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

Strengthening and modernizing your agency's security protection, detection, and remediation.

CROWDSTRIKE | zscaler™

Both defense and civilian government agencies face an unprecedented challenge in securing data, as the COVID-19 pandemic 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 stay within their budgets.

Zero Trust Architecture Offers a Better Approach

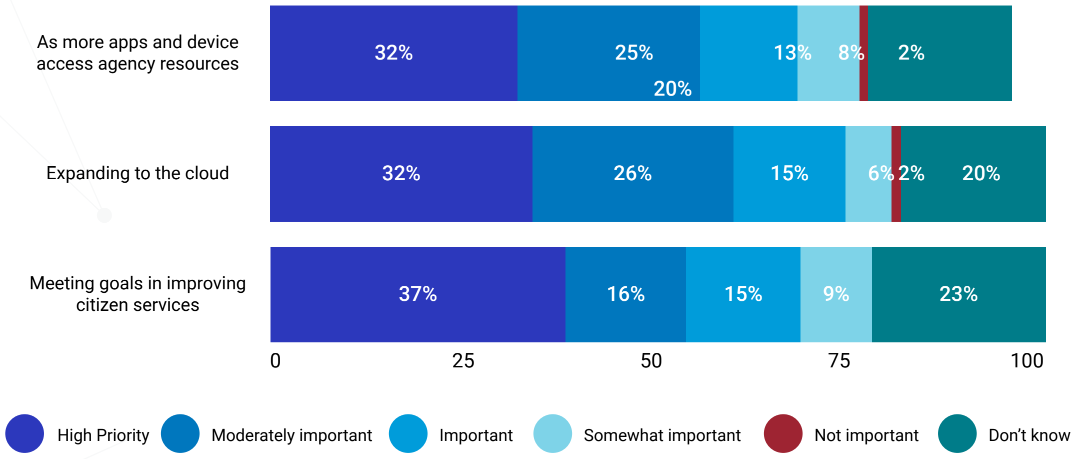
According to the Gartner Market Guide for Zero Trust Network Access, "Users and applications are already in the cloud. Hence, secure access capabilities must evolve to cloud delivery, too…ZTNA provides adaptive, identity-aware, precision access. Removing network location as a position of advantage eliminates excessive implicit trust, replacing it with explicit identity-based trust."[1]

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 its perception of zero trust strategies. The research showed that most agencies believe zero trust strategies are a high priority.[2]

The Importance of Zero Trust for Federal Agencies



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

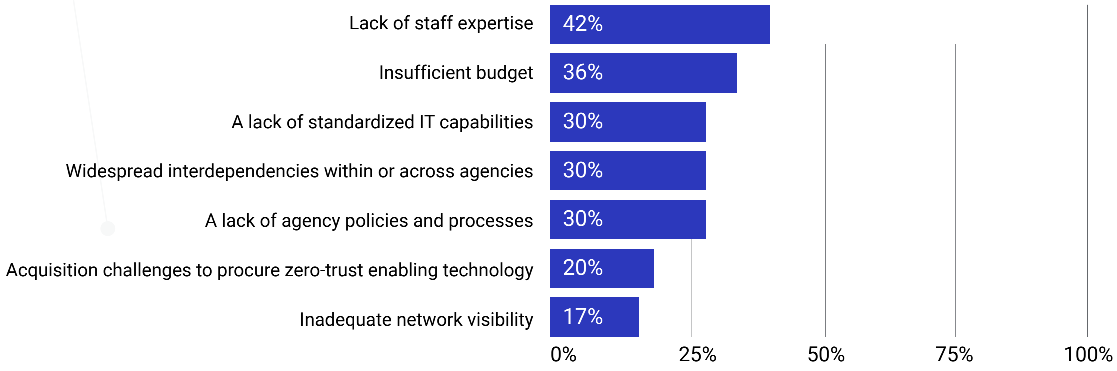
[1] Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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

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

Despite the importance of zero trust strategies, agencies face obstacles in implementing them—most notably, relying on 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.

