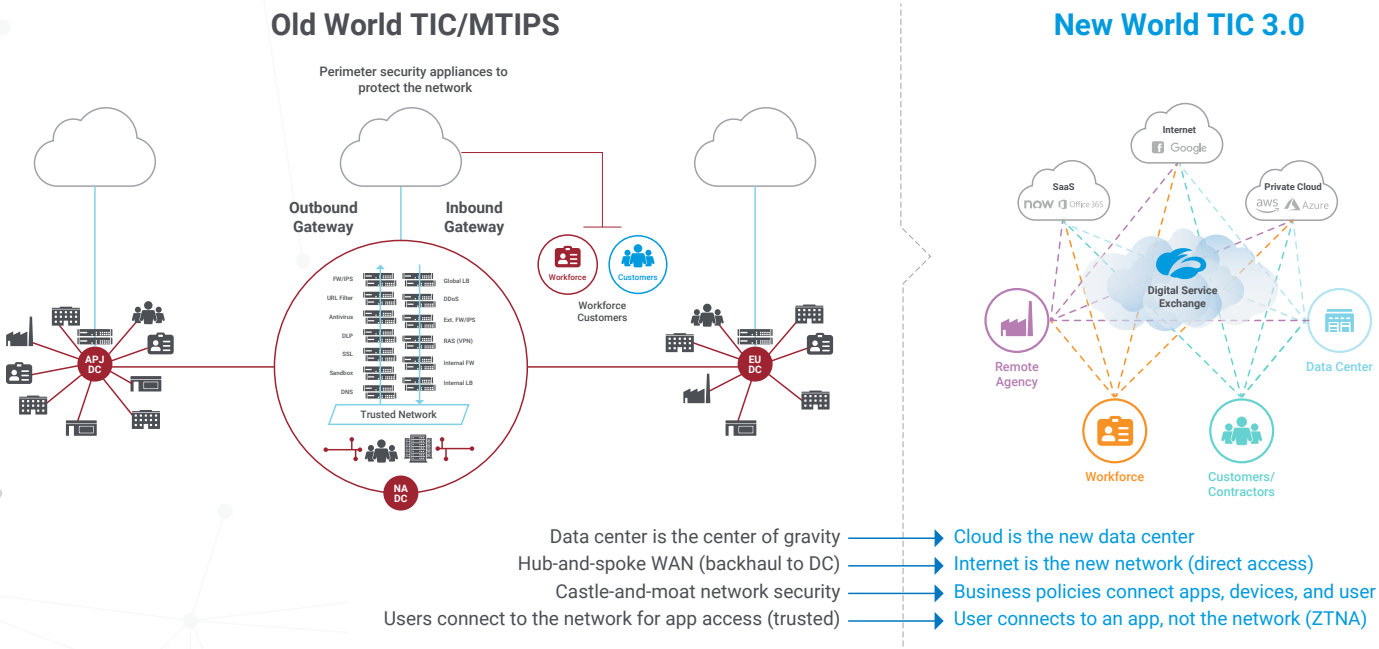
Modernizing Cloud and Internet Access with SASE-Based TIC 3.0 Solutions

Reducing the attack surface helps remove cloud transformation barriers

zscaler™

With federal cloud adoption at an all-time high and growing with IT modernization, federal teams need secure 24/7/365 access to data and applications anywhere, from any device. For years, the Trusted Internet Connection (TIC) policies, combined with the use of remote VPNs, limited agencies' ability to move to the cloud due to the restrictions the old TIC policies placed on internal and external connections to the network and the internet. This made the traditional TIC model untenable in today's cloud-first world.

