observable
networks

Press your advantage
Know your endpoints

Don’t get fooled again: avoid surprises in network security and gain the upper hand over adversaries

When it comes to security breaches, there are only two categories: Those who know they’ve been hacked, and those who don’t know it…yet.

Death, taxes…and network attacks? Unfortunately, we’ve reached the point where hacks, data breaches, and other security attacks have truly become inevitable. For proof, you only have to turn your attention to the news, where high-profile examples seem to pop up on a weekly basis (if not more frequently). Attacks have become so common that there is now an inside joke among security professionals: “When it comes to security breaches, there are only two categories: Those who know they’ve been hacked, and those who don’t know it…yet.”

Yet even with each new story, IT staff, security professionals, and C-level executives still seem surprised that adversaries continue to get the upper hand. Many cling to the mindset of “a breach won’t happen here,” thinking that they have the right people, technology, and overall security approach. It is true that many organizations have a complete security stack—a combination of tools such as encryption, antivirus, log-based audits, malware removal software, and more. Yet since none of these provide a “silver bullet” capable of defeating all threats, it is time for a different approach.

To borrow a lyric from The Who, don’t get fooled again when it comes to thinking attacks won’t continue, and that they can’t happen to you. Today, endpoint modeling technology offers a profoundly different—and extremely effective—way to improve network security.

What is endpoint modeling?

Finding threats in your network before damage is done depends on your ability to detect sensitive changes to network activity on all of your network endpoints. Remember, before any theft or malicious actions occur, a compromised endpoint device will begin to behave differently. This is where endpoint modeling technology comes in.

Additional IT security shifts

Other trends that contribute to the need for endpoint modeling:

- **Device proliferation and BYOD:** Today, the Internet of Things (IoT) and Industrial Internet of Things (IIoT) trends mean that almost every device and piece of technology connects to the network. Plus, the Bring Your Own Device (BYOD) trend creates additional blind spots in a company's overall security posture.
- **Increasingly complex networks:** Networks are much more sophisticated, offering partner and mobile connectivity while relying on third-party hosting and SaaS services. All of this contributes to much more porous perimeters and additional risks.
- **Insider threats:** Many of today's breaches come from inside the company so they simply must watch everything, including employees, contractors, and more.
- **Too many vectors:** In such a world, it is impossible to know all of the threats as well as all of your vulnerabilities. The ways in which a company can be attacked and compromised, including device diversity, OS and application vulnerabilities, accessibility, and partner connectivity, are essentially unbounded.

Endpoint modeling can address these challenges by providing visibility into network activity, minute-by-minute endpoint behavior assessments, and a thorough knowledge of what is expected from each individual endpoint.

This insight gives security professionals the best chance to spot the activities of a potential attack since, in most cases, an adversary's actions will create recognizable changes to the overall security picture.

Endpoint modeling monitors each device in your environment and tracks its behavior. For example, it models how each device uses the network, how it connects, what it connects to, and other details. The model that emerges from these processes is similar to the one your credit card company uses to protect your account. It enables an automated system to "ask" if a specific current network activity (or a specific transaction in the case of a credit card company) is consistent with behavior that would be predicted by the model.

Then, whenever a device starts exhibiting abnormal behaviors, endpoint modeling lets you see them so you can take fast, efficient, and effective action. Endpoint modeling even continues to learn what is typical in your environment and builds more intelligence, in the form of model fidelity, over time.

Overcoming challenges inherent in data encryption

Additionally, endpoint modeling enhances existing security methods, unlike outdated threat detection methods that depend on attempting to know something about every single threat.

Consider the example of data encryption. Clearly, encryption is on the rise, to the point where encrypted data is 25-35% of total network traffic. Yet as companies move toward increasing the use of encryption to protect the privacy of network communications, the effectiveness of many network security tools decreases.

It may seem counterintuitive, but it's true. Many traditional security solutions depend on the ability to "look inside" network conversations to determine if malware is present. Unfortunately, encryption makes this impossible. This general approach to network security is known as deep packet inspection (DPI), and it's an important part of many IPS/IDS solutions, next-generation firewalls, and other payload-analysis tools.

Using DPI, security tools scan network packets for recognizable threat information. Yet since this encrypted data is invisible to conventional security tools, the encrypted data is able to pass through without the appropriate level of scrutiny and analysis. Some companies are already facing challenges related to DPI-based tools today. Many others will need to anticipate the day when all network communications become encrypted. When it does, all tools that attempt any form of network-based DPI will be rendered useless.

Increased visibility leads to increased security

When it comes to defending your network, don't be lulled into a full sense of security. While traditional security approaches are all important, many new and emerging trends may leave you more vulnerable than you may think. All of this means it's time to consider a new, non-conventional security approach. Endpoint modeling is that solution.

observable
networks

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