Zero Trust Dynamic Access Service Description

1 Acronym Definitions

CASB – Cloud Access Security Broker
CCN – CMS Certification Number
DLP - Data Loss Prevention
DNS - Domain Name System
IAM – Identity and Access Management
ICAP - Internet Content Adaptation Protocol
IdP – Identity Provider
IoT - Internet of Things
MFA - Multi Factor Authentication
NIST - National Institute of Standards and Technology
OT - Operational Technology
PEP - Policy Enforcement Point
PII – Personally Identifiable Information
SaaS - Security as a Service
SCP – Secure Copy Protocol
SFTP - Secure File Transfer Protocol
VDI - Virtual desktop infrastructure
VPN - Virtual private network
WCCP - Web Cache Communications Protocol. (Cisco-developed content-routing protocol)
ZTA - Zero Trust Access

2 Overview

Verizon's Zero Trust Dynamic Access helps to prevent breaches by making applications, data and services virtually inaccessible to attackers while allowing trusted users to securely and directly connect to protected resources. Zero Trust Dynamic Access provides a cloud-based security service edge solution for secure access to the open internet, cloud applications, private applications and data, and public cloud services helping to ensure security, compliance and reporting. The Zero Trust Dynamic Access cloud security platform is provided by iboss, a leading cybersecurity company.

Companies are moving to a 'Zero Trust' model of cyber security which takes the approach that no users or devices are to be trusted without continuous verification, while limiting potential system response latency. The main drivers for a Zero Trust architecture include the frequency of target-based ransomware and cyber-attacks, increasing regulations for data protection and information security and the fact that users and resources are now distributed outside of the office making them accessible by attackers.

Zero Trust Dynamic Access is specifically designed to meet the cybersecurity needs of today's distributed organizations. Built for the cloud as a SaaS offering, Zero Trust Dynamic Access can defend today's complex and decentralized networks, branch offices, and the remote and mobile users that depend on them. Zero Trust Dynamic Access provides the flexibility required to drop-in and replace existing on-premises legacy secure web gateway (SWG), virtual private network (VPN), and virtual desktop infrastructure (VDI) solutions, helping organizations to transition to a Zero Trust architecture smoothly, without the need to re-architect their existing networks.

A distinct advantage of Zero Trust Dynamic Access is based on its containerized architecture which allows security to not only be placed close to the user, but also allows security to be close to the resource regardless of where the resource resides. It does this by stretching the secure service edge near data and applications, such as those within a datacenter, while maintaining a single, unified service edge which helps guarantee consistent security, policies and visibility across all users and resources. This design also can enable the most direct to resource connections without forcing data through unnecessary paths which helps ensure the fastest and lowest latency connections.

3 Zero Trust Dynamic Access Packages & Features

Zero Trust Dynamic Access is available in three packages – Core, Advanced, and Complete. All packages come with 500 GB of Cloud Storage for logging, reporting and analytics at no additional cost.

3.1 Core Package Features

The Core Package is the base-level cloud security offering that provides essential security controls for both on- and off-network users and devices and includes the following standard Zero Trust security service edge features:

- **Unified Zero Trust Security Service Edge** - Combines connectivity and security capabilities into a single platform that connects users and devices to enterprise-owned resources and the public Internet. The platform replaces legacy VPN, Proxies, and VDI solutions with a consolidated cloud-based service that can improve security, increase the end-user experience, consolidate technology, and may substantially reduce costs.
- **Zero Trust Resource Access Policies** - Enables privilege-based access to resources through definition of criteria necessary for a user to access a resource. (e.g., by geo-location, specific user, user group).
- **Resource Catalog for Apps, Data, and Services** – A catalog of over 5000 3rd party public cloud resources that are classified by type and risk level which an organization may choose to connect to the Policy Enforcement Point.
- **User & Asset Catalog** - An integrated database used to catalog enterprise assets and users. Automatically catalogs assets and users as they interact with resources.
- **Resource Tagging by Type and Location –** Ability to tag resources by type, location, and risk classification.
- **Resource Risk Level Classification** - For each identified Resource Type, ability to define the potential impact level if the Security Objective is compromised.
- **User and Group Based Access Policies via Cloud Connectors** – The cloud connector agent automatically captures the username and group of the currently logged-in user of the device based on the credentials the user leveraged to log into their system and provides that information to the platform.
- **Zero Trust NIST 800-207 Criteria-Based Access Policies** – Enables privilege-based access to resources through definition of criteria necessary for a user to access a resource. by geo-location, specific user, user group membership from federated identity providers such as Okta, Ping, Microsoft AD, etc.
- **Connect Cloud Accessible Resources to Zero Trust SSE** - Connect to and help protect any proprietary applications with a publicly accessible IP address.

