IMPACT REPORT

Zscaler Private Access aims to simplify the inbound side of security stacks

NOVEMBER 7 2017
BY FERNANDO MONTENEGRO, PATRICK DALY (/ANALYST-TEAM/ANALYST/PATRICK+DALY)

Historically, organizations built their enterprise networks based on the idea of securing the perimeter, largely by designing, buying, implementing and operating their own security controls in-house. As the industry has matured in terms of understanding the role and reliability of external service providers – the booming adoption of cloud-based services is one example – there is greater understanding and acceptance of relying on external service providers, particularly for resource-constrained firms facing a chronic scarcity of skilled security staff.

Zscaler has built a substantial business around helping overworked technology teams outsource the infrastructure and operations needed to secure outbound access to external resources – initially websites and applications. The company has now turned its attention to securing inbound access to internal resources with its Private Access offering, which directly targets a staple of most networks – the venerable firewall/VPN appliance.

The 451 Take

The constant demand to 'do more with less' that affects most enterprise security teams has fueled several industry initiatives around simplifying and automating manual processes, such as incident response and security provisioning. Zscaler offers a portfolio of services aimed at removing the need to own or operate the security stack, and adding support for inbound remote access is a logical extension of Zscaler's current suite of offerings. By simplifying – though not completely eliminating – the security perimeter and securing bidirectional traffic, Zscaler Private Access offers the potential to greatly simplify existing security architectures and operations, if it can overcome the ingrained architectural patterns at its target enterprise customers.

Context

Based in Sunnyvale, California, Zscaler was founded in 2007 by Jay Chaudhry, a serial entrepreneur who was also behind successful security startups CipherTrust (acquired by Secure Computing) (/report-short?entityId=27001), AirDefense (acquired by Motorola Solutions) (/report-short?entityId=54310), CoreHarbor (acquired by USI/AT&T), Air2Web and SecureIT (acquired by VeriSign). With the help of K. Kailash, former chief architect at NetScaler, Chaudhry and his team built a distributed network of processing nodes to support their cloud-based SaaS offering.

The company has received $148m in funding since 2012, with the latest round of $25m led by Google Capital in 2015. It currently has 900 employees, and boasts a renewal rate that indicates customers are renewing at higher levels of service.

Technology

Zscaler's overall proposition is to offer security functionality delivered via a SaaS model, as opposed to traditional on-premises security appliances. In essence, by routing their traffic through Zscaler's cloud-based services (Private Access and Internet Access), customers can implement security controls and manage policies from centralized locations without needing to manage the security products themselves.

To minimize latency, the Zscaler infrastructure consists of multiple datacenter locations distributed across the globe – the company claims over 100 locations – similar to public cloud providers such as AWS, Microsoft Azure and GCP. Customers connect to the Zscaler service via a variety of methods, including generic router encapsulation tunnels and traditional IPsec VPN tunnels for headquarters and branch locations, or proxy redirection via PAC (proxy auto configuration) files. For endpoints not on a protected network, such as remote employees and third-party users external to the organization, Zscaler offers a lightweight client application (Z-App) that requests access to internal applications. The entire service supports multi-tenancy, meaning each customer has access to their segmented view of the broader Zscaler service.

The Zscaler architecture is made up of three major components that are implemented in a high-availability manner: a 'central authority' used for policy definitions and updates; a Zscaler Enforcement Node, which performs the actual inspection of traffic according to policy; and a Nanolog cluster that is used for collecting logs and generating reports. The architecture also uses some supporting servers, such as sandbox servers and PAC file distribution servers, among others.

A customer's Zscaler deployment can also connect to existing corporate data and third-party products. The most common use cases are for leveraging existing IAM sources, such as Microsoft, Okta and Ping (usually via SAML), or logging, with support for SIEM tools from Splunk, IBM and HPE ArcSight. Integrations also exist with other network security offerings, such as Cisco and Juniper for IPS; Akamai for DDoS protection; and Viptela, Cisco, Riverbed and CloudGenix for SD-WAN capabilities.

Products

Until recently, the primary use case for Zscaler was to secure activities performed by customers as they interact with external internet resources. Its Zscaler Internet Access offering covers three major areas of security functionality: access control (firewalling, URL filtering, bandwidth controls and DNS filtering), threat prevention (sandboxing and antivirus) and data protection (DLP and cloud application control features).

