OpenDNS

OpenDNS is now part of Cisco.

Case Study:

HOW GREAT RESEARCH HELPS A GREAT RESEARCH UNIVERSITY PROTECT USERS AND CUT INVESTIGATION TIME IN HALF

"Investigate has given me back 50% of my time."

- **Andre' DiMino**
Principal Security Engineer
George Washington University

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Organization Snapshot

Company:
The George Washington University

Location:
Washington, D.C.

Number of users protected:
26,000+

Challenge:
Secure a large, unmanaged network against current and potential malware threats without impacting users' freedom

Solution:
OpenDNS Umbrella
OpenDNS Investigate

Impact:

- Achieved 50 percent savings in investigation time
- Reduced infections, and cut engineering and incident response teams' time by 25-to-30 percent
- Secured users against malware with no impact to user experience
- Gained deep threat intelligence to achieve shorter incident response resolution and prevent future threats

THE CHALLENGE

Protection that ensures student freedoms and secures university IP
Mike Glyer appreciates the value of research. In his role as director of information security services at the George Washington University (GWU), he's part of a team tied to the nerve center of this world-renowned research university that's been classified by the Carnegie Classification of Institutions of Higher Education as having the "highest research activity" and named a Top 25 Private Research University by The Center for Measuring University Performance.

Much of that research takes place at the ten schools and colleges and nearly 100 research centers spread over the three campuses of the Washington, D.C.-based institution. And while the strength of GWU's research helps its students, faculty and staff look beyond the classroom and into the world, Glyer himself relies on research to help protect all those parties as they do so.

"Our large user base is unmanaged, which provides the absolute online freedom typical of academic environments," Glyer says. "That openness, however, created a major malware problem that required a lot of engineering and incident response attention, and took away much-needed time from the really high-value protection of our most critical data."

"We knew we had to act to protect our most important asset: the global reputation as a research leader that draws talented students, researchers and faculty to GWU."

> *"That openness created a major malware problem that required a lot of engineering and incident response attention."*
>
> - **Mike Glyer**
> Director, Enterprise Security & Architecture

THE SOLUTION

Security that goes deep

To protect that reputation, Glyer has dedicated most of his time at GWU to strengthening the university's overall security posture by updating security architectures, improving incident response, and guiding GWU's move to a cloud architecture.

Part of this effort included analyzing existing security products and the processes required to track and resolve any network threats. Says Glyer, "In keeping with GWU's openness, we do very little in the way of outbound filtering, which in the past has led to increased breaches. When those occur, typically we start our incident response workflow by looking at our Cisco Advanced Malware Protection for Networks intrusion detection system (IDS), which is a core part of our security. But, once we've got an alert, we need to find out: A. Did this attack actually work? and B. what happened with respect to whatever domain it was trying to reach?"

"As we moved to address our growing malware issues, it was clear that blocking attacks was a key step, but it was only half of the equation," observes Glyer. "We really needed to make sure that we were gaining threat intelligence to further our incident response efforts. To truly understand each incidence of malware—specifically any information around related domains and their lifecycles—we needed a good source of data."

"We chose OpenDNS because it offered a really high level of protection for our various different user bases, with a really low level of interaction required to implement the solution, so we could start blocking attacks and begin saving IR analyst time immediately," Glyer adds.

Others on Glyer's team were drawn to the unique data available from OpenDNS. "Investigate provided information we could use to better respond to incidents, research DNS traffic, and predict attacks before they happen," recalls GWU principal security engineer Andre' DiMino.

"Investigate provided information we could use to better respond to incidents, research DNS traffic, and predict attacks before they happen."

- **Andre' DiMino**
  Principal Security Engineer

THE RESULTS

Improved protection and prevention

"We hoped to centralize where DNS was being routed so that we could have a better view of it, and also reduce the number of successful malware infections—we've definitely done that with OpenDNS," notes Glyer.

"In our open environment, we were seeing people infected by malware almost every day, but now much of it never actually ends up fully being installed because when it tries to go to its command and control, OpenDNS Umbrella blocks it," he says.

"Our analysts spend 25-to-30 percent less time chasing infections that Umbrella now blocks, which allows their limited time to be more effectively invested in high-value analysis, like active pursuit of more advanced attackers," concludes Glyer. "The time we've saved using OpenDNS has allowed us to significantly improve the overall security posture at the university."

Part of that improvement is due to the increased visibility into global Internet and attacker trends that OpenDNS Investigate has provided. As DiMino explains, "We can see queries per hour across OpenDNS's millions of users. Given that volume, we can see what's happening across the Internet in real time. You can't get this anywhere else, and it's instrumental to our incident response process."

DiMino continues: "For example, when a phishing attack or an exploit kit is suspected, we'll get an alert. We know there may be several GW hosts calling out to a domain, so we can quickly use Investigate to determine how popular the domain is and how long it's been in existence. If the domain was just registered yesterday, and has just a few queries along with an obscure name, we know something's up and can quickly block the domain, which allows us to protect the rest of the network," DiMino explains. "The integration between Investigate and Umbrella, which administers our domain-blocking policies, is invaluable, as is the reporting functionality that details who else has hit that domain in its brief existence."

"Investigate allows me to quickly make determinations about domains and IP addresses, and the ability to run pattern searches is really useful as well. Investigate has given me back 50% of my time because I no longer have to jump around to many different tools in different locations in an attempt to hunt down the information that Investigate delivers – along with a comprehensive view of IPs and domains – all in one spot," DiMino offers. "Being able to go to one place to be able to do the bulk of our research is incredibly valuable, and such a significant time savings frees me up for higher-level incident response to advanced alerts, which subsequently speeds resolution."

"For now, the actual experience of bolstering GWU's security with OpenDNS Umbrella and Investigate has proved positive for users and Glyer's group alike. Notes DiMino, "The OpenDNS team is second-to-none. They're always responsive and they care about our success. Some vendors tend to answer help requests with crickets, but knowing there's a big team waiting to support us if we need anything has really added a sense of comfort and confidence in the Umbrella and Investigate products."

For a free trial or more sales information, contact our team:
1-877-811-2367 | sales@opendns.com | www.opendns.com