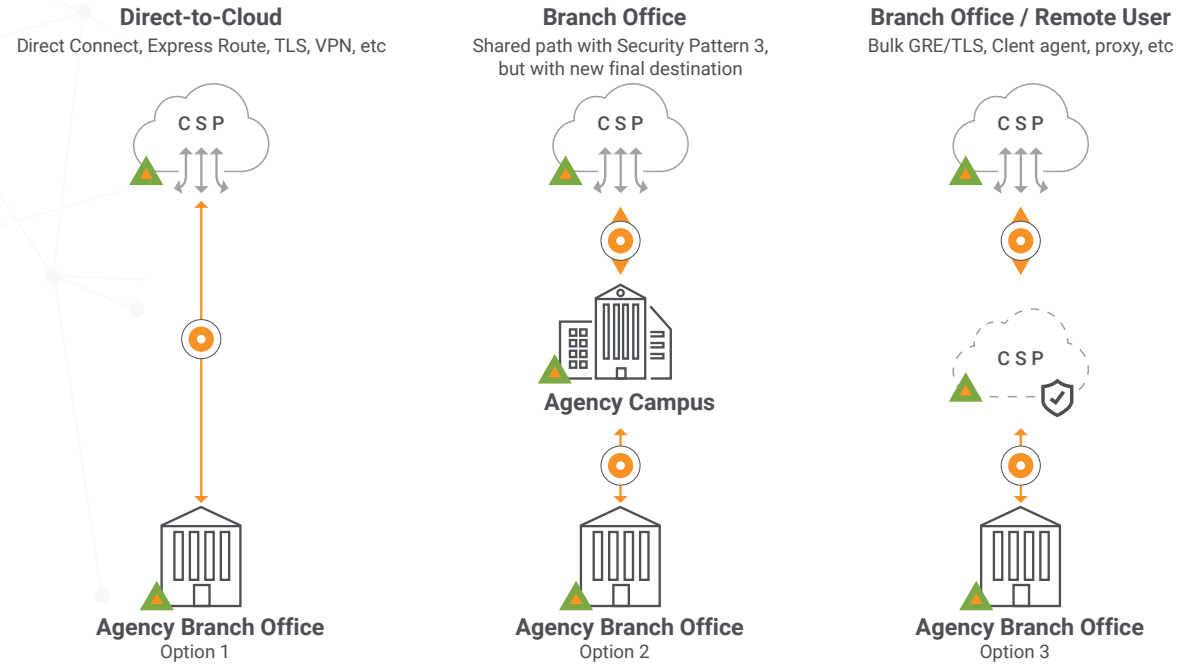


Fast forward to today, the volume of cloud-based applications and the associated high-volume, high-demand traffic is exploding. The number of mobile devices is exceeding desktops, and the perimeter is almost completely dissolving.

Responding to these challenges, the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB) released an important TIC policy update. The new TIC 3.0 guidelines expand on the original program to drive security standards and leverage advances in technology as agencies adopt mobile and cloud environments. The goal of TIC 3.0 is to find new and innovative ways to secure federal data, networks, and boundaries while providing visibility into agency traffic, particularly for cloud communications.

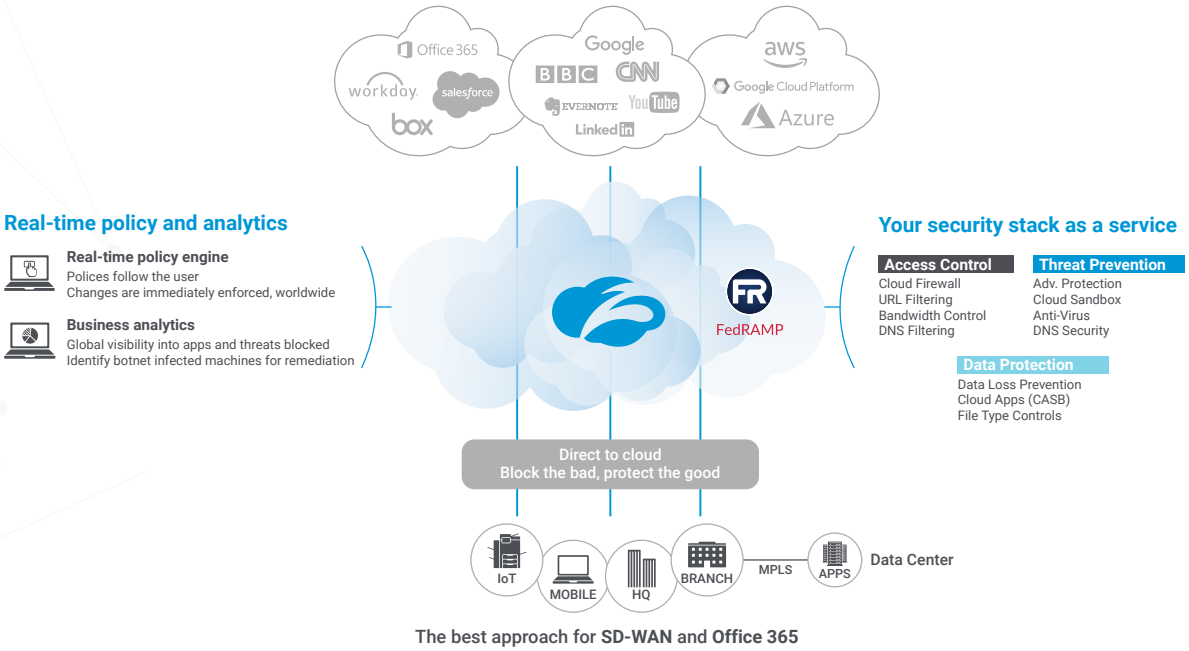
TIC 3.0 offers vital support for broader cybersecurity efforts, including Cloud Smart, the National Cybersecurity Protection System (NCPS), and the Continuous Diagnostics and Mitigation (CDM) programs.

