observable
networks

Press your advantage
Know your endpoints

Mind the Gap:

Common Security Tools are Failing in the Presence of Modern Threats

> **“The time has come for a new approach to network security and one that can overcome the flaws inherent in traditional security tools. Endpoint modeling is exactly that approach.”**

Today, information security is more difficult than ever before. This view is now supported by mountains of research that show that a majority of security professionals believe that managing security processes and technologies is much more challenging now than at any time in the past. For example, each year, companies in all industries consistently report a significantly higher amount of security threats than the previous year.

It is important to note that improving security is not a matter of simply trying harder. These challenges are not due to a lack of effort on the part of IT and security professionals. Additionally, new trends constantly surface that make it even more difficult for companies to protect their systems and data. For proof, consider the recent trends related to the rising use of encryption, the limitations of signature-based malware detection, and the industry shift toward Bring Your Own Devices.

These trends present their own significant security challenges, but they are even more troubling when you consider that they can be used to exploit shortcomings in five of the most commonly used security tools: firewalls, antivirus, SIEMs, malware removal, and IDS/IPS (intrusion-detection and prevention systems).

A better security solution: endpoint modeling

The time has come for a new approach to network security: One that doesn't depend on information that isn't available, such as the content of packets that have been encrypted, or the signature of brand-new viruses, or the delivery mechanism of the latest malware.

Endpoint modeling is a prime example of this new class of solution, which adds a valuable new layer to your security stack.

Closing security gaps

Observable Networks' Dynamic Endpoint Modeling solution maintains a device-specific software model of each endpoint in your environment and tracks its behavior. For example, Dynamic Endpoint Modeling monitors how each device uses the network, how it connects, what it connects to, and other details. Whenever a device starts exhibiting abnormal behaviors – acting in a way that it hasn't before, or against the documented model – endpoint modeling lets you see it, so you can take fast, efficient, and effective action to defend your IT environment. And endpoint modeling works for all kinds of devices, even those without users.

START YOUR FREE TRIAL NOW

To learn more about Dynamic Endpoint Modeling – and start a free trial now – please visit www.observable.net today.

Five security tools we will continue to use — but offer decreasing levels of security

To be clear, these five tools will continue to play an essential role as components of a conventional "security suite." But it's important to understand where their shortcomings are, how they present security gaps, and look closely at newer security solutions that are better equipped to address the current challenges. Let's take a closer look at these five tools to better understand their limitations:

1. **Next generation firewalls** can be bypassed by attackers through the use of encryption, devices introduced to the network by BYOD, or applications that were designed to connect outside of the firewall. For example, the use of "pinned keys" by Google and other vendors actually requires that holes be punched through the firewall.

2. **Signature-based antivirus solutions** are fighting the uphill battle to identify the signatures of an ever-increasing array of viruses. These include polymorphic viruses, whose code mutates while keeping their original algorithm intact. Meanwhile, hackers are determined to stay one step ahead, and can use the latest antivirus tools to see if their latest work can be detected. This is why the industry is seeing major vendors stepping back from traditionally lucrative security products.

3. **SIEMs and log management solutions** are reactive, slow, and inefficient. SIEMs are helpful in finding evidence of attack — the problem is where to look. An IT or security professional can spend days analyzing logs, trying merely to establish a correlation between a logged event and a problem. The next challenge is causation, followed by remediation. Meanwhile, damage is being done. More, most SIEMs are not "cloud friendly" and can't provide insight into assets in a cloud, leaving more than just a gap in your security program.

4. **Malware removal solutions** tend to resemble a game of Whack-a-Mole. It's an exercise in trying to identify and respond to threats that appear, seemingly at random and without end, before you are defeated. No wonder some IT and security professionals get discouraged and adopt an attitude of "Let's wait for the next update of the software, and we'll see what the next mole looks like."

5. **IDS/IPS systems** require the ability to "look inside" network traffic to see if malware is present. But steadily rising levels of encryption mean that more and more payloads are invisible to this kind of inspection, essentially "turning the lights off" on network security analysis. An encrypted — and problematic — payload can even be introduced to your network accidentally, by an employee or contractor using a personal device.

Their shortcomings aside, these five tools provide functionality that makes them useful in helping to secure organizations' systems and data. But it doesn't matter if they are used individually or in combination, they can't provide a "silver bullet" solution capable of defeating all threats. Endpoint modeling is the perfect complement to these tools, capable of overcoming their gaps and providing next-generation security.

observable
networks

For further information contact us at
info@observable.net or visit **www.observable.net**