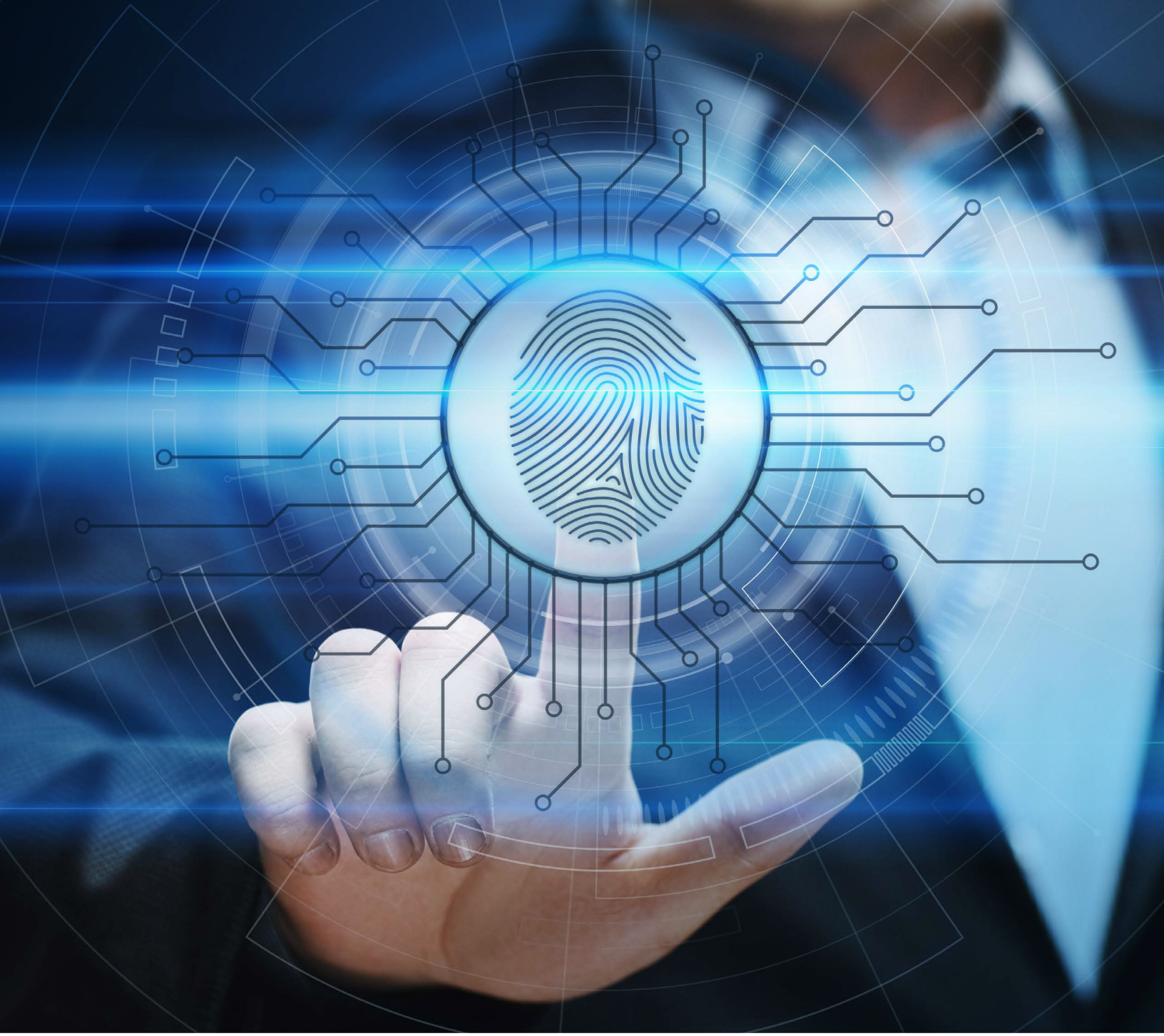


Zero Trust Architecture: Modernizing Federal Security from the Endpoint to the Application

Strengthen your agency's security protection, detection, and remediation

zscaler™

CROWDSTRIKE

Both defense and civilian government agencies face an unprecedented challenge in securing data as the COVID-19 pandemic has created a rapid surge in remote working and connections with non-enterprise devices.

Agencies already in the midst of modernization and cloud migration efforts, increasingly sophisticated cyberattacks, and complex systems and work environments must now figure out how to manage these challenges on an accelerated schedule and while staying within their budgets.

