Hamamatsu Chooses OpenDNS to Provide Network Visibility and Security

HAMAMATSU
PHOTON IS OUR BUSINESS

THE PROBLEM:

A lack of visibility prevented Hamamatsu from identifying threats in their network

Jim Hnasko, Network Manager of Operations at Hamamatsu, was already familiar with OpenDNS's home product when disaster struck—an unidentified malware-infected device was sending spam, wreaking havoc on their internal network and causing their email to be blacklisted. With severely limited network visibility, it was impossible to determine where the problem had originated, even with a firewall in place. "The logs weren't very clear as to where the infections were coming from," Mr. Hnasko explained.

Beyond this isolated incident, maintaining a security presence for a network of 200+ users was proving to be a challenge, especially when dealing with malicious activity. Without substantial visibility or clear reporting, it was difficult for Jim and his IT staff to pinpoint which machines were infected. The prevalence of BYOD and roaming devices among employees only added to the confusion.

THE SOLUTION:

OpenDNS security provides added visibility to help identify and stop threats, with no added latency for roaming devices

OpenDNS provides an optional virtual appliance to add internal network and user identities to DNS requests before they're enforced by our cloud-delivered network security service. Within a few hours of calling OpenDNS, Hamamatsu had deployed virtual appliances to all of their US locations, complete with AD integration.

According to Jim, "as soon as we turned on the malware filter, it showed us not only the internal IP address, but also the user it was coming from." With the origin of the infection located, the team was able to get their email flowing again in just 8 hours, after three days of their email being blacklisted. In contrast to the convoluted firewall logs, "OpenDNS helped us view our network traffic clearly–showing us the malicious traffic, and allowing us to hone in on the infected PC."

Organization Snapshot

Location: Main US office in Bridgewater, NJ, with additional locations in San Jose, Boston, Chicago, Denver, and San Diego

End users supported: 230

Using OpenDNS for: Increased network visibility and reporting helps to identify and remediate threats quickly

What They're Saying

"Being able to show [my CEO] where we were before OpenDNS and where we are now, it's night and day. Hopefully we can continue to be proactive."

- James Hnasko, Hamamatsu

Since the resolution of the email incident, OpenDNS has continued to provide Hamamatsu with valuable insight into their network. "We have daily reports that pinpoint any malware infections and help us remediate them immediately. Not just remediate, but also prevent malicious traffic from going out to the Internet." Since deploying OpenDNS, Hamamatsu has experienced an overall decrease in infections. Mr. Hnasko estimates that their network has gone from having 20% of their machines infected to less than 1%. "We went from being reactive to being proactive," he added.

Hamamatsu has also installed OpenDNS's roaming client on over 200 laptops to protect them when they leave the network—extending beyond their security perimeter to provide coverage anywhere. As an added benefit, Mr. Hnasko saw no added latency, with either the devices themselves or third-party apps. "It was a pretty seamless integration."

Adding to the ROI of the OpenDNS deployment, Mr. Hnasko produces measurable results for upper management. "Being able to show [my CEO] where we were before OpenDNS and where we are now, it's night and day. Hopefully we can continue to be proactive."

"We have daily reports that pinpoint any malware infections and help us remediate them immediately. Not just remediate, but also prevent malicious traffic from going out to the Internet."

- James Hnasko, Networks Manager of Operations for Hamamatsu

RESULTS:

1. Increased visibility into the network allows for faster remediation of infections.

2. Roaming client ensures visibility and protection for devices that travel off-network.

3. Efficient and clear reporting keeps management informed.