- **Encrypted Traffic Inspection and Protection (HTTPS Decrypt)** – Apply security policies against encrypted (HTTPS/SSL) traffic. Micro-segmentation to selectively decrypt based on content, device, user, or group.
- **Cloud Security Controls** - Enable blocking access to harmful online content and help to ensure an organization is compliant with data privacy and protection policies and regulations. Controls include:
  - Content-based analysis and inspection
  - Dynamic policies based on user and group membership
  - Stream-based protection, including all ports and protocols (TCP & UDP)
  - Granular category- and user-based filtering
  - Alerts based on keywords, events, and other customizable triggers
  - File extension, domain extension, and content MIME type blocking
  - Port access management
  - Dynamically updated URL database
  - DNS Security for guest networks, BYOD, Internet of Things (IoT), and Operational Technology (OT) device protection
  - Policies for blocking access
- **Policy Tracing for troubleshooting policies** – Ability to troubleshoot policies (e.g., if a specific policy is used to block access to a resource).
- **Proxy Combinatorial Rules & Actions** - Block, Allow, Redirect, or Manipulate http headers, force or bypass authentication requirements, forward to external ICAP.
- **Reporting & Analytics** - Extensive Analytics Dashboards, Detailed Logging that provides clear visibility into cloud use, Drill Down Reports, and Reporting Templates.
- **Zero Trust Reporting** - By Resource Type, Resource Location, Security Objective and Security Impact Level.
- **Cloud Connector Agents for Windows, Mac, iOS, Chromebooks, Linux and Android** - Endpoint app used to connect enterprise-owned devices to the Zero Trust SSE. Cloud Connectors connect devices from any location and ensure traffic is always steered through the Zero Trust SSE where security is applied, and logging is generated for visibility. The Cloud Connectors run transparently to users and eliminate the need to enable or disable a VPN in order to connect to private resources.
- **DNS Security** - The Zero Trust SSE can be configured to act as a DNS Resolver to secure forward lookup requests and then log and report on those queries. DNS Requests can be blocked or allowed based on configured security policies.
- **SAML & OIDC Identity Provider (IdP) Integration** – Eliminate unauthorized users by integrating with federated identity providers (e.g., Okta, Ping, Microsoft AD, etc.).
- **Extend Modern Authentication (SAML/OIDC) to Legacy Apps & Resources** – Helps to ensure that modern authentication including MFA can be enforced on all resources, including legacy applications that have no ability to integrate with federated identity services.

3.2 Advanced Package Features

The Advanced Package is the mid-level offering that includes all the Core Package features, plus advanced threat protection and the ability to connect users to private on-premises resources for VPN replacement.

- **Zero Trust NIST 800-207 Score-Based Access Policies** - Continuous per-request access decisions extend access policies beyond the point of login and apply to every request between a user, asset, and resource. Enables blocking or isolating access to critical resources when conditional access requirements are not met by utilizing a trust scoring algorithm for every transaction.