The new guidance also provides a catalogue of approved agency use cases, where agencies can review results for environments with security requirements similar to their own and consider new possibilities. These use cases could include:



The Zscaler multitenant 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.

Zscaler meets the TIC 3.0 framework with fast, secure access to the internet, SaaS, and IaaS/PaaS via SASE and zero trust architecture

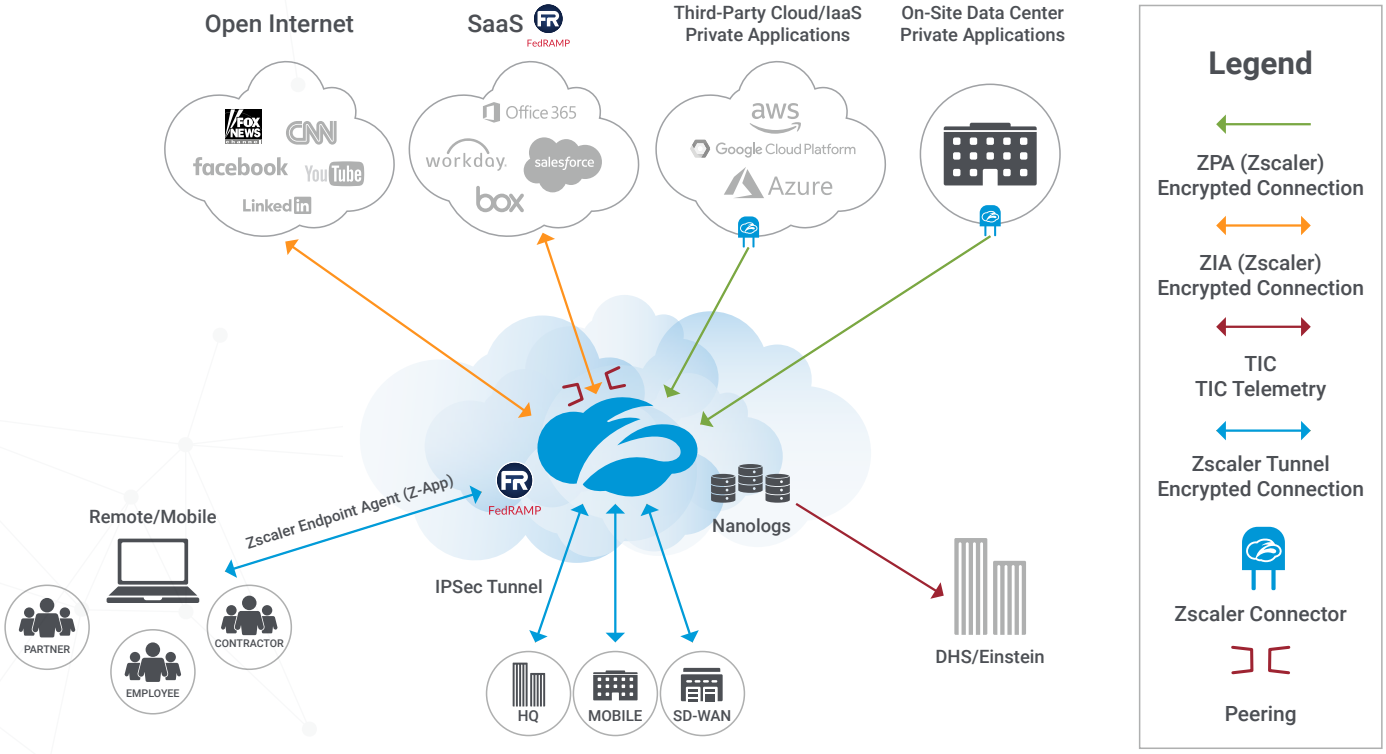


The best approach for SD-WAN and Office 365

Improve security controls – Keep IT focused on innovation with TIC in the Cloud

Federal IT leaders can improve on the who, what, where, when, and how they see, protect, and control user traffic to the internet by moving TIC security controls and other advanced security services to a cloud platform. The goal: immediate remediation on a global scale. This approach offers agencies global internet access and peering with FedRAMP-authorized applications. In addition, agencies capture extensive log/telemetry data and keep CDM reporting in place, while storing all agency data on U.S. soil with U.S. citizen-only access.

