AKAMAI WHITE PAPER

The Outside-In Enterprise: Why the Network Perimeter has Failed

Akamai
FASTER FORWARD

Bigger security budgets fail to stop data breaches

In the wake of ongoing data breaches, organizations are spending more money to ensure their networks and applications – and the data they possess – remain secure. Enterprise global spending on information security will reach $75.4 billion in 2015, an increase of 4.7% over 2014 according to Gartner, driven in part by high-profile data breaches.

Mega-breaches like those at Target, Sony, Home Depot, OPM, and others help security departments get greater buy-in and bigger budgets. After the Target breach, 61% of organizations increased their security budgets by an average of 34% in 2014, according to a study conducted by the Ponemon Institute on behalf of Identity Finder, LLC.

Organizations are more aware of data breaches, but many continue to invest in network perimeter solutions that have failed to deter or otherwise thwart cybercriminals. Unfortunately, most of the money spent by enterprises on security is targeted at shoring up a perimeter built at a time when the majority of users were situated inside the physical enterprise. Enterprises now operate with an "Outside-In" access model, where most users – badged employees, contractors, and third parties – gain access to cloud and on-premise corporate network and computing resources.

Despite the addition of a wide variety of sophisticated security appliances, security detection approaches, and remediation techniques, the current network perimeter fails to fulfill its mission of keeping the bad guys out of the enterprise infrastructure. Can anything be done to shore up the effectiveness of the traditional perimeter, or is it time for a new approach?

The Inside-Out Enterprise

The network perimeter remains an essential security strategy to separate enterprise insiders from public outsiders. However, the perimeter was conceived and designed long ago, when network architectures were fundamentally straightforward compared to today's complex designs. Back then, the majority of network users were "inside" the enterprise, both physically (as in they were working from a corporate office) and logically (as in they were on the local LAN), using applications like Oracle, Exchange, or SharePoint via their internal network. In the **Inside-Out Enterprise**, access was simple, since everyone had to be on the LAN. Remote users were a small minority, accessing the network via a VPN. Because their numbers were so small, the risk of a breach was also limited. In this environment, firewalls and the early security appliances did an adequate job of policing the modest amount of inbound traffic coming through the perimeter.

The Outside-In Enterprise

But today, things are different. The move to the cloud, popularity of mobility, and the sharing economy has created a new normal - the **Outside-In Enterprise**. Instead of most users being on the inside, most users come in from the outside. This shift is driven, in part, by globalization, ecommerce, and collaboration requirements that motivate corporate networks to open up their network and computing resources to partners, contractors, and other third parties at an unprecedented rate.

In addition to third parties, employees have also become outsiders. Increasingly, badged employees are not anchored to a desk in an office, and some don't have an office at all. Every employee that uses their iPhone or iPad from an airport, coffee shop, or home office via the Internet to access internal corporate applications is by-passing the company firewall and is, in essence, an outsider.

In addition to badged employees, there is a new breed of ad-hoc employee at the center of the sharing economy — the micro-entrepreneur. These independent contractors, who work for one or more web-enabled companies like Uber, Lyft, Chegg, or Airbnb, not only do not have an office, they likely use their own personal devices to access multiple corporate networks. The result: a third-party, casual 'employee' who uses a personal device on multiple enterprise production networks. It's a security manager's worst nightmare.

The resulting problem is we have opened more and more holes in the perimeter firewall to afford access to these outsiders. The perimeter has become porous, and breaches have become common. The enterprise IT team has responded by deploying two strategies: "defense-in-depth" and "extend-the-perimeter". With "defense-in-depth", the network firewall is fortified with IDS/IPS, DLP, WAF, and other products to catch ever more bad stuff trying to get through. With "extend-the-perimeter", the strategy is to establish trust with users and endpoints on the Internet before granting access to the network. Technologies like NAC (Network Access Control), and more recently Mobile Device Management (MDM) or Enterprise Mobility Management (EMM), have basically sought to take users on the outside and bring them back inside.

Despite the flip to the Outside-In Enterprise, the majority of access is still handled by the same technologies used twenty years ago — VPNs, proxies, and remote desktops — that require enterprises to punch holes in their firewalls, open up their perimeters to attack, and allow users overly broad access to network resources. As the number of holes increase, the attack surface presented to the Internet is increased, and the ability for IT and security teams to manage long and complicated access policies degrades. Even worse, when malware and bad actors get in, traditional solutions like VPNs give these vectors access to our internal networks where they can reach from system to system.

Like an ever-expanding set of firewall rules, each new product added to the perimeter increases complexity and overhead to manage policy. Yet breaches continue at an increasing rate. Can perimeter security designed for the Inside-Out enterprise work for today's Outside-In enterprise? Given the number of breaches making the news almost daily, we have to admit the answer is 'no'. Perimeter security has failed.

A New Approach to the Network Perimeter is Required

To solve the Outside-In problem, enterprises need to go in a different direction with a methodology that simplifies both perimeter security and access. But how do we define that? Let's first consider the four major inadequacies of today's network perimeter:

1. Though firewalls can be programmed to filter inbound perimeter traffic, bad stuff gets through. Broadly speaking, as long as we take the approach that the firewall will open inbound ports to users and applications, it will remain a prime target for thieves and hackers. It has long been established that the firewall looks more like a block of Swiss cheese than an actual defensive wall. **But what if we took the approach to stop opening up inbound ports to applications and apply a different technique to connecting outsiders to applications?**

2. VPNs continue to be the way most organizations provide remote access through the network perimeter to third party users and employees. While setting up a VPN can take just minutes, configuring the firewall and policy rules to support a new VPN can often take days or weeks, involving several different IT and security groups. Once a VPN user is connected, users often have access privileges to a large segment of the corporate infrastructure – access that they do not need and that you do not want them to have! **Yet, what if we took the approach to eliminate network-wide access via VPNs and, instead, provided users with only fine-grained access to applications that they need?**

3. Providing any access from the outside through the network perimeter is based on some model of 'trust' between users, devices, and the network, be it authentication, certificates, tokens, "Extend-the-Perimeter" strategies, etc. The problem with these approaches is that the trust is a fallacy, as underscored by the recent Stagefright and Heartbleed vulnerabilities. **However, what if we moved to a model of zero-trust, i.e., a model pursuant to which no user is trusted from the outset, and when trust it established, it is transient?**

4. Today's standard for a great user experience is set by SaaS applications – Salesforce.com, Gmail, Box, etc. The concept of application access on any browser-enabled device, with no client (VPN) software to install and rapid response times, is now the enterprise user expectation as well. Some security solutions lose the perspective of ease and simplicity for the user, forcing complexity to ensure security. **Yet, what if the network perimeter ensured both security and a great user experience by eliminating client software, allowing the use of any device and mitigating the effects latency introduces with WAN optimization techniques?**

Enterprises are at an inflection point with approaches to securing the network perimeter and delivering applications to users. Whether running inside a private data center or in a public cloud-computing environment, private applications need to be delivered to employees, partners, and customers with greater security and simplicity than existing access methods provide.