- **Zero Trust Scoring Algorithms** - Adaptively uses asset, subject, and resource signals to allow, block, or isolate access to protected resources.
- **Connect Resources on Private Networks to Zero Trust SSE** - Supports connections via tunnels, SD WAN, WCCP to Policy Enforcement Points.
- **Asset and Device Posture Checks** - Adaptively change resource access policies based on device posture checks.
- **Zero Trust Score-Based Reporting** - Resource score-based reporting and continuous scoring of each logged transaction provides insights into changes in risk.
- **Threat Dashboards** - Provides malware and threat statistics, including statistics by malware type, source, and statistics related to malware infections. The dashboard is organized into several tabs that provide malware and threat defense reporting from a variety of viewpoints.
- **User and Asset Incident Dashboards** - Provides access to subject and asset incident information including infected devices and users with active incidents.
- **Malware Prevention** - Capabilities include malware scanning of full content and files, including data transferred within encrypted HTTPS connections. The platform includes extensive threat feeds and intelligence that are applied to every transaction to help prevent malicious sources and automatically detect infected devices.
- **Infected Device Detection and Isolation (CnC Callback Prevention)** - Provides the ability to detect infected assets and devices by determining if they are communicating with known Command and Control (CnC) destinations using Domain, URL, and blacklisted IP monitoring. The Threat database is continuously updated with signatures and destinations that are used to detect when a device is communicating with these malicious destinations.
- **Phishing Prevention** – Dozens of leading threat and phishing feeds automatically included in the platform – e.g., PhishTank, SpamHaus, Verizon Threat Research Advisory Center (VTRAC).
- **Prevent Malicious Sources** - Malware identification and mitigation from top-ranked signature and signature-less engines including a proprietary malware registry, and integration with the VTRAC feed.
- **Malware Sandboxing** - Provides the ability to run files and URLs within a malware sandbox for controlled detonation. When files and URLs are detonated in the sandbox, a complete malware analysis is performed, and behavior is captured. The results can be displayed to determine how malware behaves, what operations it takes on a machine and how it communicates from the infected device.
- **Microsoft integrations:**
  - Microsoft Defender for Cloud Apps (formerly MCAS) Integration
  - Microsoft Authentication Context (Conditional Access) Integration
  - Microsoft Sentinel Log Forwarding Integration
- **Splunk Log Forwarding** - Native integration with Splunk to allow event logs to be forwarded from the reporting database to a Splunk environment.
- **Log Forwarding to SIEM** - Forward log events (web access logs, malware events, and data loss alerts) directly from the cloud service to external logging databases or SIEM services via standard forwarding protocols, such as Syslog and SFTP without any additional external log brokers.
- **Realtime Inline CASB** – Provide granular in-app controls to help enforce compliance, reduce risk, and gain visibility into cloud application use. For example, making Facebook read-only, ensuring access to Google Drive is corporate only and leveraging Microsoft365 Tenant restrictions.
  - Advanced application scanning and deep content inspection

  - Content-aware management of social media applications like Facebook, Twitter, LinkedIn, and Pinterest
  - SafeSearch enforcement for Google, Bing, and Yahoo
  - Clean image search and translation filtering for Google services
- **Simplified Tunnel Management (Network Connector)** - Creates secure tunnels to enable access to private resources sitting within private network environments. The Network Connector can be deployed on a server in a corporate data center allowing remote users to securely access applications, services, and data sitting within the data center. It provides automatic tunnel configuration so that there is no need for network resources to create IPSeC or GRE tunnel configuration.

3.3 Complete Package Features

The Complete Package is the most comprehensive offering. It includes all the Core and Advanced Package features, plus data loss prevention (DLP), Intrusion Prevention System (IPS), and Out-of-Band API CASB capabilities.