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.



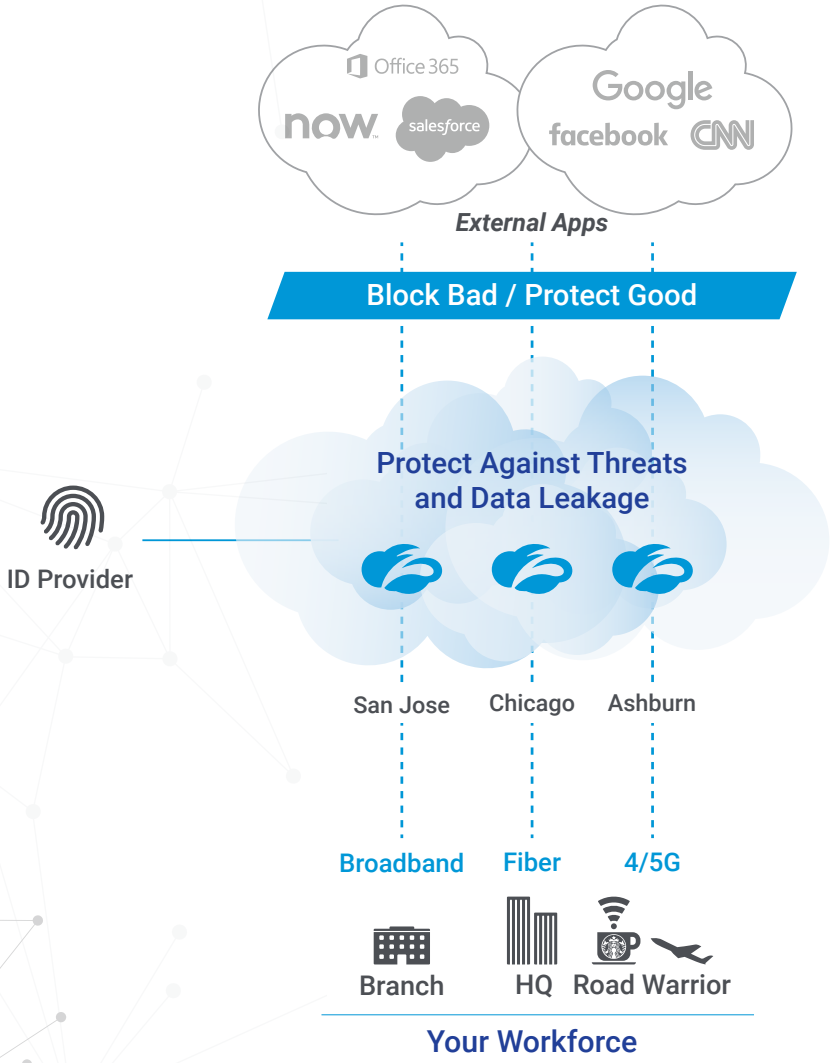
Direct-to-Cloud Architecture = Productivity, Flexibility

With a direct-to-cloud architecture, users take the shortest path to the application or internet destination, which optimizes performance. In addition, purpose-built cloud-based security technologies apply numerous techniques to minimize processing overhead, reducing latency as compared to an appliance-based solution. As agencies eliminate appliances, they reduce cost and complexity. At the same time, reduced latency means improved user experiences.

Zscaler TIC 3.0 Solutions

The Zscaler multitenant Cloud Security Platform applies policies set by the agency to securely connect the right user to the right application. As a Secure Access Service Edge (SASE) service, the Zscaler Cloud Security Platform is built from the ground up to provide comprehensive network security functions. Unlike traditional hub-and-spoke architectures where traffic is backhauled over dedicated wide area networks via VPNs to centralized gateways, Zscaler routes traffic locally and securely to the internet over broadband and cellular connections. The Zscaler SASE architecture shifts security functions to focus on protecting the user/device in any location, rather than securing a network perimeter. This ensures that users get secure, fast and local connections no matter where they connect.