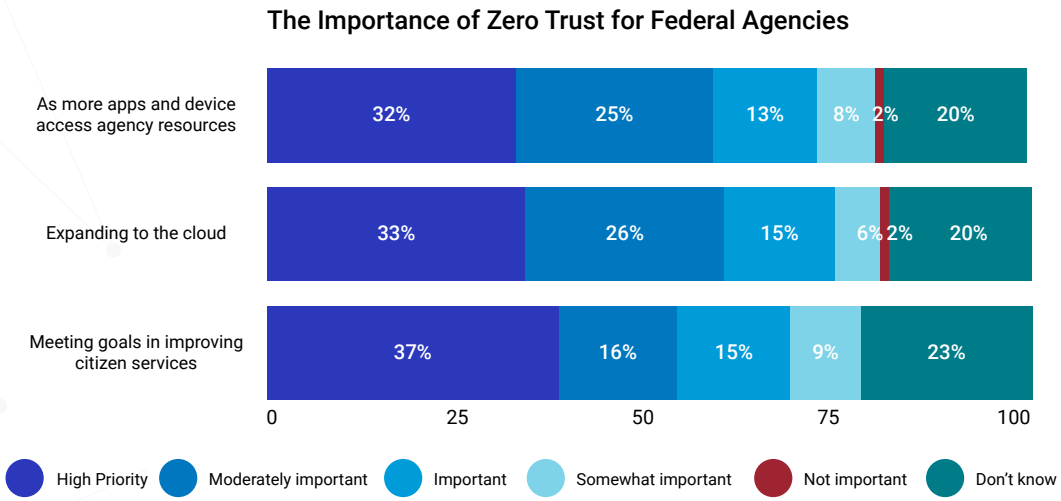
Zero Trust Architecture Offers a Better Approach

According to the Gartner Market Guide for Zero Trust Network Access, "Users and applications are already in the cloud. Hence, secure access capabilities must evolve to cloud delivery, too…ZTNA provides adaptive, identity-aware, precision access. Removing network location as a position of advantage eliminates excessive implicit trust, replacing it with explicit identity-based trust."

The National Institute of Science and Technology (NIST) offers this operational definition of zero trust:

> 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.

In November 2019, FedScoop conducted research into the government's shift to identity-centered access and perceptions of zero trust strategies[1]. The research showed that the majority of agencies believe zero trust strategies are a high priority.



Question: What challenges are keeping your agency from adopting a zero-trust strategy? (Select up to three)

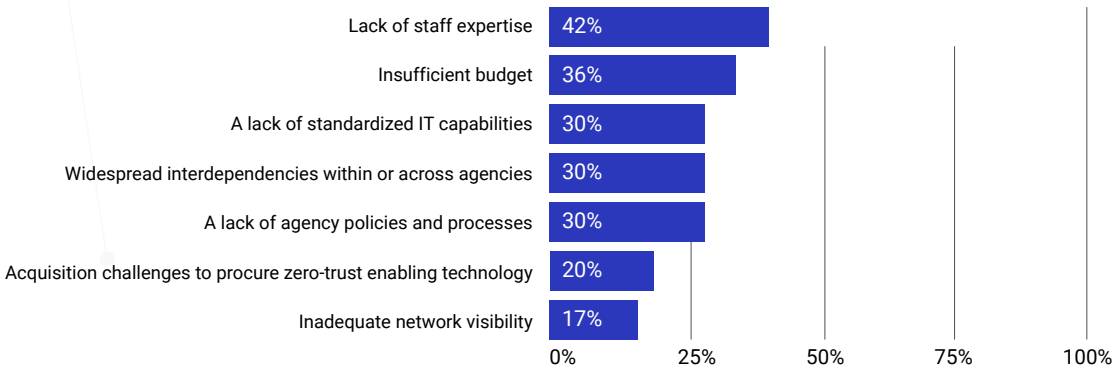
Source: "Security Without Perimeters: Government's Shift to Identify Centered Access," FedScoop, November 2019

[1] "Security Without Perimeters: Government's Shift To Identity-Centered Access," FedScoop, November 2019

The research also showed that agencies with a Federal Identity, Credential, and Access Management (FICAM) strategy to meet U.S. White House Office of Management and Budget (OMB) policy requirements are more likely to prioritize zero trust strategies. For example, 90 percent of respondents with a FICAM strategy rate zero trust strategies as important as the number of apps and devices across agency resources increases, vs. 41 percent of those without a FICAM strategy.

Despite the importance of zero trust strategies, agencies face obstacles in implementing them—most notably, inexperienced staff to manage the requirements. While this research is pre-pandemic, and some of these numbers have likely shifted, it is still clear that there are real challenges in implementing zero trust strategies.

