observable networks

Observable Networks is now a part of Cisco.

Case Study

AFGE Gains Complete Visibility into Public Cloud Traffic with Observable Networks

"We were looking for a better way to monitor network traffic in virtual private clouds. Dynamic Endpoint Modeling was the only solution that provided visibility into all our devices in our public cloud infrastructure and their network activity."

— Taylor Higley
Director of Information Security, AFGE

About the American Federation of Government Employees

The American Federation of Government Employees (AFGE) is the largest federal employee union, representing 670,000 federal and D.C. government workers nationwide and overseas. Workers in virtually all functions of government at every federal agency depend upon AFGE for legal representation, legislative advocacy, technical expertise, and informational services.

Security Goals and Challenges

- Protecting members' personal information, including PII data
- Identifying previously undetectable vulnerabilities
- Adding a simple and affordable security solution to complement existing tools

Solution

- Dynamic Endpoint Modeling from Observable Networks

Benefits

- Gained complete visibility into network traffic in public cloud infrastructure
- Enjoyed a fast, easy implementation — successfully deployed the product trial in mere minutes
- Took advantage of a service-based delivery model that minimized budget impact and headcount
- Obtained peace of mind related to cloud server activities

Observable makes it possible for AFGE to "see" all IP traffic in its cloud networks at a glance. This is critical to extend traditional network security into public cloud networks, an area most traditional security tools can't address.

As the nation's largest federal employee union, the American Federation of Government Employees (AFGE) is committed to providing the very best services to the nearly 700,000 government workers it represents across 70 different agencies. "We are really focused on earning our members' trust," explains Taylor Higley, AFGE's director of information security. "We view each member as a valued partner. Protecting their interests is a serious responsibility, and one that we take very seriously."

Security is critically important. AFGE must protect members' private data, which includes personally identifiable information (PII) such as HR and payroll data, social security numbers, and other sensitive information like federal officers' home addresses. To provide the best security possible, AFGE prides itself on protecting members' confidential data through each step of their process.

Comprehensively monitor public cloud traffic

To achieve its security goals, AFGE recently deployed Observable Networks' Dynamic Endpoint Modeling solution. This advanced threat detection service identifies compromised network devices, even those that may escape detection from traditional security tools. With endpoint modeling, Observable's algorithms model each endpoint device in multiple dimensions of behavior. If a device starts acting abnormally, Observable notifies AFGE so staff members can quickly take action to identify and remediate potential threats.

"Dynamic Endpoint Modeling gives us visibility into our entire network, even cloud-based traffic in our public cloud infrastructure. This helps us identify anomalous behavior and evaluate potential threats quickly. Dynamic Endpoint Modeling is the only solution that gives us this complete peace of mind."

— Taylor Higley
Director of Information Security, AFGE

For AFGE, the most important benefit came from Dynamic Endpoint Modeling's ability to monitor network activity in the public cloud. Observable makes it possible for AFGE to "see" all IP traffic in its cloud networks at a glance. This is critical to extend traditional network security into public cloud networks, an area that most traditional security tools can't address.

"Being able to monitor our public cloud network traffic is a huge improvement," says Higley. "Now we have complete visibility into all of our networks, so we know what is 'normal' traffic and what is not, even if it's in the cloud. No other security vendors or tools could provide this functionality."

Easy installation, impressive results

Higley recalls just how fast and easy it was to get started with Dynamic Endpoint Modeling. "The entire process was very impressive," he remembers. "I started with Observable's free product trial late one Saturday night, and I was surprised to get an email from a service team member right away. They were live and took me through the entire process in just a few minutes that night. It was so easy that I really didn't have to do anything."

Equally impressive was how fast the Observable solution started delivering alerts — many of them showing new details about AFGE's network activity. "We received an alert almost immediately, and now get them about every other day," explains Higley. "We are getting updates about events we didn't know were occurring before, such as when a device in a country where we don't do business attempted to connect to our network. Also, the number of alerts

> **"The fact that Dynamic Endpoint Modeling is delivered as a service is a significant advantage. This means we don't need to implement more tools that could blow up our budget or allocate one or more FTEs to support it. With Dynamic Endpoint Modeling in place, we can focus on other challenges."**
>
> — Taylor Higley
> Director of Information Security, AFGE

is perfect. We don't receive too many false positives, so we are always glad to get an alert."

Higley also reports that the entire information security team loves Dynamic Endpoint Modeling. "They rave about it because they are getting valuable information that they just weren't getting from other security tools. We are always looking for ways to free up staff to focus on providing better services to our members, and Dynamic Endpoint Modeling definitely helps us achieve this goal."

Providing complete peace of mind

When asked to summarize the most significant benefits AFGE has gained, Higley doesn't hesitate. "Dynamic Endpoint Modeling gives us visibility into our entire network, even cloud-based traffic in a virtual private cloud," he says. "This helps us identify anomalous behavior and evaluate potential threats quickly. Dynamic Endpoint Modeling is the only solution that gives us this complete peace of mind."

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**