Zscaler Internet Access-Government (ZIA): The first FedRAMP-authorized secure internet and web gateway securely connects users to externally managed applications, including SaaS applications and internet destinations, regardless of device, location, or network.



Use Cases

Office 365
- App prioritization/peering with Microsoft
- One-click deployment

Threat Protection
- Inspect encrypted traffic at scale
- Cloud-effect: Identify once, protect all

Secure SD-WAN
- Local breakouts for branch internet
- API integration with SD-WAN vendors

Data Protection
- Shadow IT discovery
- Protect IP/PII/Compliance

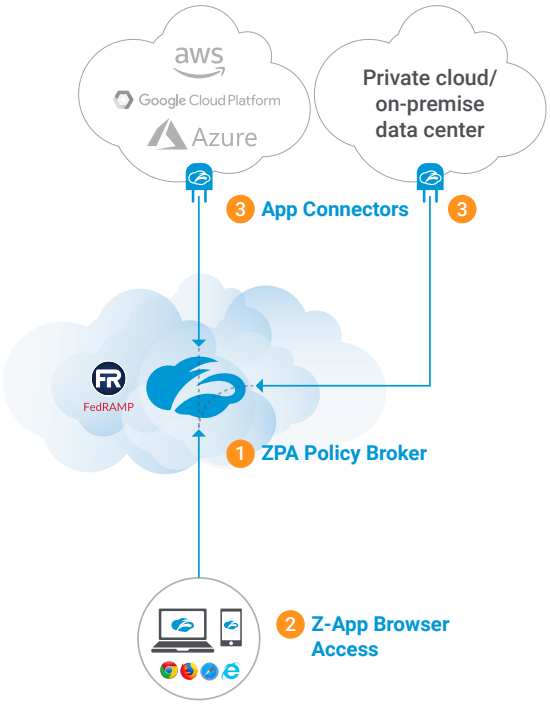
- Standardization • Simplification • Identical Protection (mobile, branch, HQ)

- Delivers the security stack as a service from the cloud, enabling agencies to route more mission-critical traffic straight to the cloud
- Connects users securely to externally managed applications regardless of device, location, network
- Reduces costs associated with backhauling traffic through outdated technology
- Reduces complex array of security applications, while increasing performance

Zscaler Private Access-Government (ZPA): The first FedRAMP-authorized zero trust cloud solution, ZPA-Government has achieved FedRAMP Ready status at the High Impact level. It provides seamless and secure zero trust access to internal applications for authorized users using a software-defined perimeter, not appliances, to provide comprehensive security and a fast, transparent user experience.

Zero trust security architecture

1. **ZPA Policy Broker**
   secure user to app connection
2. **Z-App/Browser Access**
   request access to app
3. **App Connectors**
   sit in front of apps
   outbound-only connection



Zero trust access with ZPA

- Treat all as untrusted both outside and inside the perimeter
- Verification prior to granting access
- Access is granted on a strict "need to know" basis
- App access without requiring network access
- Segment of one is created between named user and named application

- Delivers the same access whether agency applications are hosted in the government data center, in the AWS GovCloud, or in another service
- Replaces legacy VPN technology and provides encrypted (TLS 1.2) connections to applications
- Connects users to applications without placing users on the network, reducing risks introduced by unmanaged devices and eliminating the threat of lateral movement
- Ensures applications are "dark" to unauthorized external and internal users, reducing the possibility of DDoS or other internet-based attacks
- Provides visibility into an agency's full internal application environment, enabling IT to understand user activity, and discover and define access policies for internal applications

9 Consecutive years: Named a Leader on Gartner's Magic Quadrant for Secure Web Gateways

100 Million Threats Detected Per Day

120,000 Unique Security Updates Per Day

Internet Exchange Peering with 150+ vendors, including Office 365, AWS, Azure

Future Forecast – A zero trust-optimized TIC 3.0 environment

Zscaler provides the entire internet security stack as a service, continuously applying policies and threat intelligence to protect agencies from malware and other advanced threats. Identifying and understanding the user, while protecting the application with inside-out connectivity, precise access, and "trust no one" encryption, removes the network and the device used to access it from the security equation.

Whether the user is in the office or working remotely in the field, Zscaler's patented technology allows policies to follow the user, determining trusted and untrusted connections to make routing decisions appropriately -- creating a zero trust-optimized TIC 3.0 environment.

For more information, visit
zscaler.com/resources/ebooks/zscaler-cloud-security-platform

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™

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