network and security infrastructure. As cyber security threats grow in number and complexity, Level 3’s combination of threat intelligence, global network visibility, broad portfolio of security services, and comprehensive 24 x 7 customer support can help efficiently and effectively manage risks to an organization’s network and data assets.


“Network-based security offers threat intelligence to complement CPE solutions.”