Obstacles to adopting a zero-trust strategy



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

This white paper explains the unique risk factors federal agencies face, 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—requiring upfront CapEx investments and can cause constant distraction away from 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 (virtual private network) approach impacts users and their experiences as they are repeatedly connected and disconnected from the VPN to balance productivity with the required secure access to mission-critical applications.
- A bring-your-own-device (BYOD) approach introduces unmanaged devices into government networks, increasing the risk of compromise and data leakage. Yet, in the new COVID reality, people often need to use their own devices and their home networks to do agencies' work.
- Traditional security solutions cannot detect advanced threats effectively and in a timely manner. 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 on the 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" approach — which is on-premises, 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, but one cannot protect what one cannot see outside of the premises. With the internet becoming the data network for everyone, cloud-native Zero Trust is the better model for protecting endpoints and applications 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 rooted in zero trust.

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

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

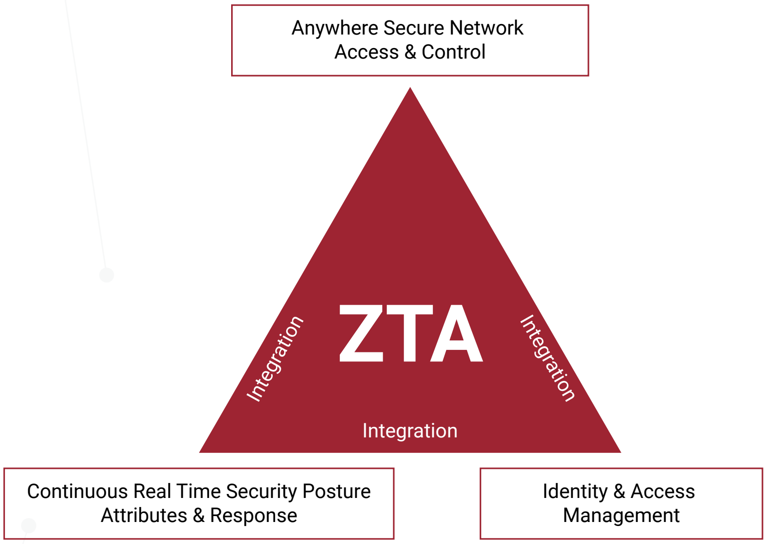
A zero trust strategy is a proactive approach to security, but zero trust isn't inherently cloud-native, which may leave agencies vulnerable despite believing they are protected. Cloud-native approaches have the advantage of being elastic and scalable. These approaches can respond to sudden surges in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

How to Achieve a Superior Zero Trust Strategy

Achieving a superior zero trust strategy requires at least three key elements to ensure that granular, least-privilege policies can be effectively created and enforced. These critical elements comprise the following:

- Continuous real-time security posture attributes and response
- Identity and access management
- Secure network access and control regardless of location

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


Anywhere Secure Network Access & Control
ZTA
Integration
Integration
Integration
Continuous Real Time Security Posture Attributes & Response
Identity & Access Management

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 that support multifactor authentication (MFA). In addition, SCIM which allow for auto provisioning and updates for accurate and timely policy remapping.

"Anywhere Secure" Network Access and Control

With a zero trust architecture, users begin with zero implicit trust and then gain trust as they successfully pass a series of security policy checkpoints. Access policy must be adaptive and consider 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 (Federal Information Processing Standard) 140-2-compliant cryptography and protect against interception or replay attacks.

The Zscaler and CrowdStrike Integration

ZERO TRUST ACCESS TO PRIVATE APPS

STEP 1: CrowdStrike Falcon evaluates device posture with Zero Trust Assessment

CrowdStrike Falcon collects OS and sensor settings from an endpoint device and calculates its ZTA score. Any changes in settings will automatically trigger a recalculation of the ZTA score. By comparing the ZTA score with the organization's baseline score, CrowdStrike can measure the health of the user's device relative to the organization's baseline and recommended best practices over time.

STEP 2: Zscaler Private Access™ (ZPA™) implements access policies

ZPA™ implements zero trust access policies in two layers. First, Zscaler Client Connector checks if the CrowdStrike Falcon sensor is running on the endpoint device. Next, Client Connector reads the device's ZTA score and compares it against the policy threshold defined for selected private applications. If these conditions are met, access to applications is granted. If not, then access is not given. Access policies on the Zscaler dashboard can be adjusted to change the threshold of the score based on the organization's requirements.

