DoD Network Security-as-a-Service Transformation

The evolution of information security within the Department of Defense

zscaler™

Background

Post 9/11, the Department of Defense (DoD) realized that its agency networks were too siloed, preventing critical information sharing between agencies and global mission partners. Additionally, each agency continued building out its own network and designing its own security architecture. The practice of building silos continued, and thus resulted in continued duplication of effort and ever-increasing costs for the overall design. As a result of these inefficiencies, the DoD developed the Joint Information Environment (JIE) framework in December 2012. The goal of JIE was to create a unified way in which the DoD agencies would modernize their information technology networks. This framework helped ensure that agencies and mission partners could share information securely while reducing wasted manpower and continued infrastructure expenditures.

> "JIE will have federated networks that are built to common standards and configurations, and expanded use of shared IT infrastructure and enterprise services, which include thin clients, everything-over-IP, e-mail, and cloud services. The services will continue to operate and maintain their portion of the JIE, as well as provide mission-unique capabilities while incorporating shared IT transport services and common applications."
>
> **– Former DoD Chief Information Officer Teri Takai (The Department of Defense Strategy for Implementing the Joint Information Environment, 2013)**

JIE was an ambitious goal and a necessary evolutionary step for the DoD. JIE did not grow from an official program of record, but instead, from end-user demand, formed from the bottom up and summarized in a 15-star supported memo. This demand resulted in a framework agreed upon at the highest levels of command within the DoD and Fourth Estate communities. Within this framework, two of the most difficult technical challenges were the **single security architecture** and **cloud computing.**

Single security architecture (SSA)

The original DoD strategy for implementing JIE noted the following goals and benefits of the SSA:

- Collapsing network security boundaries.
- Reducing the Department's external attack surface.
- Standardizing management, operational, and technical security controls.

The DoD continues to leverage the technical and operational expertise of the National Security Agency (NSA), Defense Information Systems Agency (DISA) and the DoD Components in designing, certifying, and accrediting a standardized set of security suites deployed at optimal locations across the DoD Information Network (DoDIN).

"The number one most important advantage is the ability to actively defend the DoD networks in a time frame that we need to execute cyber defensive operations. What I mean by that is the single security architecture will allow us to understand what's going on across the entire DoD network with global cyber situational awareness to a level that we can't do today."

– Mark Orndorff, DISA's former chief information assurance executive (Slabodkin, 2013)

Two of the most critical components of the SSA are the **Joint Regional Security Stacks** and the **internet access points.**

