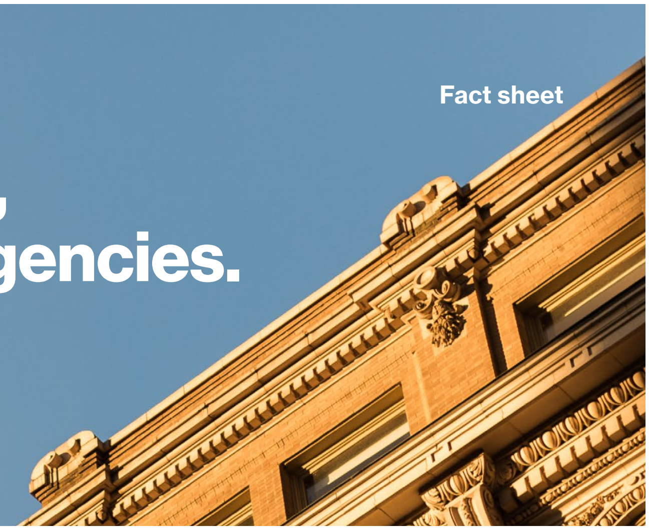
Fact sheet

Public Sector zero trust solutions for state, local, education and civilian agencies.

Zero Trust Dynamic Access.



As a result of the changing IT landscape, today's public sector agencies are faced with multiple challenges to effectively secure access to sensitive public and private resources and enforce compliance from wherever users and devices are located.

These challenges include:

- The security edge has expanded due to a decentralized remote workforce and cloud adoption so traditional/legacy network security solutions may no longer be sufficient at providing the protection, control, and visibility needed.
- Remote users accessing applications, data, and services that have moved out of the datacenter to the cloud create security blind spots and make them more easily accessible by attackers.
- Remote traffic sent through slow and overloaded VPNs may limit remote users from working effectively and high bandwidth usage, latency and costs are associated with backhauling traffic to the datacenter.
- Too many security point solutions that are expensive and difficult to manage.
- Significant rise in the frequency of target-based ransomware and cyber-attacks.
- New regulations for data protection and information security.

As a result, the cybersecurity strategies for public sector agencies need to continue to evolve.

The move towards a Zero Trust Architecture

Due to these challenges, organizations, including some within the public sector, have begun to abandon the traditional appliance-based solutions that are no longer effective to meet the security requirements of the expanding security edge. Instead, organizations are moving toward a more modern approach that utilizes zero trust access methodologies to help protect their critical resources from threats per transaction. By migrating to a single cloud-based Zero Trust access platform, cyber risk can be reduced by helping to make applications, data and services inaccessible to attackers while allowing trusted users to securely and directly connect to protected resources from virtually anywhere.

The National Institute of Standards and Technology (NIST) Special Publication 800-207 provides a clear and distinct definition of a zero trust architecture that can be used to transform an enterprise to a zero trust model. Organizations wishing to implement zero trust according to the NIST 800-207 zero trust architecture principles and guidelines can use Zero Trust Dynamic Access capabilities to implement the technology foundation of this architecture.

A single platform provides a global zero trust service edge to protect public and private resources.

Zero Trust Dynamic Access is a global unified zero trust security service edge that provides both connectivity and security to private on-prem, cloud and SaaS resources to eliminate blind spots. The platform acts as the policy decision and enforcement point as part of a zero trust architecture framework that can allow cloud, SaaS, and on-prem organizational resources to be labeled, categorized, and protected. Zero Trust Dynamic Access replaces legacy VPN and SWG solutions with an automatic and always-on service that can encrypt and secure all traffic to help ensure security, compliance and logging are applied at any location.

Zero Trust Dynamic Access can provide public sector agencies a secure pathway to modernization as they review shifting from static, perimeter-based tools to dynamic, fully integrated platforms that help protect users, data, applications and devices.

Continuous adaptive access algorithms allow for per request access decisions to resources.

Zero Trust Dynamic Access connects approved and trusted users to the resources automatically by inspecting and authorizing every single transaction between a user and a protected resource. Every transaction is inspected for CASB, malware defense and data loss prevention to help eliminate the risk that typically exists between authentication and sensitive data access. The platform continuously makes per-request access decisions which utilize criteria and role based access policies every time a transaction to sensitive apps and data occurs. This greatly reduces risk by cutting access to sensitive data and applications as soon as a device is determined to be infected with malware or ransomware.

Drive data loss prevention

Zero Trust Dynamic Access not only inspects internet data as it enters an organization by helping stop malware on the way in, but it can also inspect internet data as it leaves an organization. This deep file-based data loss prevention service helps detect and block the transfer of sensitive data from your enterprise. It protects against unauthorized cloud use and sensitive data loss. By screening content such as credit card numbers, personal data, email addresses and phone numbers, agencies can be notified when sensitive information is shared using automated alerts sent directly to security teams.