- **Data Loss Prevention (DLP)** - Inspects full content, including content on documents, spreadsheets, web page content data, and SaaS applications. With access to the full content when data is transferred between users and applications, the ability to apply data loss prevention rules that are capable of searching for personal data and sensitive information is possible. The platform inspects data as it moves between applications, devices and users and enforces policies that ensure data only resides where it is compliant and secure. Advanced detection and content analysis capabilities include:
  - Screens all content to help prevent unintended loss of sensitive information.
  - Capable of scanning: Credit card numbers, PII, email addresses, phone numbers.
  - Supports regular expressions (regex) to search for text strings deep within transferred content.
  - Process and parse targeted files to ensure that even compressed content is accessible to the detection engines.
  - Set compressed file max scan depth to search for content deep within zip files.
  - Analyzes numerous file types including: Base16, GZip, PDF, Outlook data files, SQLLite Database, Windows PE Executables, Zip files, RAR files, Windows Hibernate Files, Windows LNK files, Windows PE Files.
  - **Intrusion Prevention (IPS) -** Provides proactive monitoring and protection against unauthorized intrusions, malware, and viruses. By analyzing the organization’s network traffic, it can detect and block threats before they reach the internal resources and endpoints.
    - Identify threats in stream-based data
    - Quickly and easily view event detail, including source and destination IP addresses
    - Automatic signature threat feed subscriptions
    - Category-based malware rules
    - Visual rule creation and editing
  - **Out-of-band API CASB** - Discover sensitive files and content present within SaaS applications as well as identify inappropriately publicly shared sensitive content within those applications by identifying public share links that point to those files. Provides the ability to apply fine grained controls, gain visibility into cloud applications, and inspects data at rest.

3.4 Optional Feature Add-Ons

- **Remote browser isolation** – Browser isolation limits sensitive data leaks from unmanaged device use and helps protect users from threats when accessing high-risk web sites. Ideal for Virtual Desktop Infrastructure (VDI) replacement.
- **Intrusion Prevention (IPS)** – Provides proactive monitoring and protection against unauthorized intrusions, malware, and viruses. By analyzing the organization's network traffic, it can detect and block threats before they reach the internal resources and endpoints. Quickly and easily view event detail, including source and destination IP addresses. Includes automatic signature threat feed subscriptions, category-based malware rules and visual rule creation and editing.
- **Endpoint Detection and Response Integrations** - Endpoint Detection and Response (EDR) integrations allow for enhanced visibility and response capabilities on end-user devices by integrating existing endpoint EDR services with continuous Adaptive Access policies. This helps ensure that every interaction between a user and data is authorized to immediately cut access when a device gets infected or a high-risk user is detected, thereby reducing the risk of a breach.
- **Data Loss Prevention (DLP)** – Monitor and control data transfers outside the company's enterprise resources which help in preventing unauthorized data leakage, either accidental or malicious to non-enterprise owned resources.
- **Exact Data Match** – Provides enhanced data protection capabilities by helping to ensure that exact sensitive data within content, like specific personal information, cannot be transferred outside the organization's resources without proper authorization. Note that this add-on requires the DLP feature.

3.5 Other Add-Ons

- **Cloud storage options** – 500GB of log storage on the platform is included at no additional cost for the following regions: US, UK, Germany, Singapore, Japan, and Canada. Logs can be streamed to external log storage/SIEM solutions or deleted based on parameters controlled via the admin portal. Additional cloud storage can be purchased if required.
- **Regional surcharges** – Additional surcharges will apply when cloud gateways need to be located in multiple locations (Zone 1 - US, Canada, Mexico, UK, Belgium, Bulgaria, Denmark, Finland, France, Germany, Helsinki, Ireland, Italy, Netherlands, Norway, Poland, Spain, Sweden, Switzerland, Turkey, Mexico City, Singapore). Additional surcharges will also apply when Cloud Gateways need to be located in certain countries to account for higher data center prices (Zone 2 - Columbia, Israel, S. Africa, India, South Korea, Japan, Hong Kong, Australia, Brazil and Zone 3 - China, UAE, Egypt, Taiwan, New Zealand, Argentina).
- **Private cloud hardware** – Policy Enforcement Points (PEPs) can be leased and placed in private data centers (e.g., for regulatory compliance, to be closer to critical resources, to replace existing on-premises hardware proxies, etc.).
- **Implementation and Professional Services** – Depending upon the project scope and configuration requirements, implementation or professional services fees may apply. The number of Implementation service hours will be determined during pre-sales and included on the customer quote. See Section 4 for a description of included and excluded implementation services.
- **Mission Critical Support** – See Section 5 for a description of support options.
- **Technical Account Manager** – A dedicated Technical Account Manager (TAM) service may be purchased with options of up to 32, 16, or 8 hours per week. The dedicated TAM resource guides clients through the implementation process and maintains responsibility for customer success as clients transition to operations mode. TAMs provide best practice

information, help with design and security documentation, and ad-hoc user training where applicable. Available TAM service is provided Monday-Friday business hours of 8AM-5PM based on geographies selected.