Joint Regional Security Stacks

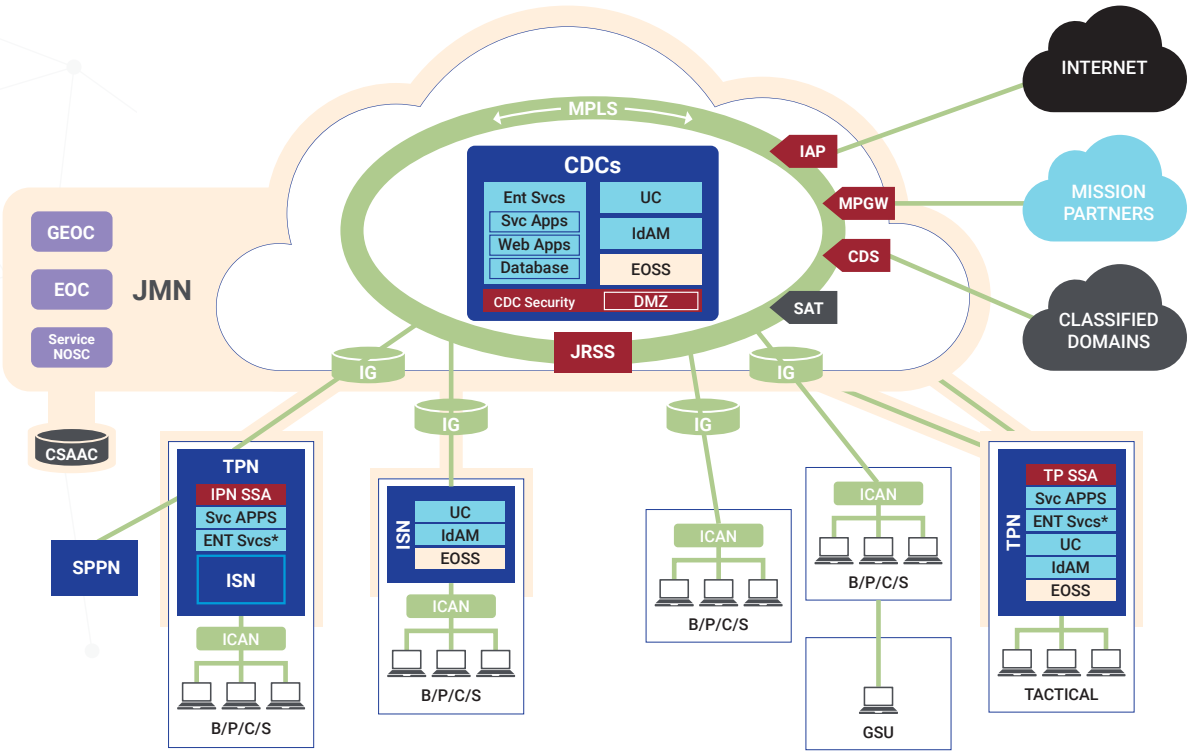
The Joint Regional Security Stacks (JRSS) initiative provides the starting point for the JIE SSA network security stacks that will protect the enterprise network. It will provide the perimeter security for the tenant Community of Interests at the base/post/camp/station (B/P/C/S) and Installation Campus Area Networks. According to the JIE STIG overview, ***"A Joint Regional Security Stack (JRSS) is a fully redundant set of Information Assurance (IA) capabilities, switches, and routers designed to replace multiple local B/P/C/S and Installation Processing Node (IPN) security stacks with a single physical JRSS instance, providing network security and visibility at regional locations and contributing toward realization of the CYBERCOM vision."*** (Team, 2016)

Today, there are 22 redundant JRSS sites around the world—11 Continental United States (CONUS) and 11 Outside Continental United States (OCONUS).

Internet access points

The JIE perimeter defense starts at the Internet Access Point which is a security stack that acts as a secure gateway to the internet from the DoDIN. The IAP also allows approved connections from the internet to the Non-Secure IP Router Network (NIPRNet) of the DoDIN. It provides enterprise security functions, such as Enterprise Email Security Gateway, intrusion detection, firewall, and access controls.

Taken as a whole, the JIE Framework can be illustrated as shown in Figure 1.



JIE CAPABILITIES	
UC	United Capabilities
Ent Svcs	DoD Enterprise Service (*Extended)
IdAM	Identity and Access Management
Svc Apps	Dod Component Applications

JIE GATEWAYS	
IAP	Internet Access Point
MPGW	Mission Partner Gateway
CDS	Cross Domain Solution
SAT	Satellite Communications Gateway

JIE ORGANIZATIONS	
GEOC	Global Enterprise Operations Center
EOC	Enterprise Operations Center
NOSC	Network Operations & Security Center

JIE DATA CENTER & NODS	
CDC	Core Data Center
IPN	Installation Processing Node
ISN	Installation Service Node
TPN	Tactical Processing Node
SPPN	Special Purpose Processing Node

JIE MANAGEMENT NETWORK	
JMN	JIE Management Network
EOSS	Enterprise Operation Support System

JIE SSA COMPONENTS	
JRSS	Joint Regional Security Stacks
CSAAC	Cyber Sit'l Awareness Analytic Cloud
DMZ	Demilitarized Zone

JIE TRANSPORT INFRASTRUCTURE	
IG	Installation Gateway
BAN	Base Area Network
MPLS	Multiportocol Label Switcing

Cloud computing

One of the challenges that was identified early on for the JIE with regards to cloud computing was the management of cyber security as part of the SSA. In response to this challenge, the DoD leverages the Federal Risk and Authorization Management Program (FedRAMP) and the Secure Cloud Computing Architecture (SCCA). The DoD uses FedRAMP for low- and moderately-sensitive data. FedRAMP establishes a standard approach for accessing and authorizing cloud computing services.

