observable networks

Observable Networks is now a part of Cisco.

Case Study

Ichthys IT Services Improves Clients' Security with Observable Networks

"Our clients needed a network security tool that did the job effectively at a price they could afford. Dynamic Endpoint Modeling was exactly the right solution."

— Thom Fiorini, Founder and Managing Partner, Ichthys IT Services

About Ichthys IT Services

Ichthys IT Services has been serving the technology needs of small and medium-sized businesses in southern New England since 1992. Ichthys offers complete engineering, design, and support services for almost any IT project, helping its clients take advantage of technology to achieve their most critical business goals.

Challenges

- Providing clients with an effective — yet affordable — network security solution
- Helping clients manage endpoint devices, especially related to BYOD
- Ensuring clients have visibility into device behaviors in time to identify threats
- Managing many different types of platforms and devices on behalf of its clients

Solution

- Dynamic Endpoint Modeling

Benefits

- Improved visibility into clients' networks and the activity of each device
- Gained real-time, actionable alerts to identify previously undetected threats
- Added a new layer to traditional security methods
- Collaborated with a true business partner focused on their long-term success
- Easily integrated with existing services and service delivery systems

Searching for the right solution

Ichthys IT Services prides itself on providing the best possible IT services for a large portfolio of clients, most of which have less than 100 employees. “We really do it all,” says Thom Fiorini, Ichthys’ founder and managing partner. “In most cases, we serve as their IT team, since most of them don’t actually have one.”

When it comes to network monitoring and security, many of Ichthys’ clients either didn’t have a solution in place, or simply couldn’t afford enterprise-level systems. This was risky because several of Ichthys’ clients are healthcare providers who need to protect patient medical information. As a result, the Ichthys team was looking for a solution it could use to monitor client networks. “Since our clients tend to be smaller, we didn’t really need to have all the bells and whistles,” says Fiorini. “But it had to do the job effectively, and it had to come at a reasonable price.”

Traditional tools fall short

Ichthys might have been content to continue using traditional security tools until the Bring Your Own Device (BYOD) trend exploded. “We always faced the threat of security breaches or data theft, but now we had to find a way to manage a growing number of personal devices,” explains Fiorini. “Since these devices could gain unauthorized network access and connect to the Internet, they clearly represented a security threat.”

Ichthys concluded, as many organizations have, that traditional network monitoring and security tools such as firewalls, antivirus, and malware-removal couldn’t do the job alone. While they are all important — and all necessary parts of any larger security solution — together, they don’t effectively address challenges posed by trends such as BYOD, the Internet of Things (IoT), and increased data encryption.

Discovering Dynamic Endpoint Modeling

Ichthys recently attended a security conference and participated in a session led by the founder of Observable Networks. “It was like he was in our office and talking about the challenges we face every day,” recalls Fiorini. After learning more about Observable Networks and its Dynamic Endpoint Modeling solution, Ichthys decided to evaluate the solution as part of a free trial.

> **“On the first full day we used it, Dynamic Endpoint Modeling helped us identify a questionable server behavior. If you’re looking for time to value, that’s about as fast as you can get.”**
>
> — Thom Fiorini,
> Founder and Managing Partner,
> Ichthys IT Services

The Dynamic Endpoint Modeling solution works by observing the behavior of endpoint devices on the network and building a baseline model of this behavior. Then, if a device ever acts “abnormally” with respect to this baseline behavior, the system generates a real-time, device-specific alert, so IT staff can respond quickly. Using this approach, Dynamic Endpoint Modeling achieves the long sought-after goal of generating a small number of highly accurate and self-documenting alerts, which minimize disruptions to critical personnel and improve productivity.

Ichthys was impressed by how fast they were able to implement Dynamic Endpoint Modeling. “We loved the fact that there is no agent software to install, so we were up and running in a matter of minutes,” says Fiorini. “In fact, on the first full day we used it, the solution flagged a questionable server behavior. If you’re looking for time to value, that’s about as fast as you can get.”

In this case, Dynamic Endpoint Modeling detected an Ichthys server sending large volumes of data outside of the firewall. Ichthys uses a dedicated server for back-up, and sends all of the company’s data to storage in the cloud once an hour. So while the behavior turned out to be innocent, the alert was fast and valuable. “The Observable solution alerted us to this potentially suspicious behavior in just two instances of the hourly back-up,” says Fiorini. “It wasn’t a hack, but I was still pleased to receive this kind of alert. If any other device acted like this, it would be a problem.”

> **“Dynamic Endpoint Modeling has now become a standard component in our network monitoring and security service.”**
>
> — Thom Fiorini,
> Founder and Managing Partner,
> Ichthys IT Services

After evaluating Dynamic Endpoint Modeling in their office, Ichthys quickly rolled it out on behalf of a small group of clients. Fiorini reports that the alerts have been manageable — but valuable — so his team can quickly see potential issues and quickly take steps to resolve them. “The amount of alerts has been ideal,” he says. “We haven’t been swamped with too many false positives but have been alerted to a few issues that required attention.”

World-class support

Ichthys also gives Observable high marks for its support team. “Observable really provides the industry’s best support and are extremely proactive in helping us monitor our clients’ networks,” explains Fiorini. “Of all the partners and vendors we work with, Observable’s support really stands apart. They provide great feedback and recommendations that show they are really invested in our success.”

Future plans for Dynamic Endpoint Modeling

Ichthys’ experience with Observable has been so positive that it now plans to use Dynamic Endpoint Modeling with all of its clients. “Dynamic Endpoint Modeling adds another layer to a traditional security approach at a reasonable cost,” says Fiorini. “It is simple to use, easy to manage, and extremely effective. Dynamic Endpoint Modeling has now become a standard component in our network monitoring and security service.”

Free Trial

To learn more about Dynamic Endpoint Modeling and-start a free trial now-please visit www.observable.net/trial 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**