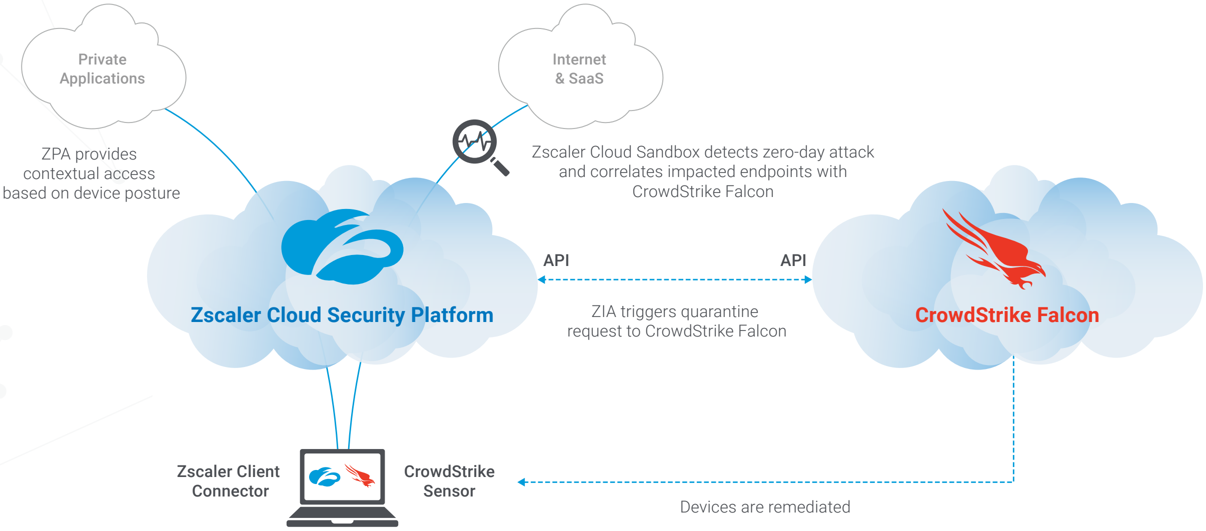
ZERO-DAY DETECTION AND REMEDIATION

STEP 1: Zscaler Cloud Sandbox correlates zero-day malware detection with CrowdStrike Falcon telemetry

The Zscaler Cloud Sandbox sits inline at the cloud edge to detect zero-day threats. Malicious files are detonated in the sandbox, creating a report that is correlated with endpoint data from Falcon. This ties the threat detected at the network edge with endpoint data.

STEP 2: Administrators quarantine and remediate threats with a cross-platform workflow

The correlation automatically identifies infected endpoints within the entire environment and facilitates a one-click trigger to the Falcon platform for rapid quarantine action. Administrators can pivot from the Zscaler Insight Log to the Falcon console with automatically populated data for endpoint investigation.


Private Applications
Internet & SaaS
ZPA provides contextual access based on device posture
Zscaler Cloud Sandbox detects zero-day attack and correlates impacted endpoints with CrowdStrike Falcon
API
API
Zscaler Cloud Security Platform
ZIA triggers quarantine request to CrowdStrike Falcon
CrowdStrike Falcon
Zscaler Client Connector
CrowdStrike Sensor
Devices are remediated