According to DISA's public website, SCCA is a suite of enterprise-level cloud security and management services. It provides a standard approach for boundary and application-level security for Impact Level 4 and Level 5 data hosted in commercial cloud environments. The purpose of the SCCA is to provide a barrier of protection between the DoD Information Services Network (DISN) and commercial cloud services used by the DoD while optimizing the cost-performance tradeoff in cybersecurity.

Evolving to a cloud-first approach

The DoD has publicly stated that it wants to get out of the infrastructure business and consume information technology as-a-service from cloud service providers. JIE has been a step in the right direction, but many of the underlying designs are rooted in architectures that were developed more than 10 years ago and have taken nearly a decade to roll out into production and have kept DoD continuing to consume mass amounts of infrastructure. The Army and the Air Force are exploring "Enterprise IT as-a-service" (EITaaS) solutions from commercial solution providers to reduce costs and maintain a competitive edge over their adversaries. Defense Enterprise Office Solution (DEOS) is an example of this evolution to the cloud approach.

According to DISA, "DEOS is an Enterprise Commercial Cloud Service Offering (CSO) that supports the Department of Defense (DoD) Enterprise Collaboration and Productivity Services (ECAPS) strategy to replace existing DoD Unified Capabilities (UC) by acquiring and implementing common enterprise applications and services for joint use across DoD, standardizing cloud adoption, and enabling cross-Department collaboration at local base/post/camp/station (B/P/C/S) levels to include deployed and afloat organizations." (Defense Enterprise Office Solution (DEOS), 2019)

In the past, each agency maintained its own cluster of Microsoft Exchange Servers, which was highly inefficient and expensive for the DoD to maintain. DISA's Defense Enterprise Email was the first step that provided a consolidated DoD Enterprise solution for all of DoD that was hosted and managed by DISA.

> "We think the Enterprise Email System is the core foundation for what we're envisioning as key enablers for the Joint Information Environment."
>
> **– John Hale, DISA's former chief of enterprise applications. (Crank, 2013)**

Defense Enterprise Email was an important first step as it allowed the DoD to migrate from a distributed email solution to a centralized enterprise service and paved the way to moving to a cloud office solution offered completely as a service by a cloud service provider. In the same way, the SSA components of JIE can be provided as a service to the DoD. The DoD has already begun to explore alternative Cloud Access Point solutions, which will allow DoD agencies to efficiently consume IL-4/5 services directly from cloud service providers without the bottlenecks and delays associated with the current JIE SSA implementation. The IAPs, which are hosted and managed by DISA today in 10 locations around the globe, could be provided as-a-service by a cloud service provider offering a FedRAMP IL-2 security stack-as-a-service solution. In moving to a cloud solution, many of the overlapping functionality between the JRSS, IAP and CAP could be consolidated, providing a more efficient and streamlined path of service consumption for the DoD users and warfighters.

Moving from a network-centric to resource-centric framework

The current JIE design is network-centric, meaning that the focus is on securing the network itself with the assumption that once the network is secured, resources and users will be protected as well. This belief has been experientially proven wrong and there many examples of exploitations that have occurred because too much trust was placed on the secured network. What the DoD needs is a modern approach that adopts the zero trust architecture as it is being defined by NIST, which offers this operative definition: ***"Zero trust (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan."*** (Scott Rose, 2020)

The basic tenets of the zero trust architecture defined by NIST are:

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy—including the observable state of client identity, application, and the requesting asset—and may include other behavioral attributes.
- The enterprise ensures that all owned and associated devices are in the most secure state possible and monitors assets to ensure that they remain in the most secure state possible.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture.

The DoD has already begun exploring zero trust solutions and ZTA is becoming the focus for protecting resources from inside the network while solutions, such as the IAP and CAP, protect the perimeter. Once ZTA is embraced and implemented, the network itself becomes just a means of information delivery.

Zscaler – Security delivered as a service

For more than a decade, Zscaler has delivered security as a service to some of the largest commercial enterprises around the world. In late 2018, Zscaler became the first cloud-based security solution to achieve FedRAMP accreditation. Zscaler offers two services – Zscaler Internet Access™ (ZIA™), which is FedRAMP Moderate, and Zscaler Private Access™ (ZPA)™, which is FedRAMP High.