Obstacles to adopting a zero-trust strategy



Question: What challenges are keeping your agency from adopting a zero-trust strategy? (Select up to three)
Source: "Security Without Perimeters: Government's Shift to Identify Centered Access," FedScoop, November 2019

This white paper explains the unique risk factors for federal agencies, what a superior zero trust framework includes, and how cloud and endpoint security can join together to strengthen security protection, detection, and remediation.

Risk Factors for Federal Agencies

"In line with the federal government's updated approach to modernization, it is essential that agencies' ICAM strategies and solutions shift from the obsolete Levels of Assurance (LOA) model toward a new model informed by risk management perspectives, the federal resource accessed, and outcomes aligned to agency missions."

–White House Memorandum for Heads of Executive Departments and Agencies, May 21, 2019[2]

In May 2019, the White House directed federal agencies to change their approach to security. The standard "trust but verify" was no longer practical given emerging threats.

[2] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

As shown below, federal agencies have multiple risk factors underscoring the need to shift to a more modern approach:

- On-premises security solutions are complex to deploy, manage, and maintain. They require training IT and security experts to configure these systems correctly, and they cannot quickly scale — something agencies cite as the primary obstacle to implementation.
- Appliance-based security systems have different refresh cycles, which require upfront CapEx investments and cause constant distraction to an agency's mission during upgrade processes.
- With remote users connecting to the cloud directly, the risk to government data increases due to a lack of visibility into these activities. Moreover, the traditional VPN approach impacts users and their experiences as they are repeatedly connected and disconnected from the VPN to balance productivity and the required secure access to mission-critical applications.
- A bring-your-own-device (BYOD) approach introduces unmanaged devices onto government networks, increasing the risk of compromise and data leakage. Yet, in the new COVID reality, people will need to use their own devices, and often their home networks, to do agencies' work.
- Traditional security solutions cannot detect advanced threats effectively and timely. While the volume of attacks grows daily and tactics become more sophisticated, federal agencies cannot hire cybersecurity experts fast enough to respond.
- Focusing on discrete components of the enterprise, rather than as an entire ecosystem, adds cost, complexity, and risk.

Beginning the journey to a zero trust environment

The legacy security model no longer fits the security requirements of the cloud era. While security professionals could trust the traditional "Walled Garden," which is on-prem, contained, and monitored, applications are now in the cloud and employees are working remotely. Because of these changes, "trusted networks" no longer exist.. Thus, the focus should be to gain visibility and protect endpoints and access to applications along with the data in-between. Gone are the days when VPN-based, all-or-nothing, access control was sufficient; however, one cannot protect what one cannot see outside of premises. With the internet becoming the data network for everyone, cloud-native zero trust is the better model for protecting endpoints and applications from end-to-end.

Implementing a zero trust strategy

The preceding sections focused on the federal Government recognizing that they need to move from a "trust but verify" security posture to one of zero trust.

Zero trust is a security paradigm centered around protecting data by having *zero implicit trust with least privilege access based on required data flows.*

This section will focus on the components needed to implement an effective zero trust strategy.

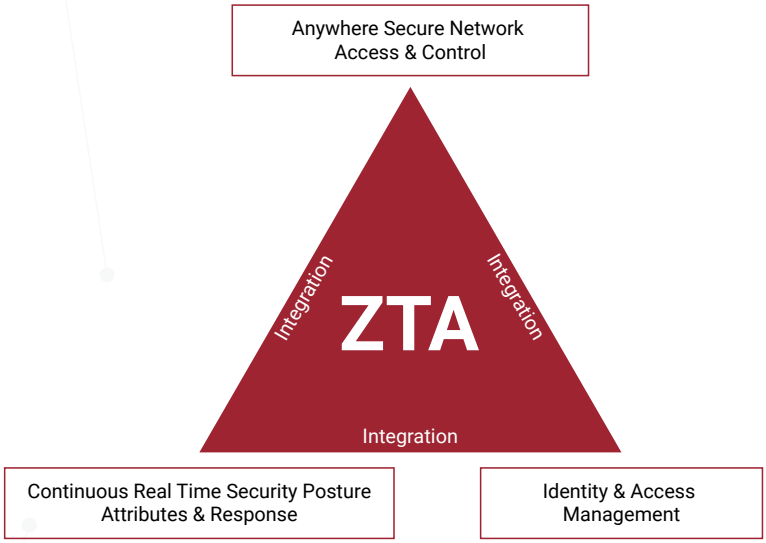
A zero trust strategy is a proactive approach to security; however, zero trust isn't inherently cloud-native, which may leave agencies vulnerable despite believing they are protected. Cloud-native approaches have the advantage of being elastic and scalable. These approaches can respond to sudden surges in demand and are also better at providing consistent policy-based security on multiple factors, allowing users to access applications from anywhere, at any time, with superior threat intelligence gathered from a large user community.