4 Deployment of Zero Trust Dynamic Access

Zero Trust Dynamic Access will be provisioned by iboss, Verizon's third party vendor. After the customer account is provisioned, a welcome letter will be emailed to the designated customer administrator and if needed, an implementation engineer will provide dedicated technical product expertise to assist the customer with onboarding on the cloud platform:

4.1 Implementation Services Provided

- Implementation kickoff call
- Coordination of project & implementation plan with identified milestone and completion dates
- Provide template user acceptance testing spreadsheets and user documents
- Live technical assistance configuring the platform for the following:
  - Assistance creating administrative users in the platform
  - Assistance enabling multi-factor authentication for admin users
  - Review of traffic redirection options
  - Time zone configuration
  - Platform maintenance scheduling
  - Email setting configuration
  - Backup configuration
  - Guidance developing web security groups
  - Assistance integrating with a cloud Identity Provider/Identity and Access Management (IdP/IAM)
  - Assistance creating a customized SSL decryption certificate
  - Assistance downloading and configuring cloud connectors for required device types (up to 5 devices)
  - Guidance on resource categorization
  - Guidance on configuring trust algorithms
  - Guidance on policy configuration
  - Creation of 1 custom branded block page
  - Creation of 1 custom report schedule
  - Creation of 1 custom IPS rule
  - Customization of 1 PAC script
  - Integration with 1 external SIEM for logging

4.2 Implementation Services Excluded

- Mass deployment, updates, or removal of cloud connectors in a customer's environment
- Active Directory, Azure, eDirectory or other directory service configuration or support
- Mobile Device Management (MDM) configuration or support
- Policy migration from legacy on-prem gateway proxies or firewall
- Configuration of customer firewalls, routers, switches, computers, or third-party software or applications

4.3 Private Cloud Deployment Option

Zero Trust Dynamic Access is delivered as a complete SaaS offering in the cloud without the need for on-premises appliances. In some cases, however, a customer may want to extend the service into a "private cloud" deployment. The containerized architecture of the solution allows the cloud configuration to extend into an optional private cloud Point of Presence (PoP). The private cloud is a dedicated on-premises gateway capacity that can be used to replace existing legacy proxies. The private cloud POP is shipped directly to the customer premises for installation.

Because the private cloud is just an extension of the global cloud, any policies or controls configured within the platform can automatically extend into the private cloud PoP. The private cloud becomes part of the global cloud extending it to private points of presence. This provides the consistency in security and user experience necessary when extending into a private cloud since a single policy-set and a single pane of glass is used for administration.

The security service edge can also be extended directly into the Azure cloud to protect Azure infrastructure with ZTDA gateways hosted directly within customer-managed vnets, and connect Azure services across vnets with ZTDA gateways directly in Azure. These private gateways can be purchased directly from the Azure marketplace.

5 Customer Support

Zero Trust Dynamic Access is offered with two customer support packages: Standard Support and Mission Critical Support delivered by iboss, Verizon's third party vendor, as described below.

Support Packages	Standard	Mission Critical
Online Support Center Access	included	included
Knowledge Base	included	included
Online Training, Videos, User Guides	included	included
Named Support Contacts	0	2
Live Support Hours	8am-8pm EST Monday-Friday (excluding major holidays)	24/7
Professional Services	Not Included	Up to 1 hr/month
Severity Level 1 Response Time	2 hours	15 minutes
Severity Level 2 Response Time	4 hours	1 hour
Severity Level 3 Response Time	24 hours	4 hours
Pricing	**Included in All Packages at no additional charge**	**Additional charge based on number of users**