Case Study

University of Wisconsin-Madison Maintains Visibility and Security After Major Network Upgrade with Help from Gigamon

> Using Gigamon, we sent the same traffic to our existing opensource security tools and the firewall under consideration—real, live traffic, not lab traffic. We were able to see an apples-to-apples comparison of performance and reliability without affecting production traffic.

GREG PADDEN
Network Engineer
University of Wisconsin-Madison

Challenge

Find a new approach to maintain comprehensive visibility and security.

Solution

Gigamon Deep Observability Pipeline

Customer Benefits

- Maintain visibility and security after network upgrade
- Reliable data access for tools and teams
- Improve network troubleshooting
- Accelerate testing of new tools

As one of the most prolific research universities in the world, the University of Wisconsin-Madison (UW-Madison) shares massive amounts of data with other facilities such as CERN, home of the Large Hadron Collider that was instrumental in discovering the Higgs boson.

"We recently adapted our WAN design to accommodate the increasing volume of data that comes through our network daily through the internet and peering arrangements we have with other facilities," explained Greg Padden, network engineer for UW-Madison.

However, the university realized it was facing a challenge when it came to network upgrades. Its new performance and availability benefits were coming at the cost of overall security. Originally UW-Madison designed its security approach around a range of 10 GB tools, including its intrusion detection system (IDS), to which it forwarded all incoming and outgoing traffic for inspection. Unfortunately, when the internet connection was expanded from 20 GB to 100 GB, the monitoring platform just wasn't able to keep up. Even when monitoring a 20 GB connection, 10 percent of traffic was being dropped.

That's a risky situation to be in, especially with today's highly sophisticated threats," said Jeff Savoy, Campus Information Security Officer at UW-Madison.

In addition to the need to optically tap up to 100 GB without packet loss, UW-Madison also needed the flexibility to send traffic to multiple departments easily.

"In addition to the security team and the network operations team, each department manages their internal network, and everyone needs to see what's going on," Padden added.

With these requirements in mind, the university began to evaluate its options.

Selecting a Solution

Initially, UW-Madison considered designing a software-defined networking solution in-house to send monitored traffic to the necessary tools but estimated that a project of that scope would take at least six months, and the need to reduce risk was immediate. So, the university began to solicit possible vendors through an RFP process. "We awarded the contract to Gigamon in part because it enabled multiple teams to have visibility into the traffic on our 100 GB links and across the network. We got this so we could have UW-Madison traffic analyzed by our security monitoring systems," said Jeff Savoy, Campus Information Security Officer, University of Wisconsin-Madison.

The platform's easy-to-use mapping capabilities and the volume of traffic made it an excellent fit for UW-Madison. Finally, providing its tools and teams visibility into 100 percent of all traffic to monitor for security and network management issues and direct it to wherever it was needed—across multiple tools and departments to accelerate network troubleshooting and threat detection.

"We were able to optically tap the two 100 GB Internet connections and forty-eight 10 GB LAN ports to get 100 percent visibility of all North-South and East-West traffic. With Gigamon, we are now able to send traffic from any point on our network to any team that needs it," said Padden.

Discovering Additional Benefits

Additionally, UW-Madison eliminated one of its biggest frustrations with troubleshooting network problems through passive optical tapping with Gigamon.

"Without tapping, you have to ask the problem node to mirror all traffic to a monitor port, which changes the behavior of the node you're trying to troubleshoot," Padden said. "We would find that the problem would go away, only to come back once we turned off mirroring." Optical tapping allowed the network operations team to troubleshoot more efficiently and have more confidence in their solution.

The Gigamon solution also proved invaluable when evaluating a commercial Layer 4-7 firewall. To run a proof of concept on a single tool, security administrators can spend weeks rerouting traffic, changing firewall rules and reconfiguring servers and network devices. If they cut any corners or make any mistakes, it can influence the outcome of the test and have significant consequences for security and network performance.

In a world where all types of malicious traffic pose a constant threat, UW-Madison was able to use Gigamon to maintain network visibility and security as they upgraded their network to keep up with the demanding needs of a top research university.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-derived intelligence to amplify the power of observability tools. This powerful combination helps IT organizations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: Modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the ten largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

06.23_02