observable networks

Press your advantage
Know your endpoints

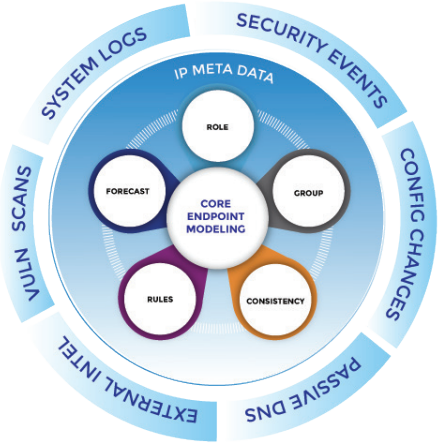
Know More About Your Network than Any Adversary

Stem security breaches with endpoint visibility and faster threat detection.

Unfortunately, we've reached the point where hacks, data breaches, and other security attacks have become inevitable. Whether it's password hacking, adversaries posing as legitimate users, or other more sophisticated methods of attack, the bad guys are doing all they can to exploit weaknesses on every device on your network.

Most organizations have a complete portfolio of security tools, such as firewalls, antivirus, malware-removal solutions, and more. While these systems are important — and comprise a larger security solution — they can't adequately address challenges posed by emerging trends such as BYOD, the Internet of Things (IoT), and increasing levels of data encryption. Organizations are adjusting their strategies to address these challenges, and a crucial area of focus is better endpoint visibility and faster threat detection.

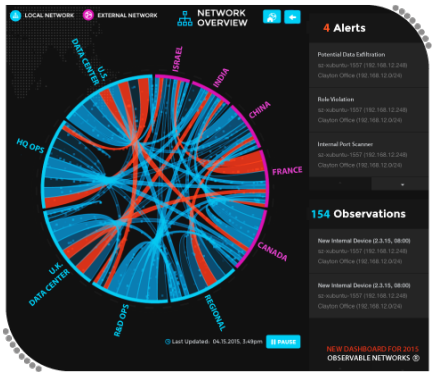
Observable Networks' Dynamic Endpoint Modeling provides a new, more efficient approach that improves network security. With endpoint modeling technology, organizations in any industry can understand the normal behavior for every device on their network. Then, if devices deviate from legitimate behavior, IT and security professionals receive alerts to identify those indicators faster, allowing them to investigate, and remediate potential threats — more efficiently and effectively than ever before.

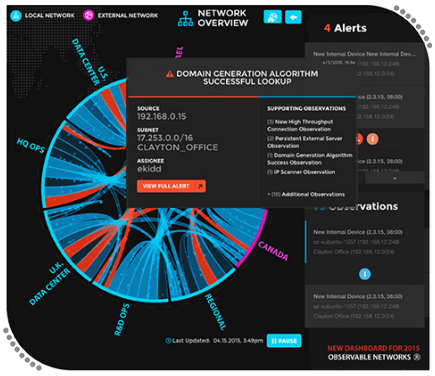


With the five dimensions of analysis, you can know more about your network than any adversary.

Improved insight drives improved security

Dynamic Endpoint Modeling addresses the challenges posed by the growing number and diversity of assets that comprise corporate networks. The growth of these unmanaged assets represents a significant threat to any network's overall security.





Gain real-time visibility into all the devices on your network, and drill down to quickly remediate potential threats.

Our solution increases your security by helping you understand the dynamic behavior of all of your network devices, on networks of any size — even those in virtual private clouds (VPCs). This increased visibility into all of your network devices delivers significant benefits that simply aren't available using conventional security methods.

- **Real-time alerts:** Endpoint modeling technology sends real-time alerts when a device starts to act abnormally — critical in detecting risky or suspicious traffic.
- **A new level of awareness:** Dynamic Endpoint Modeling helps you quickly identify potential indicators of compromise without dependencies on log file monitoring, deep packet inspection (DPI), or signature-based methods.
- **Immunity to encryption:** Unlike other security tools that depend on "looking inside" network traffic — and experience blind spots when they can't — Dynamic Endpoint Modeling monitors and models device behavior, even in environments with end-to-end encryption.
- **A solution that learns:** The longer Dynamic Endpoint Modeling is in place, the more valuable and effective it becomes. This solution continues to learn about your environment and becomes smarter about your devices over time. This is critical to improving threat recognition while minimizing false positive alarms.

Cloud powered

Dynamic Endpoint Modeling delivers a cloud-based critical network security solution that simplifies installation, maintenance, and scalability. Our passive network sensor is provided as a free virtual appliance and is easily deployed on common physical hardware and virtualization platforms.

Once your sensor is connected, we'll do the rest. Dynamic Endpoint Modeling immediately begins to collect real-time metadata from your network and automatically discovers active network devices. At the same time, we begin to establish a 30-day behavior model, which will continue to evolve as it learns, providing unprecedented insight into your network devices.

SaaS subscription

Dynamic Endpoint Modeling is available as a SaaS subscription, one that offers cost-effective monthly or annual plans. This model eliminates the need for capital business cases, complicated deployments, time-consuming employee training, and ongoing maintenance and configuration. Now, making the right security decision has never been easier, and such a simplified engagement frees you to focus on what's really important — improving your network security.

Better network security starts now

New threats call for new tools. While traditional security products are important elements of your overall security portfolio, many new and emerging threats may leave you more vulnerable than you may think.

All of this means it's time to consider a new, non-conventional security approach that offers new levels of threat-detection capabilities, smarter and more efficient security actions, and improved operational durability. Dynamic Endpoint Modeling is that solution.

START YOUR FREE TRIAL NOW

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

observable networks

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