FireEye
SECURITY REIMAGINED

FireEye and OpenDNS Umbrella from Cisco

Extend FireEye Threat Protection Capabilities Beyond the Network pPerimeter

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- **Identifies advanced attacks:** Organizations can protect any device with the powerful combination of OpenDNS's predictive intelligence and big data analytics and FireEye's APT and behavioral analysis.
- **Immediately detects and mitigates attacks:** The combined solution enables organizations to identify advanced attacks instantly when they hit the network, and leverage that intelligence to quickly stop the spread of malware infections and minimize any potential damage.
- **Extends protection to remote users:** The FireEye Email Threat Prevention Platform (EX Series) and Threat Prevention Platform (NX Series) can direct intelligence to OpenDNS to extend protection to all user devices, whether they're inside or outside the corporate network.

OVERVIEW

Today, employees access corporate resources from just about anywhere. Likewise, advanced threats come from many external sources. For security teams tasked with safeguarding corporate assets, these realities create significant exposure—one that traditional security defenses simply do not address.

While gaining visibility into advanced attacks that hit the corporate network is vital, it's not enough. Now, intelligence about advanced attacks has to be extended outside the corporate network, to where many users and devices operate.

OpenDNS

cisco OpenDNS is now part of Cisco.

THE CHALLENGE

The FireEye Email Threat Prevention Platform (EX Series) and Threat Prevention Platform (NX Series) provide powerful security for people on the network. But not everyone works on the corporate network.

Today, mobile employees increasingly bypass their VPN agents for a variety of reasons. If VPNs are not always on, traffic will not always pass over the network's perimeter where deployed security appliances reside. These employees' devices are only defended by traditional endpoint anti-malware, which relies on comparing data files to known threat samples to block malware. Advanced malware is seldom, if ever, blocked using this signature-based technique.

OpenDNS predictive intelligence learns where attacks are being staged even before the first victim is hit—automatically blocking emergent threats. It constantly observes new and unusual DNS request patterns, atypical domain names, and suspicious DNS records or BGP route changes. The volume of information creates a real challenge for even an army of researchers to analyze it all. OpenDNS addresses this challenge by using data scientists to train statistical models that identify malware, command & control callbacks and, phishing based on real-time and past activity. The OpenDNS Security Labs team uses visualization, advanced data mining techniques, and security domain expertise to develop algorithmic classifiers to categorize and score data. These classifiers are used to reveal patterns automatically, detect anomalies, classify malicious domains, and predict future malicious sites.

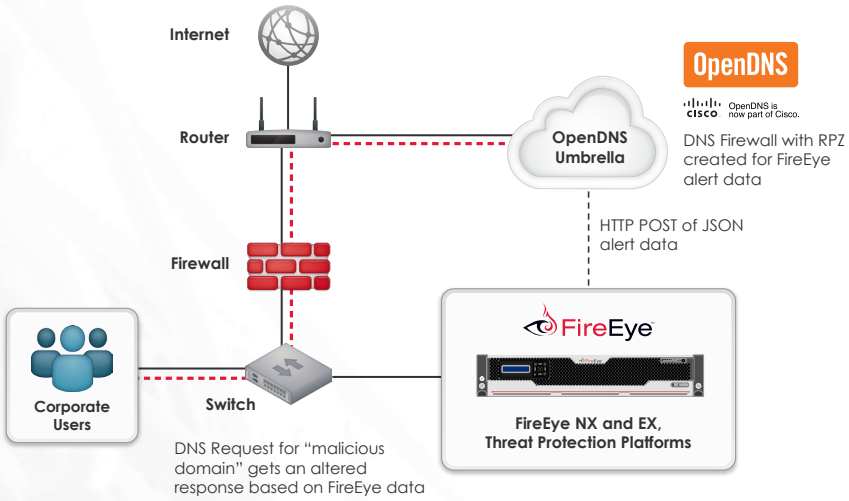
FIREEYE PRODUCT AND VERSION

FireEye Network Threat Prevention Platform (NX Series) version 7.5

FireEye Email Threat Prevention Platform (EX Series) version 7.6

OPENDNS PRODUCT AND VERSION

All OpenDNS Umbrella supported versions



THE INTEGRATED SOLUTION

The synergy created by the OpenDNS capabilities and the advanced threat identification and analysis from FireEye delivers a powerful joint solution to address a wide range of threats to customer networks:

- **Extends FireEye's advanced threat protection** to the cloud and provides centralized security policy enforcement to any device, on or off the network.
- **Blocks threat callbacks to malicious domains** enabling the enforcement of policies over any port, protocol, or application.
- **Blocks malicious domains, IP addresses, or URLs** before they are used in new attacks.

HOW THE JOINT SOLUTION WORKS TOGETHER

OpenDNS enforces network security policies across any device, anywhere, using our global network. It blocks malicious connections at the Internet's DNS layer over Web and non-Web traffic. This enforcement stops an attack's initial malware infection or its subsequent botnet callbacks. By integrating with FireEye's real-time threat detection capabilities, OpenDNS automatically validates and globally enforces the local threat intelligence that FireEye gathers on-premises.

OpenDNS automatically parses FireEye alerts and adds malicious hosts to a block list. This action instantly extends FireEye protection to all remote users and devices and provides another layer of enforcement to corporate networks.

The FireEye appliances discover Internet-based indicators of compromise, such as domains or IP addresses that host threat software or command-and-control servers used in malicious activities or phishing campaigns. These appliances immediately send this information to OpenDNS.

If the information sent from FireEye is a confirmed threat, the malicious domain or IP address is added to the FireEye Block List. The updated policy is then immediately applied to any devices governed by OpenDNS.

THE VALUE OF THIS PARTNERSHIP

Joint customers using FireEye and OpenDNS benefit from global protection against advanced attacks. In less than a minute, OpenDNS reports the specific devices or employees that were protected using both OpenDNS global intelligence and FireEye local intelligence. Additional security insights and investigative features allow security practitioners to determine whether the attack was targeted and if it is related to other known or advanced threats.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. The FireEye Global Defense Community includes 3,700 customers across 67 countries, including over 250 of the Fortune 500.

ABOUT OPENDNS, NOW PART OF CISCO

OpenDNS Umbrella is cloud-delivered network security service that adds a new layer of breach protection and Internet-wide visibility. OpenDNS Investigate provides the most complete view of the relationships and evolution of Internet domains, IPs, and ASNs, and adds the security context needed to uncover and predict threats.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**