The most recent service delivered by Zscaler, Private Access, provides the ability to secure inbound connections by external users (mobile employees, external partners, contractors, etc.) attempting to access internal applications, delivering an alternative to remote access VPNs. As users connect to the Zscaler service, connections are authenticated and an application- and user-specific policy allows access to the target application(s).

Once remote access is granted, rather than connecting directly to the corporate network – as would be the case on a standard remote access VPN – users connect to an intermediate broker, which controls access and stitches together the user and the application. The advantage of this approach is that users are never placed on the network, and the true location of the application – be it on-premises or on an external cloud provider – becomes immaterial.

Competition

When it comes to securing remote access to internal applications, Zscaler competes first and foremost against well-ingrained habits – organizations have leveraged remote access VPNs as a transport mechanism since the first corporate networks were originally built. Zscaler's primary battle is to overcome this traditional mindset of enterprise security, network engineering and operations, and IT architecture. From a vendor perspective, competition stems from myriad remote access VPN vendors that all claim that their approach works just fine. The list of vendors includes, but is not limited to, Pulse Secure, Cisco, Juniper Networks, Palo Alto Networks, Check Point, F5 and Citrix.

As an architectural alternative to VPNs and perimeters, some organizations are considering a 'zero-trust networking' model, which is centered on redesigning the network to assume all connections need to be properly validated. Zscaler's approach may fit into this model. Other companies taking this approach include Google's BeyondCorp, Duo Security's derivative offering DuoBeyond, ScaleFT and others.

VPN replacement is also a possible use case for SD-WAN vendors, although most SD-WAN discussions have been centered on site-to-site VPN replacement, not remote user access, and could therefore coexist with Zscaler Private Access. OPAQ Networks (fka Bat Blue) offers a cloud service as well, although it appears to target a slightly different market segment (focusing on smaller organizations) by leveraging brand names as opposed to the more custom approach that Zscaler has adopted. Cato Networks, Cradlepoint and Aryaka (Smart Access) seem to offer services that potentially compete with Private Access.

For scenarios where the application being protected is available publicly – often in a cloud provider or other SaaS offering – there might be potential competition from cloud access security brokers, such as Symantec (Blue Coat), Forcepoint, Netskope, Oracle CASB Cloud Security and Skyhigh Networks, which aim to provide a variety of security functionality for SaaS, PaaS and (in some cases) IaaS, including application discovery and risk scoring, DLP, encryption, and threat protection. Access control

for cloud applications is also an adjacent area addressed by identity-as-a-service vendors such as Okta, OneLogin, Microsoft, Ping Identity, VMware, Centrify, CA, Simeio, Google (via Bitium), Centrify and SailPoint Technologies.

SWOT Analysis

Strengths

The ability to secure traffic in both directions should provide a more compelling alternative to traditional security stacks. Private Access allows more granular policies for users that would typically be remote access VPN users.

Weaknesses

The proprietary methods used to implement network and security functionality may lag newer approaches in response to threat evolution. The Private Access offering replaces remote access VPNs, but organizations may still require site-to-site VPNs for machine-to-machine communications.

Opportunities

The pace of change in 'new IT,' along with the chronic shortage of security staff, raises the potential benefits of radical simplification of existing security operations. Zscaler fits into that worldview. The adoption of hybrid cloud models and the prevalence of lift-and-shift workloads for corporate applications open the door for mechanisms to control access to those cloudified resources.

Threats

Some of the customers targeted by Zscaler may prefer to deal with vendors that have a more diverse portfolio of security offerings. As applications shift to cloud-native and SaaS models, vendors with different approaches are offering alternative security services and delivery architectures.

Fernando Montenegro (/analyst-team/analyst/Fernando+Montenegro)

Senior Analyst

Patrick Daly (/analyst-team/analyst/Patrick+Daly)

Senior Research Associate

M&A ACTIVITY BY SECTOR

Security / General (24) (https://makb.the451group.com/results?basic_selected_sectors=136)

M&A ACTIVITY BY ACQUIRER

ACCPAC International, Inc. (52) (https://makb.the451group.com/results?basic_acquirers=ACCPAC+International, Inc.)

Air2Web, Inc. (4) (https://makb.the451group.com/results?basic_acquirers=Air2Web,+Inc.)

Akamai Technologies Inc. (19) (https://makb.the451group.com/results?basic_acquirers=Akamai+Technologies Inc.)