Zscaler Internet Access

Zscaler Internet Access (ZIA) is a secure internet and cloud service provider (CSP) gateway delivered as a service. Think of it as a secure on-ramp to the internet and CSP — all you do is make Zscaler your gateway to the CSP. For military installations, simply set up a router tunnel (IPsec) to the closest ZIA Public Service Edge (formerly known as Zscaler Enforcement Node). For mobile employees, you can forward traffic via our lightweight Zscaler Client Connector (formerly known as Zscaler App) or PAC file.

The main function of the IAP and CAP within the SSA is to provide a comprehensive and robust security stack to protect the DISN from the internet and CSP, respectively. ZIA has a proven track record of providing this type of protection for its customers worldwide. ZIA sits between your users and the internet or CSP, inspecting every byte of traffic inline across multiple security techniques, even within SSL. You get full protection from web, internet and cloud threats.

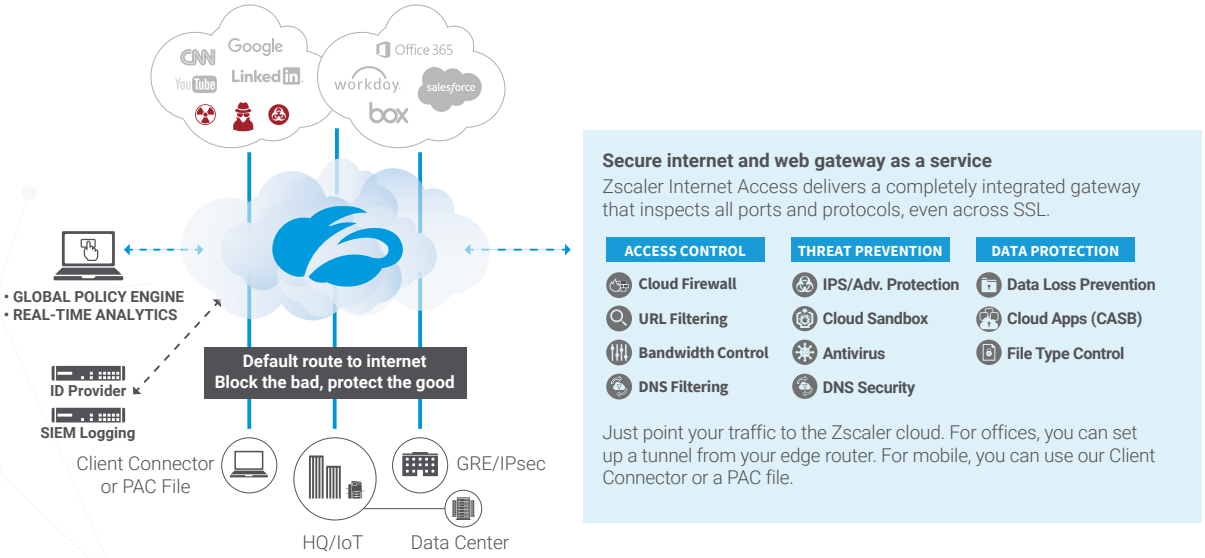


Figure 2 - Zscaler Internet Access

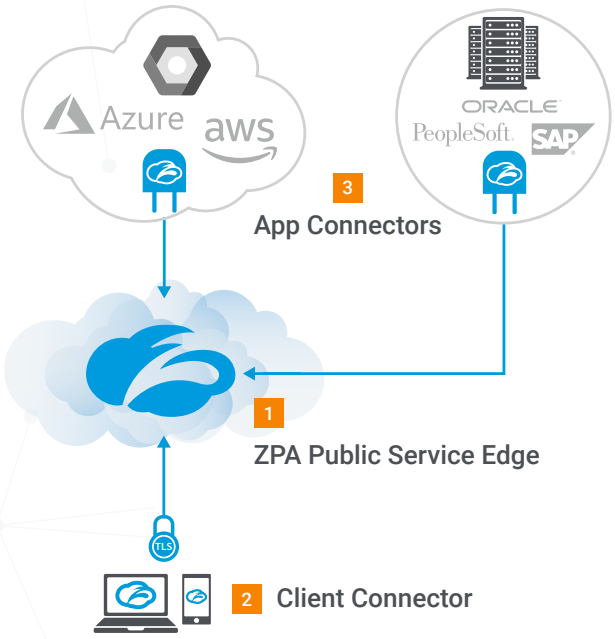
Zscaler Private Access

ZPA is a FedRAMP High/IL-4 cloud service that provides zero trust, secure remote access to internal applications running in a cloud or private data center. With ZPA, applications and services are never exposed externally, making them completely invisible to unauthorized users. The service enables the applications to connect to users via inside-out connectivity vs. extending the network to them.

Zero trust access is based on four key tenets:

- Application/service access no longer requires access to the network or use of VPN.
- Inside-out connections ensure apps and services are invisible to unauthorized users.
