


## Case Study

---

# University of Glasgow Scales Its Intrusion Detection System to Support 30,000 Users with Gigamon



The Gigamon technology has solved our scale issues. Now we can detect compromised PCs before damage is done in a way we couldn't do earlier — helping identify users with a virus and taking remedial action.

### **CHRIS EDWARDS**

Information Security Coordinator  
University of Glasgow

### **Challenge**

Find a way to scale to keep up with a growing volume of traffic without overlooking potential threats.

### **Solution**

Gigamon Deep Observability Pipeline

### **Customer Benefits**

- Reliable data delivery to security tools
- Granular traffic filtering
- Improved load balancing for the IDS
- Accelerated testing of new security tools

Like all large institutions, the University of Glasgow must protect itself against the ever-increasing rise of IT security threats. The university uses an intrusion detection system (IDS) to alert it to potential malicious activity, but with 30,000 users, it faced significant scalability challenges.

Chris Edwards, information security coordinator at the university, said, “The cybercriminals will keep upping their game, and it’s up to us to keep pace with them. Using the IDS to monitor our network traffic is similar in many ways to using an antivirus program on a PC. But we have to be able to do this concurrently for 30,000 users. This means we have to monitor huge volumes of internet traffic.”

The university had been using a mirrored port on one of its internet gateway routers, which fed the existing IDS, but it was limited to 1Gb of traffic. As traffic volume grew to tens of gigabits per second, this port was only able to monitor a fraction of the overall capacity, and it became increasingly likely the system would fail to identify malware or other malicious activities.

The issue couldn’t be resolved simply by adding multiple mirrored router ports, because the algorithms within the routers only allowed traffic to be mirrored to a single port, rather than spread across several ports. That meant that the only way to scale the existing IDS would be to mirror all traffic to a single port running faster than 10Gb.

Even if the university deployed additional expensive gateway routers, the IDS servers could only support 1Gb interfaces, so they couldn’t have received information at this higher rate. To maintain a sufficient security posture, the university needed a solution that would allow its IDS visibility into 100 percent of relevant traffic.

## Selection Criteria

The university looked at a wide range of possible solutions before being introduced to Gigamon technology by a systems integrator, Syntex Solutions. The university was impressed by several characteristics of the Gigamon solution, including:

- 10Gb capabilities with room for growth
- Granular hardware-based filtering
- Cost-effective and extremely scalable platform

## A Scalable Solution

The university ultimately selected the Gigamon Gigamon Deep Observability Pipeline to scale its IDS. All external internet traffic is now mirrored using Gigamon optical traffic splitters, which duplicate all traffic passing over the 10Gb links. Then Gigamon hardware-based Flow Mapping® technology isolates and sends only traffic relevant to the IDS for it to examine.

Edwards added, “For example, we might be sending some massive data files from the Large Hadron Collider project — which we know we can trust and might be too large for our IDS servers to analyze. We can use Gigamon to filter this traffic out, based on source and destination addresses, and significantly reduce the load on the IDS servers. When new sources come online, it’s an easy process to exclude the ones we aren’t interested in.”

The Gigamon platform also performs a load balancing function to share the traffic across multiple 1Gb ports on the intrusion detection servers, using IP addressing to share the load evenly. This approach enables the university to spread the IDS function across multiple cost-effective Linux servers, rather than having to invest in new high-end, higher bandwidth hardware.

## Quantifiable Benefits

Today, the University of Glasgow can monitor all of the traffic coming across its 10Gb internet links.

Edwards explained, “The Gigamon technology has solved our scale issues. Now we can detect compromised PCs before damage is done in a way we couldn’t do earlier — helping identify users with a virus and taking remedial action. It enables us to split the traffic load across multiple monitor ports, minimizing packet loss, so we can operate a cluster of multiple IDS boxes, comprised of cheap commodity hardware, each of which ‘watches over’ a portion of our campus.”

Since an optical splitter now feeds traffic to the system, the original mirror port on the router has been freed up and can be used for other purposes. Additionally, because Gigamon can pre-filter the traffic exposed to tools, it has been possible to reuse existing network monitoring and measuring equipment. And that means improved ROI and OpEx.

Edwards was positive about his experience of working with Gigamon. “We had direct contact with Gigamon from the outset,” he said. “They lent us a trial system and provided engineering support. Once they’d explained how the system worked, we had a good understanding and could configure it ourselves — saving us a lot of time. We tend to use the CLI rather than the web GUI, which is nice and simple, and we can’t fault it.”

Now that Gigamon solutions are installed, the university also sees other potential uses, including evaluating new security tools, such as firewalls, with live traffic, without disturbing the production network.

## Looking Forward

The university’s network continues to grow and now has 40Gb speeds running in its core. Like many educational establishments, it is also seeing a surge in demand for BYOD (Bring Your Own Device), increasing the potential exposure to malware even further. Despite this, the university believes Gigamon solution will continue to perform well into the foreseeable future to help its teams and tools detect threats.

Edwards concluded, “The network traffic continues to grow, but now we can detect malware and attacks even better than we could before. I’d advise anyone in a similar position to talk to other similar organizations to see how they’ve solved this problem. We’ll certainly be sharing our experiences around other U.K. universities.”

## 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 organisations 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 organisations worldwide. To learn more, please visit [gigamon.com](https://gigamon.com).



### Worldwide Headquarters

3300 Olcott Street, Santa Clara, CA 95054 USA  
+1 (408) 831-4000 | [gigamon.com](https://gigamon.com)

© 2020-2023 Gigamon. All rights reserved. Gigamon and Gigamon logos are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at [gigamon.com/legal-trademarks](https://gigamon.com/legal-trademarks). All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.