Amazon Web Services Inc. [aka AWS] [Amazon.com Inc.] (7) (https://makb.the451group.com/results?basic_acquirers=Amazon+Web Services Inc. [aka AWS] [Amazon.com Inc.])

ArcSight, Inc. (1) (https://makb.the451group.com/results?basic_acquirers=ArcSight,+Inc.)

AT&T Corporation (34) (https://makb.the451group.com/results?basic_acquirers=AT&T+Corporation)

Blue Coat Systems, Inc. (8) (https://makb.the451group.com/results?basic_acquirers=Blue+Coat Systems, Inc.)

Check Point Software Technologies Ltd. (9) (https://makb.the451group.com/results?basic_acquirers=Check+Point Software Technologies Ltd.)

Cisco Systems Inc. (134) (https://makb.the451group.com/results?basic_acquirers=Cisco+Systems Inc.)

Citrix Online [Citrix Systems] (43) (https://makb.the451group.com/results?basic_acquirers=Citrix+Online [Citrix Systems])

Cradlepoint Inc. (2) (https://makb.the451group.com/results?basic_acquirers=Cradlepoint+Inc.)

F5 Networks, Inc. (11) (https://makb.the451group.com/results?basic_acquirers=F5+Networks, Inc.)

Google Inc. (190) (https://makb.the451group.com/results?basic_acquirers=Google+Inc.)

IBM Corporation (169) (https://makb.the451group.com/results?basic_acquirers=IBM+Corporation)

Juniper Networks Inc. (22) (https://makb.the451group.com/results?basic_acquirers=Juniper+Networks Inc.)

Microsoft Corporation (164) (https://makb.the451group.com/results?basic_acquirers=Microsoft+Corporation)

Motorola Computer Group (51) (https://makb.the451group.com/results?basic_acquirers=Motorola+Computer Group)

Okta Inc. (1) (https://makb.the451group.com/results?basic_acquirers=Okta+Inc.)

OneLogin Inc. (3) (https://makb.the451group.com/results?basic_acquirers=OneLogin+Inc.)

Oracle Corporation (126) (https://makb.the451group.com/results?basic_acquirers=Oracle+Corporation)

Ping Identity Corporation [fka Next Identity Corporation] (2) (https://makb.the451group.com/results?basic_acquirers=Ping+Identity Corporation [fka Next Identity Corporation])

Riverbed Technology Inc. [NASDAQ: RVBD] (7) (https://makb.the451group.com/results?basic_acquirers=Riverbed+Technology Inc. [NASDAQ: RVBD])

SailPoint Technologies (2) (https://makb.the451group.com/results?basic_acquirers=SailPoint+Technologies)

Secure Computing Corporation (7) (https://makb.the451group.com/results?basic_acquirers=Secure+Computing Corporation)

SpringSource Inc [fka Interface21] [VMware] (40) (https://makb.the451group.com/results?basic_acquirers=SpringSource+Inc [fka Interface21] [VMware])

Symantec Corporation (50) (https://makb.the451group.com/results?basic_acquirers=Symantec+Corporation)

VeriSign Inc. (20) (https://makb.the451group.com/results?basic_acquirers=VeriSign+Inc.)

Websense Inc. (3) (https://makb.the451group.com/results?basic_acquirers=Websense+Inc.)

Figures shown indicate number of transactions

COMPANY MENTIONS (PRIMARY)
Zscaler (/search?company=Zscaler)

COMPANY MENTIONS (OTHER)
Air2Web , AirDefense , Akamai , ArcSight , Aryaka Networks , AT&T , Amazon Web Services , BeyondCorp , Bitium , Blue Coat , CA Technologies , Cato Networks , Centrify , Check Point , CipherTrust , Cisco , Citrix , CloudGenix , CoreHarbor , Cradlepoint , Duo Security , F5 , Forcepoint , Google , Google Capital , Hewlett Packard Enterprise , IBM , Juniper , Microsoft , Motorola Solutions , NetScaler , Netskope , Okta , OneLogin , OPAQ Networks , Oracle , Palo Alto Networks , Ping Identity Corp , Pulse Secure , Riverbed , SailPoint Technologies , ScaleFT , Secure Computing Corp , SecureIT , Simeio Solutions , Skyhigh Networks , Splunk , Symantec , VeriSign , Viptela , VMware (/search?company=VMware)

CHANNELS
Information Security (/dashboard?view=channel&channel=5)

SECTORS
All / Security / General (/search?sector=136)