- App segmentation, not network segmentation, connects users to a specific app or service and limits lateral movement.
- Secure network communication is achieved via end-to-end encrypted TLS tunnels.

ZPA provides a simple, secure, and effective way to access internal services. Access is based on policies created by the IT admin within the ZPA Admin Portal and hosted within the Zscaler cloud. On each user device, a piece of software called Client Connector is installed. Client Connector ensures the user's device posture and extends a secure microtunnel out to the Zscaler cloud when a user attempts to access an internal service.



Zero Trust Architecture

1 ZPA Public Service Edge
- Brokers a secure connection between Client Connector and an App Connector
- Hosted in cloud
- Used for authentication
- Customizable by admins

2 Client Connector
- Mobile client installed on devices
- Requests access to an app

3 App Connector
- Sits in front of apps in Azure, AWS, and other public cloud services
- Listens for access requests to apps
- No inbound connections

Figure 3 - Zscaler Private Access

Both services integrate with the DoD's existing identity provider via an industry standards-based SAML 2.0 connection and also have the ability to stream transaction logging information to the DoD's SIEM architecture. This means that Zscaler will integrate with the DoD's existing cybersecurity platform and big data initiatives. Both ZIA and ZPA can be extended on-premises allowing for highly efficient traffic engineering. With ZIA providing cloud-based protection at the perimeter of the DoDIN, and ZPA providing a zero trust architecture to protect connections within the DoDIN, the greatly simplified architecture looks as follows:

