The Modern Security Stack: Network Security in the Cloud Era

Our networks, devices, identities, and data have shifted out of the perimeter and into new cloud and mobile platforms. To address these changes, a new security stack has emerged. OpenDNS is part of this stack. We deliver network security in the cloud to defend corporate offices, data centers, remote sites, and roaming devices against attacks before they happen.

The Way We Work Has Changed

<table>
<thead>
<tr>
<th>LAPTOPS, MOBILE DEVICES, AND CLOUD APPS EVERYWHERE</th>
<th>NETWORK SECURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenDNS</td>
<td>Bit9 + CARBON BLACK</td>
</tr>
<tr>
<td>zscaler</td>
<td>McAfee</td>
</tr>
<tr>
<td>illumio</td>
<td>Microsoft</td>
</tr>
<tr>
<td>Bit9+</td>
<td>Check Point</td>
</tr>
<tr>
<td>Carbon Black</td>
<td>Symantec</td>
</tr>
<tr>
<td>MobileIron</td>
<td>RSA</td>
</tr>
<tr>
<td>Lookout</td>
<td>Symantec</td>
</tr>
<tr>
<td>CipherCloud</td>
<td>Trend Micro</td>
</tr>
<tr>
<td>Duo</td>
<td>SafeNet</td>
</tr>
<tr>
<td>Skyhigh</td>
<td>Blue Coat</td>
</tr>
</tbody>
</table>

Figure 1: Example solution providers in the existing (gray) and modern (orange) security stacks.

Network and Endpoint Security

We increasingly connect to the Internet from networks beyond our corporate perimeter. Client devices are no longer just running Windows. And we are enabling new “things” to connect to the Internet. In response, we are shifting network security, and even parts of our network, into cloud infrastructures. We are protecting any type of device in the cloud by leveraging built-in functions such as ActiveSync and DNS. And we are adopting new technologies to automate breach prevention, detection, and response.

Identity Management and Data Loss Prevention

We have enabled employees to use their own devices to access cloud apps. So we are now authenticating the user’s identity and protecting the data directly in cloud infrastructures. New technologies include SAML-based single sign-on, phone-based authentication tokens, and cloud access security brokers.

Many businesses have already begun shifting to a modern security stack to complement and eventually replace the existing one. The rest of this paper discusses how OpenDNS defends new regions of the network environment against new attacks.
The New Network is “Direct-to-Internet” and Anywhere

By adopting cloud infrastructure, we are reducing the cost and time to host server workloads. But more importantly, it enables our remote sites and roaming devices to connect directly to the Internet, which cuts massive telecom budgets and reduces network latency. Together, we are no longer reliant on the traditional hub-and-spoke wide area network model to access corporate data. This means that we are already getting work done from anywhere.

The New Attack is One-of-a-Kind and Targeting Us

Remember when we were excited to shorten the delay from days to hours to defend against a new attack? Then, a few years later, this collect and react cycle was reduced to mere minutes. What does that get us today? Well, just protection against “known” attacks. Attacks that are widespread and may cause some damage or downtime, but are not targeting specific businesses and data. The problem with this approach is that there will always still be a “patient zero.” And it could be us! Many security companies now focus on real-time detection, and sometimes prevention, of “unknown” threats. And often, they work against repurposed attacks. But more sophisticated attackers have proven that they can evade these new technologies. So what are we to do? At OpenDNS, we believe the answer is to stop being so reliant on collecting (after-the-fact) or detecting (in real-time) malicious payloads or traffic to prevent threats. We need to get visibility into what’s “emerging” within attackers’ Internet infrastructures—before the attack happens!
The Problem: Widening Gaps in Network and Attack Defenses

We've done a decent job deploying common defenses across our network environment to protect against known attacks. Yet as roaming devices increasingly connect to the Internet without the VPN client turned on, gaps in protection appear.

We've covered (or will soon cover) our core network egresses with appliance-based advanced defenses against unknown attacks. Yet these appliances tend to be too complex and costly to deploy across all remote sites. And without backhauling all Internet traffic to corporate offices or data centers, roaming devices remain exposed. Attackers exploit these gaps to essentially turn our roaming devices into “Trojan horses” and remote sites into “worms”. By compromising these expanded regions of the new network environment, attackers laterally pivot back into our corporate offices and data centers, bypassing all our advanced defenses.

Worse yet, most of us have yet to leverage any defenses that provide visibility for where attacks will emerge. Attacks do not just suddenly happen. There is a development life cycle to create new threats similar to how we create new applications. We build something, test it a few times, and then launch the new service. And later, we may improve upon it or fix deficiencies. Attackers do the same. They build software payloads, stage some server infrastructure on the Internet, register a few domain names, and test it out on random targets to see how well it works. Then, they launch the attack targeting us. And a few days or months or even years later, when they realize that their payloads or infrastructures have been detected, they make some changes. Just talk to any sysadmin about how time consuming and expensive it can be to completely rebuild server infrastructures. It’s no different for attackers, so they often reuse much of what they already built, and simply tweak a few variables here and there to fool reputation systems and blacklists. In fact, they often reuse the same server infrastructures for completely different attacks.

"By 2016, 30% of advanced targeted threats will specifically target branch offices as an entry point."

"If branch office security is not at the same level as the enterprise, consider it as an unsecure network…"

— Jeremy D’Hoinne

Bring Branch Office Network Security Up to the Enterprise Standard

---

**Figure 4: Three gaps in our security stack to defend the entire network against all attacks**
The Solution: Deliver Network Security in the Cloud and Enforce It at the DNS Layer

Emergent Threats

OpenDNS correlates the output of data mining techniques on 70 billion daily DNS requests and 500 BGP peering relationships to learn where attackers are staging or shifting their server infrastructures. We enforce this intelligence at the DNS layer—on and off corporate network—to block emerging threats. Just point DNS to us from all devices—no matter where they’re located. It’s transparent to employees and simple for sysadmins because DNS and BGP are the foundations of the Internet. And by covering DNS blind spots, we gain central, consistent domain-level Internet visibility to perform proactive incident response.

Unknown Threats

OpenDNS extends the threat protection from advanced defenses to remote sites and roaming devices. Indicators of compromise (IOCs) locally detected within corporate networks or provided by third-parties are pushed into our enforcement platform. It takes just minutes to set up due to our API-based integration. For example, a FireEye appliance protects a corporate office. The appliance intercepts an unknown file download and discovers that it is malicious. FireEye fires off a real-time alert to OpenDNS. Within seconds, our service (1) extracts relevant attributes (e.g. domain names) from the alert; (2) filters out false positives; (3) updates a per-customer FireEye security category; (4) prevents related Internet activity at remote sites, for roaming devices, and everywhere else; (5) gets real-time visibility of compromised systems; and (6) compares local activity against our global activity to identify targeted attacks.

Known Threats

OpenDNS provides similar defense against known threats as firewalls or Web gateways. The difference is that we cover the entire network environment, including roaming devices, without sacrificing performance or adding administrative overhead. By deploying client software, no matter where devices are located they will always point DNS requests to the nearest data center in the OpenDNS Global Network. The software is lightweight because all enforcement happens in the cloud.

About OpenDNS

OpenDNS provides a cloud-delivered network security service that blocks advanced attacks, as well as malware, botnets, and phishing threats regardless of port, protocol, or application. We apply statistical models to real-time and historical data to predict domains that are likely malicious and could be used in future attacks. We protect all your devices globally without hardware to install or software to maintain.