Malware defense prevents ransomware and infected devices.

With signature-based malware prevention and breach protection, malware is identified and mitigated based on threat intelligence from databases and proprietary malware registries. Intrusion detection and prevention capabilities enable quick viewing of event detail, including source and destination IP addresses. Command and Control (CnC) callback monitoring helps to further identify known malicious or high-risk connections and sites flagged for botnet activity. Zero Trust Dynamic Access also includes behavioral malware sandboxing defense to intercept and contain files– helping reduce noise and resource requirements. User downloaded files identified as suspicious are sent for further inspection in an isolated environment for secure processing.

Innovative container-based cloud architecture.

Through an innovative container-based cloud design, Zero Trust Dynamic Access protects users, devices, and locations without requiring data backhaul or the purchase of expensive appliances. Zero Trust Dynamic Access is delivered through a network cloud where the customer admin portal, policy infrastructure, and dashboards are multi-tenant, but the data plane consisting of the proxy gateway nodes where data traffic is routed is non-shared and dedicated for each customer.

This container-based approach enables a smooth transition from a private cloud (hosted or on-premises) to a public cloud or hybrid implementation. This includes the ability to drop-in replacements of legacy appliances to secure data in primary data centers without restructuring the network. All features and functions are offered regardless of the preferred deployment model.

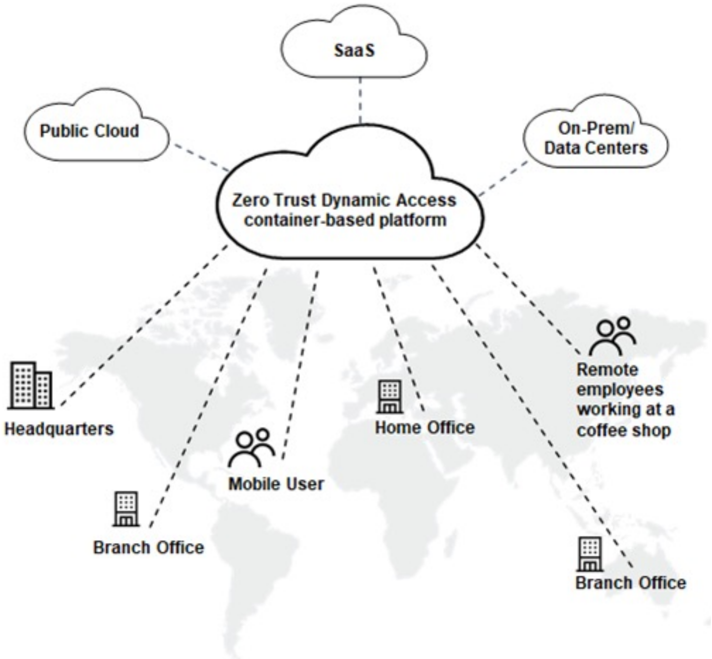
CASB controls for social media and cloud apps

Cloud application and social media controls help enterprise administrators enforce security policies for specific features of cloud-based apps and social media sites. This includes advanced application scanning, deep packet inspection (DPI) and content-aware management of social media applications like Facebook, Twitter, LinkedIn, and Pinterest. Administrators can also get control over evasive cloud applications like Tor, BitTorrent, Snapchat, Microsoft Skype and more. Zero Trust Dynamic Access also includes Safe Search enforcement for a variety of search engines, clean image search, and translation filtering for Google services.

Zero Trust Dynamic Access also includes:

- Browser Isolation for non-employee/BYOD access to resources without data leaking
- Logging and reporting for visibility of access across private and cloud resources
- Selective decryption of HTTPS traffic to inspect for compliance, malware and data loss
- Automatic resource discovery and built-in catalog to identify for resource protection
- Authenticating users against identity provider that matches the requested resource
- Single centralized management and administration portal
- Protection of devices across multiple operating systems

Zero Trust Dynamic Access utilizes an advanced non-shared cloud architecture that combines non-physical cloud nodes and optional physical nodes to help organizations deploy effective security across all locations and devices.



Why Verizon?

Verizon can also help your agency manage the Zero Trust Dynamic Access service. With MSS SaaS Policy Management, our seasoned security professionals implement, review and validate customer-initiated security policy change requests against your organization's existing policies to ensure compatibility with existing infrastructure. Agencies receive expert management of security policy rule sets and access to a dedicated Verizon Security Services Advisor (SSA) who will provide trend reporting analysis, freeing your internal staff to focus on strategic agency initiatives.

Learn more:

Find out how Zero Trust Dynamic Access can help meet the security needs of your distributed organization.

Contact your account manager or visit www.verizon.com/business/products/security/network-cloud-security/zero-trust-dynamic-access/