The Evolution of Zero Trust

For much of its short history, information security has been dominated by a perimeter-based network security model that essentially **assumes that anyone inside the corporate network boundary was 'trusted'** and anyone on the outside was 'untrusted.' This notion of trust has functioned as the basis for determining which resources or applications people can access for over 20 years.

In recent years, numerous high-profile attacks have weakened the case for this model, to the point that it has become almost cliché in security circles to claim that the perimeter is dead. This may be overstating things a bit, but it is increasingly clear that:

The perimeter is becoming less relevant, due to a number of factors, including the growth of cloud computing, mobility, and changes in the modern workforce.

To consider an example, a firm could have users who may or may not be employees in the internal HR system or directory, who could be located pretty much anywhere, and also be accessing cloud applications from an unmanaged mobile device. In such a scenario, at no point would they ever actually touch the corporate network. Obviously in those cases, perimeter-based defenses aren't going to help us much.

In recent years we have seen the emergence of a new way of thinking of security that does away with this notion of 'trusted insider' versus 'untrusted outsider' in favor of a model where all users are assumed to be untrusted, and where access to resources is based more on 'who' you are than 'where.' This model is associated with a variety of names that are more or less directly associated, and which mean largely the same thing — 'Conditional Access', 'Application-based access', Software-Defined Perimeter, Identity-Aware Perimeter and Identity-Aware Networking,', to name just a few. However, the most common term, and the one which we will use in this paper is **Zero Trust**.

The concept of Zero Trust has its roots in the Jericho Forum from the early 2000s, which was basically a bunch of security practitioners that got together to establish a framework to deal with the impact of cloud computing and this notion of 'de-perimeterization.' The specific term Zero Trust, however, is probably somewhere around 10 years old. In that time, there have been various iterations of the Zero Trust model, and in the rest of this paper we will trace the evolution of Zero Trust to establish the context for what Zero Trust means today and how it needs to adapt to modern requirements.

PHASE 1:

SEGMENTATION

The first phase of the Zero Trust phenomenon is arguably network segmentation, which actually dates back to the 1980s when VLANs were developed, but really became popular in the early 2000s when standards were developed and most of the firewall/VPN vendors were pushing VLANs. The essential idea of segmentation is that in the old perimeter model, most firms had a flat network structure. So once an attacker got inside, he or she had free rein to just about everything. But if you break up networks into logical segments, you can limit what an attacker can access once they get inside and also their ability to move laterally, which is a big component of most breaches.

Micro-segmentation is a newer update and essentially takes the segmentation concept to the extreme, with network segments reduced to isolate specific servers or even individual workloads. And one of the main drivers of segmentation was that firms wanted to extend access beyond their own employees to contractors, partners, consultants and others, without giving them free rein to the entire network.

PHASE 2:

SDP APPLIANCES

Another approach that can be seen as an extension of this concept is what has come to be known as Software-Defined Perimeters, or SDP. Most early SDP offerings uses some combination of client software, a controller and a gateway device to provide remote access to mainly internal/on-prem applications without needing a VPN, in effect 'shrinking' the perimeter around a single application. One of the main drivers for the emergence of SDP was that it can quickly become expensive and complicated to set up a dedicated VPN, particularly for users that only require infrequent access or for non-employees. One key distinction of the early SDP vendors was that architecturally, many utilized mainly on-prem hardware and software that sat in the internal network in front of applications and directories.

PHASE 3:

IDENTITY-BASED

The next class of Zero Trust vendors generally evolved from an Identity and Access Management (IAM) background and not surprisingly put forward what was largely an identity-based approach, that leans heavily on their ability to authenticate users and verify devices by leveraging existing technologies for MFA, SSO/IDaaS or PAM.

PHASE 4:

MAN-IN-THE-MIDDLE CLOUD

Content Delivery Network (CDN) vendors are also logical players in Zero Trust, given their highly distributed networks that can be used as a platform to allow employees and partners to access internal applications without a VPN. In effect, vendors that have taken the CDN

approach essentially have a proprietary "man-in-the-middle" cloud network that functions like a proxy in the sense that all traffic must be routed to their cloud for inspection and application of policies, and then passed on to the application or resource. Because CDNs are typically limited to web-based protocols accessed via the browser, some vendors extend this approach into a Network-As-A-Service (NaaS) model. NaaS supports all networking protocols by using VPN clients on devices to set up IPSec tunnels into CDN points of presence. An essential difference between the CDN/NaaS approach and the original SDP vendors is there is less need for on-prem hardware and software.

PHASE 5:

CLOUD-INTEGRATED

The latest stage in the evolution of Zero Trust is what we have come to call the Cloud-Integrated approach. The essential characteristic of this group is that, unlike a "man-in-the-middle" cloud approach where customers rely on a CDN provider's proprietary network, they take advantage the fact that most firms today have made extensive investments in their own cloud infrastructure and likely have either AWS, Azure, GCP, or other cloud providers running their workloads. So, one distinction of the cloud-integrated approach is that it allows firms to leverage those existing cloud investments to deliver a Zero Trust framework.

Another advantage of the cloud-integrated approach arises because the data plane resides in the firms' environment — they have the ability to integrate with the firms' existing enterprise security tools (such as IAM, MDM, EDR, EUBA, PKI etc) to deliver Zero Trust security across a variety of points of ingress and egress.

Cloud-Integrated vendors also aim to meet the scalability requirements of a modern firm that has adopted not only cloud, but also containers and microservices.

AGAIN, ONE OF THE CRITICAL REQUIREMENTS FOR MODERN ZERO TRUST IS TO WORK WITH EXISTING SECURITY TOOLS AND TOUCH POINTS AND NOT FORCE FIRMS TO DESIGN SECURITY PROGRAMS OVER FROM SCRATCH; THIS IS JUST TOO UNWIELDY TO ACCOMPLISH VIA TRADITIONAL GATEWAY APPROACHES.

WHAT'S NEXT FOR ZERO TRUST?

Even though the Zero Trust concept has evolved significantly to keep pace with modern requirements, we are in the very early days of implementing Zero Trust, and there will likely be many new twists and developments in the next few years.

But regardless of what you call it, I believe that Zero Trust could be one of the most significant new developments in security in the past 10 years or more, and I think it will have a huge impact on the industry and also security vendors for years to come.

Garrett Bekker, Principal Analyst, Information Security, 451 Research

Garrett Bekker is a Principal Analyst in the Enterprise Security Practice at 451 Research. He brings a unique and diverse background, having viewed enterprise security from a variety of perspectives over the past 15 years. Garrett spent more than 10 years as an equity research analyst at several investment banking firms, including Merrill Lynch, where he was the lead enterprise security analyst, in addition to covering infrastructure software and networking companies.

451 Research

About 451 Research

451 Research is a leading information technology research and advisory company focusing on technology innovation and market disruption. More than 100 analysts and consultants provide essential insight to more than 2,000 client organizations globally through syndicated research, advisory services and live events. Founded in 2000 and headquartered in New York, 451 Research is a division of the 451 Group. Learn moreand connect with 451 Research on Twitter and LinkedIn.