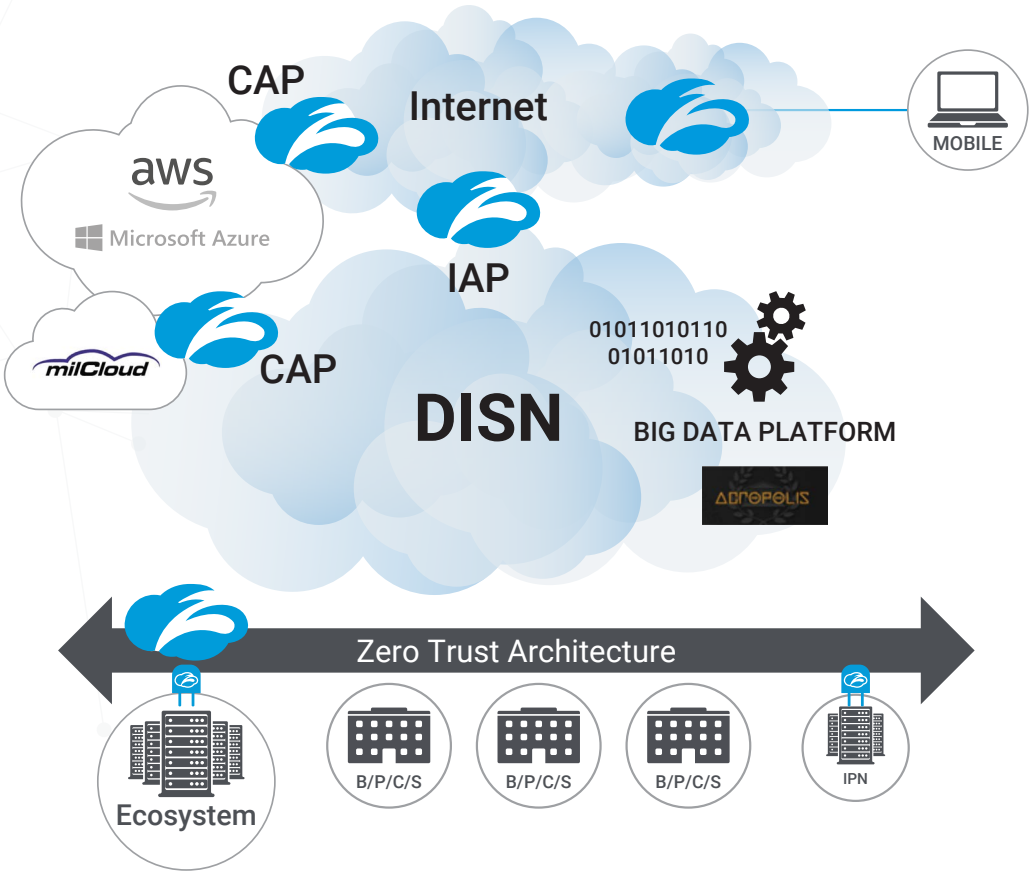


Figure 4 - JIE SSA delivered as a service

Stronger through partnerships

Zscaler provides a robust and mature security-as-a-service platform but leverages tight integration with industry partners to ensure that the service can be easily deployed and integrated for a best-of-breed overall solution. Zscaler performs some basic device posture checking as part of the ZPA service and takes that capability further through integration with endpoint detection and response (EDR) companies, such as CrowdStrike, Carbon Black and SentinelOne. By integrating with leading industry partners, Zscaler ensures that the EDR capability is active on the endpoint before connecting a user to any resources. ZIA and CrowdStrike also share threat intelligence between their clouds, meaning a threat signature detected by Zscaler anywhere around the world can be detected on an endpoint subscribed to the CrowdStrike Falcon service. Zscaler also integrates with a variety of SIEM vendors, such as Splunk, Elastic, ArcSight, and others to make it easy for those solutions to ingest our real-time streaming data. While Zscaler provides inline cloud access security broker (CASB) features, ZIA also has integration with third-party CASB solutions, such as Microsoft Cloud App Security (MCAS) and McAfee MVISION.

Conclusion

JIE was an innovative concept that took the DoD from a highly fragmented and siloed architecture, in which each agency within the DoD managed its own cybersecurity strategy, to an architecture in which there is a unified single security architecture. The more than 190 agency security stacks located at the B/P/C/S around the globe were replaced by a couple dozen stacks centrally managed by the DISA. The secure cloud compute architecture of the SSA provided a security framework for the adoption of cloud services from commercial cloud service providers.

Having taken the first step of consolidating security under a unified security architecture, the DoD is ready to begin the next transformational step, moving from managing and maintaining that architecture itself, to having it provided as a service. With a cloud-based security stack being delivered as a service, Zscaler is positioned to provide the perimeter security that today is being delivered by the IAP and CAPs. The zero trust framework of Zscaler, combined with cloud-based EDR solutions, can replace the overly complex and expensive regional security stacks that have proven to be a major bottleneck to performance. The benefits for the DoD for transforming JIE to an as-a-service model will be realized in cost savings, greater scalability, better performance for the end user and warfighter, and ultimately in a greater cybersecurity capability.

References

Crank, T. M. (2013). DISA's Enterprise Email Reaches 1 Million Users. DoD News.

Defense Enterprise Office Solution (DEOS). (2019, Febuary). Retrieved from www.disa.mil.

Scott Rose, O. B. (2020). Zero Trust Architecture.

Slabodkin, G. (2013, Jul 19). Defending DOD networks with a single security architecture. Defense Systems.

Team, S. I. (2016). Joint Regional Security Stack (JRSS) Engineering Design Specification (EDS).

(2013). The Department of Defense Strategy for Implementing the Joint Information Environment. US Department of Defense.

About Zscaler

Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a multitenant, distributed cloud security platform that protects thousands of customers from cyberattacks and data loss. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com