

University of Wisconsin-Madison Chooses Gigamon for Large-Scale Data Center Monitoring

“Our monitoring platform wasn’t able to keep up with 20Gb and we saw 10 percent of traffic getting dropped. That’s a risky situation to be in, especially with today’s highly sophisticated threats. When we upgraded to 100Gb, Gigamon provided us with the visibility we needed to reduce risks to the UW-Madison.”

—Jeff Savoy, Campus Information Security Officer, University of Wisconsin-Madison

Customer Benefits

- Optically tap 100Gb link to see 100 percent of the traffic
- Provide multiple departments access to tapped traffic for security and troubleshooting
- Bridge speed mismatches between link speeds and monitoring tool port speeds

Gigamon Solution

- Gigamon Visibility Platform

Challenges

As one of the most prolific research universities in the world, 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 the discovery of 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,” said Greg Padden, network engineer for UW-M. “Many universities have a border firewall, but as bandwidth requirements increase at the border to 40Gb and 100Gb, more universities will move to the friction-free, firewall-less traffic model—a large pipe without a firewall or intrusion prevention system (IPS) to introduce delay or a point of failure.”

In a world where all types of malicious traffic pose a constant threat, no organization can sacrifice security for performance and availability. UW-Madison designed their security around a range of 10Gb tools, including an intrusion detection system (IDS) to which they forwarded all incoming and outgoing traffic for inspection. Unfortunately, when they expanded their Internet connection from 20Gb to 100Gb, they did not have the technology to monitor a 100Gb link. That is why they sought a new solution through an RFP.

UW-Madison began the search for a traffic visibility solution that would address their needs. In addition to the ability to optically tap up to 100Gb with zero loss, UW-Madison needed the flexibility to dynamically configure the solution to send the tapped traffic to multiple departments. “In addition to the security team and the network operations team, each department manages their own internal network and everyone needs to see what’s going on,” Padden said.

Solution

Because of the flexibility requirement, UW-Madison considered designing a software-defined networking (SDN) solution to send monitored traffic to the desired tools, but such a project would take at least six months and the demand was immediate. Instead, UW-Madison selected the Gigamon Visibility Platform as the best solution to address their requirements due to its ease-of-use and the volume of traffic that can be processed. Gigamon passive optical TAPs, the 100Gb high capacity line cards, and the GigaVUE-HD4 chassis-based fabric node provide 100 percent of the monitored traffic and deliver it to security and troubleshooting tools.

Results

The RFP resulted in the selection Gigamon. “We were able to optically tap the two 100Gb Internet connections and forty-eight 10Gb LAN ports to get 100 percent visibility of all north/south and east/west traffic. We are now able to send traffic from any point on our network to any team that needs it,” said Padden.

In addition, through passive optical tapping UW-Madison eliminated one of the frustrations of troubleshooting network problems. “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. “We sent the same traffic to our existing open-source 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,” Padden said.

By implementing the Gigamon solution, UW-Madison was able to finally have visibility to 100 percent of the traffic to monitor for security and network management and direct it to wherever it was needed – across multiple tools and departments in order to accelerate network troubleshooting and threat detection and to improve the quality of CAPEX purchasing decision.

“We awarded the contract to Gigamon in part because it enabled multiple teams to have visibility into the traffic on our 100Gb 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.

About University of Wisconsin

University of Wisconsin-Madison is one of the premier research facilities in the world, home to more than one hundred research centers and programs in such diverse areas as agribusiness, biotech, fusion, nanotechnology, space engineering, and particle physics.

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon’s Visibility Platform and GigaSECURE®, the industry’s first Security Delivery Platform, deliver advanced intelligence so that security, network and application performance management solutions in enterprise, government and service provider networks operate more efficiently and effectively. See more at www.gigamon.com, the [Gigamon Blog](#), or follow Gigamon on [Twitter](#), [LinkedIn](#) or [Facebook](#).