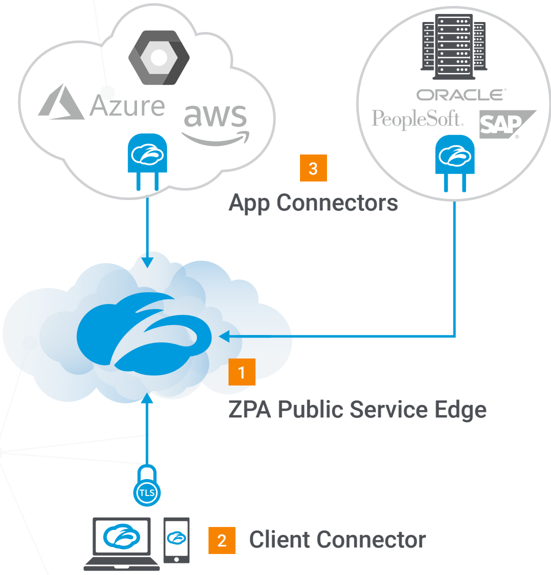
AUGMENTING ZSCALER INLINE BLOCKING WITH CROWDSTRIKE THREAT INTELLIGENCE

STEP 1: Zscaler ingests a custom blocklist

Zscaler retrieves CrowdStrike threat intelligence that's already available within a specific customer environment and automatically ingests high-confidence threat data such as URLs, IP addresses and domains to a custom blocklist. These shared indicators of compromise (IOCs) in the custom blocklist are in addition to the Zscaler global threat feeds and are specific to a customer's own environment. Attempts to access such URLs/IPs/ domains are proactively blocked as a result of the IOC sharing. ZIA (Zscaler Internet Access) and CrowdStrike Falcon ensure the same threat vector is blocked inline by Zscaler before it can infect other endpoints.

STEP 2: Administrators evaluate the severity of activity

The Zscaler Zero Trust Exchange connects to CrowdStrike's event stream APIs to retrieve high-severity IOCs for a specific customer and automatically adds this to the custom blocklist. ZIA can then block threats based on this continuous update of IOCs, enabling faster threat prevention across cloud applications and endpoints.



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. Zscaler Private Access' integration with the CrowdStrike Falcon platform ensures that users are accessing business-critical private applications only from endpoints that have the Falcon agent 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. A 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 before it reaches the endpoint. In addition, the Zscaler inline and integrated security stack—including SSL inspection, Cloud Firewall, web proxy, Cloud Sandbox, 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, apps, and locations, vastly reducing the risk of misconfiguration via disparate on-premises applications in multiple locations. There's a 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.

Spotlight on CrowdStrike: Falcon Endpoint Security and Device Control

The CrowdStrike Falcon cloud-scale platform analyzes incoming real-time data on a massive scale, crowdsourcing upward of 1 trillion endpoint-related events per day as they occur across the global CrowdStrike community. This stream of real-time threat information drives the proprietary AI-powered CrowdStrike Threat Graph® database, dynamically scrutinizing event-based data to detect anomalous behavior based on indicators of attack (IoAs) in addition to IoCs. CrowdStrike provides customers with protection and visibility across the entire threat lifecycle, no matter where the endpoints and workloads are located.

Unlike systems that rely solely on IOCs, which appear only after a breach has already occurred, IOAs are effective regardless of whether malware is present. This allows customers to detect and prevent attacks while they are still in progress and before data is exfiltrated.

Spotlight on CrowdStrike: Falcon Identity Threat Protection (ITD)

Secure Active Directories: CrowdStrike Falcon ITD improves AD security hygiene with continuous monitoring for credential weakness, access deviations, and password compromises, providing dynamic risk scores for every user and service account. Monitor Access Activity reduces the attack surface by identifying over-permissioned admins, misused service accounts, and anomalous user behavior in virtual desktop infrastructure (VDI), remote-desktop attempts, and insider lateral movement and elevation of privilege requests.

Spotlight on Zscaler: Zscaler Zero Trust Exchange

The Zscaler Zero Trust Exchange enables fast, secure connections and allows your employees to work from anywhere using the internet as the corporate network. Based on the zero trust principle of least-privileged access, it provides comprehensive security using context-based identity and policy enforcement.

The Zero Trust Exchange operates across 150 data centers worldwide, ensuring that the service is close to your users, co-located with the cloud providers and applications they are accessing, such as Microsoft 365 and AWS. It guarantees the shortest path between your users and their destinations, providing comprehensive security and an amazing user experience.

Spotlight on Zscaler: Zscaler and TIC

Zscaler's TIC in the Cloud is an innovative approach that recognizes the secure and trusted user. This means wrapping the security policy around the user rather than the network, enabling agencies to route traffic direct to the cloud through their choice of internet connection with no additional hardware required. Further, this approach lets authorized users securely and efficiently access data on their smartphones, laptops, tablets, and more. Users are protected wherever they go.

The Zscaler™ multi-tenant Cloud Security Platform and "TIC in the Cloud" approach meet TIC 3.0 guidelines. As agencies work to meet modernization goals of shared services, mobile workforce enablement, improved FITARA scores, and more, Zscaler powers the shift to a modern, direct-to-cloud, zero trust architecture, regardless of device or user location.

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, 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 5 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.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

FREE TRIAL BANNER

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