How to achieve a superior zero trust strategy

In order to achieve a superior zero trust strategy, it's important to have at least three key elements to ensure that granular, least privilege policies can be constructed and enforced. These critical elements are:

- Continuous real-time security posture attributes and response
- Identity and access management
- Anywhere secure network access and control

These elements connect the dots from the endpoint—whether a desktop or a mobile device—all the way to the application, and give information security administrators better visibility.



Continuous real-time security posture attributes and response

Zero trust access starts with securing the endpoint that will be used to access the resource and continually reassessing the device's security posture. Adding machine learning and user behavior analytics strengthens the ability of zero trust access to control, monitor, protect, and respond quickly to threats, while enabling agencies to securely provide access to resources for authorized users.

Identity and access management (IAM)

Zero trust requires a strong identity management component that utilizes open standards such as SAML 2.0, which supports multifactor authentication.

Anywhere secure network access and control

In a zero trust architecture, you begin with zero implicit trust and then gain trust as you successfully pass a series of security policy checkpoints Access policy must be adaptive and take into account several factors, such as the security posture of the client's device, the user's identity, the user's alignment with organizations, departments, or groups, the user's current location, the time of day, and the application sensitivity itself. Secure network access means that the connections from the end user to the application should use strong, FIPS 140-2-compliant cryptography and protect against interception or replay attacks.

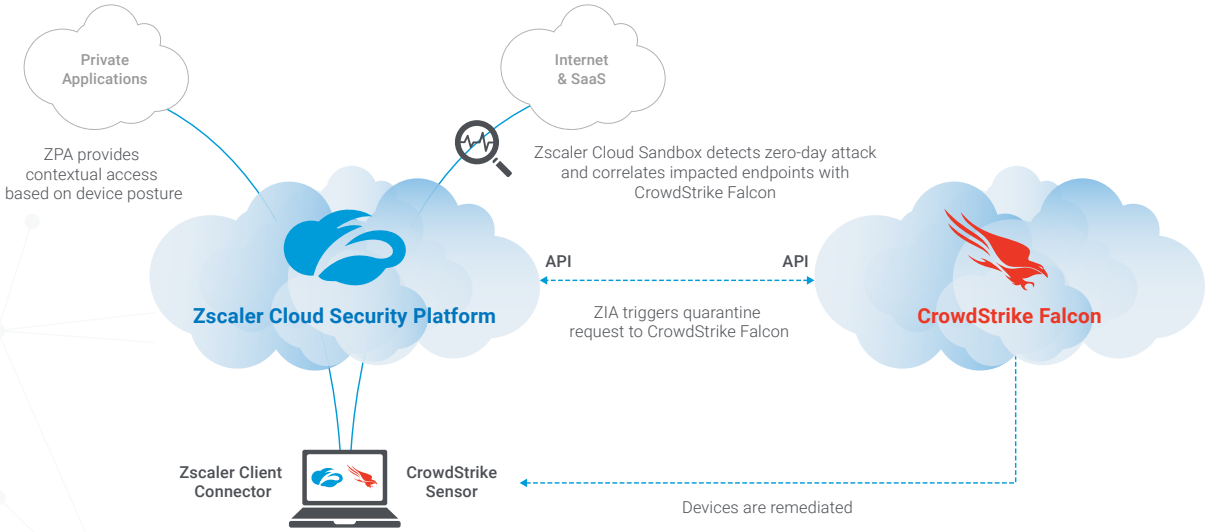
The Zscaler™ and CrowdStrike® integration

Zscaler Private Access™ (ZPA™) and CrowdStrike Falcon Platform

Conditional access based on device posture: ZPA allows conditional access to business-critical internal applications only via endpoint devices running the lightweight CrowdStrike Falcon® sensor. This prevents non-compliant or rogue endpoints from accessing sensitive applications and data. Instead of traditional all-or-nothing access controls solely based on authentication, this integration implements zero trust access control by taking device configuration into consideration. Moreover, administrators can define which applications to protect based on this policy.

