observable networks

Observable Networks is now a part of Cisco.

CISCO

Case Study

Financial Services Firm Improves Security Speed and Results with Observable Networks

"It was clear that we needed a better security approach, a next-generation security solution that could help us identify possible threats much faster. This is when we turned to Observable Networks."

— Vice President
Financial Services
Organization

Security Solutions for Financial Services

Today, the financial markets are a favorite target for cyber attackers as they attempt to access credit card information, competitive information, or other records. From banks to credit card companies, stock brokerages to insurance companies, financial services organizations must do all they can to improve network security.

Security Goals

- Protect clients' personal and financial information, including PII data
- Monitor all endpoint devices on the network, especially employees' personal devices
- Overcome challenges caused by increased levels of network traffic encryption
- Detect compromises much earlier in the process—as they occur — before damage can be done

Solution

- Dynamic Endpoint Modeling from Observable Networks

Benefits

- Automatically identified behavior that was truly unusual for the network
- Gained real-time visibility into all endpoint device behavior for faster threat detection and remediation
- Took advantage of a SaaS delivery model to reduce costs and minimize deployment and maintenance efforts
- Improved overall security practices and peace of mind

> "Dynamic Endpoint Modeling worked immediately and provided visibility to things we expected to see — such as new mobile devices connecting to the network — but in a way that was much faster than other security tools."
>
> — Vice President
> Financial Services Organization

As a financial services organization, this company works closely with its clients to help them meet their financial goals. This requires the organization to collect, process, store, and transmit data on its clients' behalf, including personally identifiable information (PII). Protecting this data is critical to enhancing client satisfaction, complying with industry-specific security regulations, and preserving this organization's reputation.

The search for a new security tool

Like most organizations today, this financial services firm has long relied on traditional security tools, such as firewalls, signature-based antivirus products, SIEMs, malware-removal systems, and more. But it recently decided it needed a next-generation security solution, one capable of responding to emerging trends that present challenges conventional solutions simply can't address.

A company vice president explains what led to the decision. "We were adding additional devices to our network, especially employees' phones and tablets," he says. "We wanted a better way to monitor the activity of these devices." He also reports that the company needed a security solution that could work with increasing levels of data encryption, a trend that makes payloads invisible to deep packet inspection and thwarts normal security protocols.

> **"Unfortunately, in today's security world, chances are good that someone is going to attempt to breach your network or perform some other kind of attack. How quickly you can detect these attacks and take effective action can become a critical advantage. Observable Networks gives us that edge."**
>
> — Vice President
> Financial Services Organization

After another high-profile data breach made national headlines, the security team wondered if it could have identified the same warning signs in time to prevent a similar attack. The company also determined that it needed a more innovative security solution to complement its existing portfolio and bolster its total capabilities. "We were looking for a better way to identify possible threats much faster," says the vice president. "This is when we turned to Observable Networks."

A new dimension in security speed

The financial services company initially signed up for a free 60-day trial of its Dynamic Endpoint Modeling solution. "It worked immediately and provided visibility to things we expected to see — such as new mobile devices connecting to the network — but in a way that was much faster than other security tools." The company was impressed enough to continue as a full customer and deployed Dynamic Endpoint Modeling as a cloud-based SaaS solution, critical to reduce costs and simplify installation and maintenance efforts.

Now, Dynamic Endpoint Modeling gives the company's security team a significant advantage over traditional network security tools: speed. This solution provides real-time insight into all endpoint device behavior and delivers immediate alerts whenever a device starts to act abnormally or whenever a device is accessed in a way that is unusual. This helps the team detect successful attacks just as they are beginning. "Dynamic Endpoint Modeling gives us the information we need to detect and defend again data leaks and attacks much faster than other security tools," says the vice president.

He also relates a story to show just how fast — and effective — Dynamic Endpoint Modeling is. "We had a case where we suddenly had a new IP address

"Dynamic Endpoint Modeling gives us the information we need to detect and defend again data leaks and attacks much faster than other security tools."

— Vice President
Financial Services
Organization

attempting to access our network from a location we didn't recognize," he says. "The Observable solution generated a real-time alert about this activity, and we immediately blocked the IP address. The incident turned out to be harmless, but we were still glad to have received such fast notification. SIEMs or log-based tools would have had a hard time providing this information so quickly."

Faster, more effective network security

This financial services company is thrilled with the security advantage and peace of mind it has gained from its use of Dynamic Endpoint Modeling, especially as data attacks continue to make headlines. "Unfortunately, in today's security world, chances are good that someone is going to attempt to breach your network or perform some other kind of attack," he says. "How quickly you can detect these attacks and take effective action can become a critical advantage. Observable Networks gives us that edge."

Free Trial

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

Observable Networks is a privately held company headquartered in St. Louis, MO.

observable networks

Observable Networks is now a part of Cisco.

CISCO

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