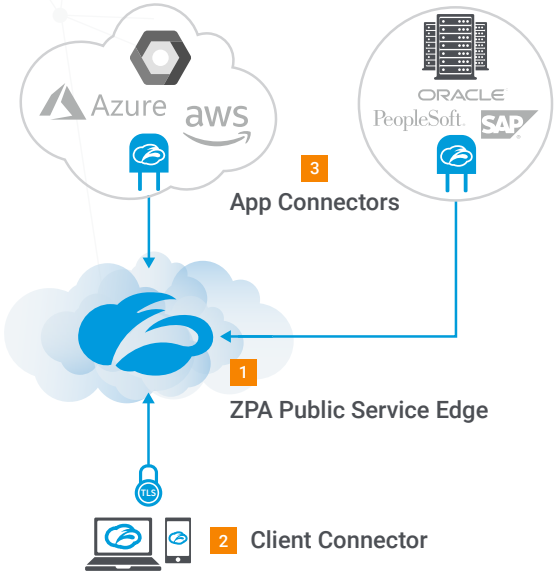
Zscaler Internet Access™ (ZIA™) and CrowdStrike Falcon Platform

Correlating zero-day detection with the endpoint environment for faster response: Zscaler Advanced Cloud Sandbox sits inline at the cloud edge to detect zero-day threats. Through API integration, the resulting report is correlated with endpoint data from CrowdStrike to automatically identify the impacted endpoints within the entire environment and facilitate a one-click trigger to the CrowdStrike Falcon platform for rapid quarantine action. Furthermore, the administrator can pivot from the Zscaler Insight Log to the Falcon console with automatically populated data for endpoint investigation.



With Zscaler Internet Access and CrowdStrike Falcon working together, you can ensure that an endpoint running the CrowdStrike sensor may be secured. Now, Zscaler Private Access can validate the presence of the CrowdStrike sensor and leverage that information as part of the policy decision to grant a user access to a sensitive application. When combined with other policy attributes, such as user identity, organizational alignment, location, time of day, etc., you can achieve adaptive granular policy decision and enforcement capabilities within your environment.

In the cloud and in private data centers, Zscaler Private Access utilizes a lightweight App Connector to front-end hosted applications. The App Connector establishes an outbound, encrypted, and mutually authenticated connection with the Zscaler cloud. No inbound communication to the data center is needed, which prevents the possibility of distributed denial-of-service (DDoS) attacks or lateral reconnaissance activities that are possible when you expose your data center infrastructure to the open internet. The Zscaler Private Access service acts as an application broker for client requests, ensuring that only users, authorized by policy, are able to reach a resource on the back end. If policy grants access, user connections are brokered in the Zscaler cloud and secured end-to-end using Federal Information Processing Standard (FIPS)-compliant encryption.



Zero Trust Architecture

1 ZPA Public Service Edge
- Brokers a secure connection between a 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

Key benefits of the Zscaler and CrowdStrike integration

- **Enabled zero trust access control:** Zscaler Private Access is the first and only zero trust remote access solution to achieve FedRAMP-High Authorization. ZPA's integration with CrowdStrike ensures that users are accessing business-critical private applications only from endpoints that have the CrowdStrike sensor installed and running. Obfuscating HTTP ports reduces the attack surface and removing the need for VPN vastly improves user experiences while strengthening endpoint security.
- **Easier reporting, faster response and remediation:** Comprehensive visibility from the network and endpoint platforms provides a more complete view of the threat landscape. One-click drill-down and pivot from the network to the endpoint, as well as cross-platform workflow, make investigation and response faster and more efficient.
- **Reduced impact of advanced threats:** Zscaler Advanced Cloud Sandbox blocks zero-day malware at the network and quarantines the host before it reaches the endpoint. In addition, the Zscaler inline and integrated security stack—including SSL inspection, Cloud Firewall, web proxy, Cloud Sandbox, and CASB and data protection—combined with CrowdStrike's advanced endpoint protection and analytics—can significantly reduce response times and business loss caused by security breaches and downtime.

- **Reduced complexity:** Zscaler and CrowdStrike are 100% cloud-native. The combined offering is easy to implement, always up-to-date, cost-efficient, agile, and rapidly scalable. Security policies are applied consistently for all users and all apps for all locations, vastly reducing the risk of misconfiguration of disparate on-premises applications in multiple locations. There's good reason that both companies are Gartner MQ Leaders in their fields.

Conclusion

The White House memorandum noted, "While hardening the perimeter is important, agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access Federal resources made by users and information systems."

A cloud-based zero trust strategy that combines robust identity access and endpoint security will ensure that agencies can follow government mandates, protect their data, support their IT teams, and meet budget requirements.

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**.

About CrowdStrike
CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

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