zentry

Zero-Trust Secure Access

A new approach to enterprise security built on zero-trust principles and zen-like ease-of-use.

As enterprises adopt cloud and mobile technologies, the traditional perimeter security model of firewalls and virtual private networks (VPN) becomes problematic. The assumption that internal networks are safe and everything inside the perimeter can be trusted no longer holds. Today's workforce requires anytime, anywhere secure access to business applications and resources from the office, from home or on-the-go. As the distinction between remote and local access dissolves, each session must be authenticated, authorized and encrypted based on device, user identity and access control policies.

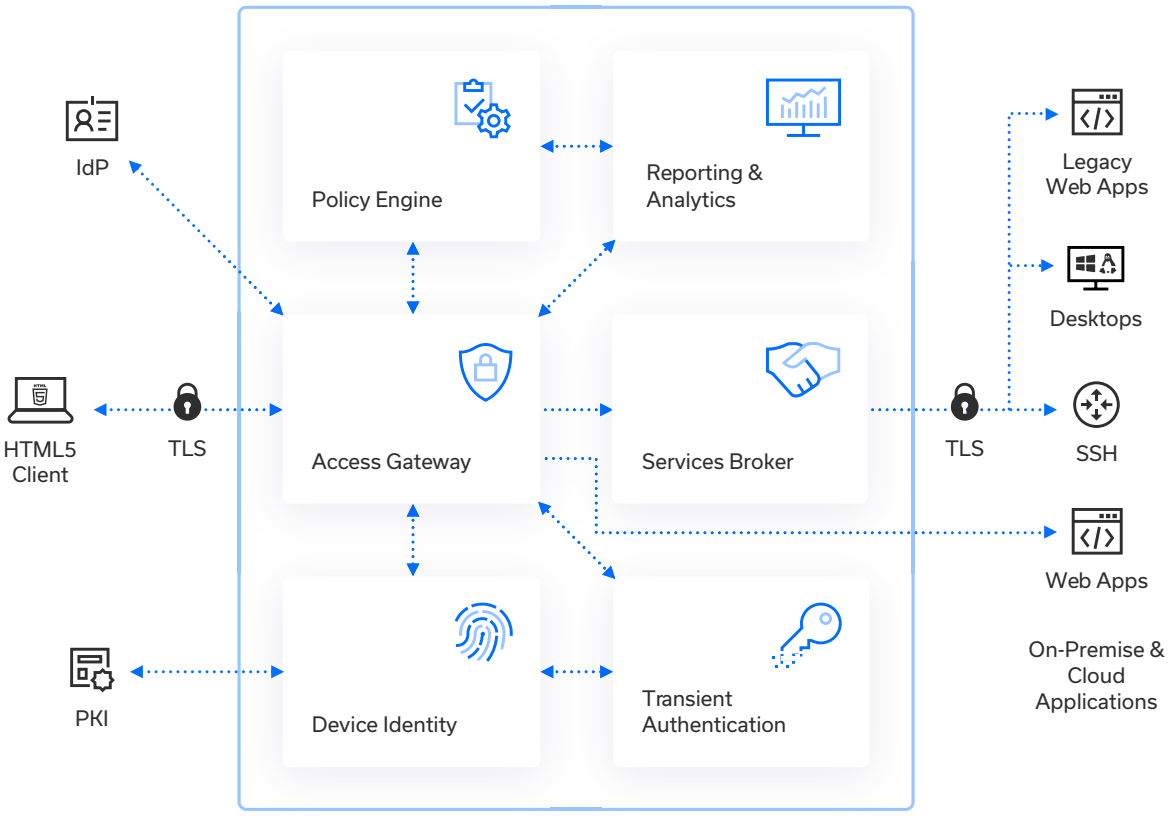
Zentry is a next-gen secure access solution based on zero-trust principles of 'never trust, always verify'. It allows IT to provide the workforce with secure access to any application or resource, whether on-premise or in the cloud, from anywhere on any device. Zentry eliminates the need for client software and replaces legacy network-level VPN connectivity with application-level connectivity that shrinks attack surfaces and prevents data leakage and lateral movement. Using Zentry, IT can replace monolithic HW security with pay-as-you-go services that improve security and the user experience.

HIGHLIGHTS & BENEFITS

- 100% clientless solution, OS agnostic and requires only an HTML5 browser for access
- Uniform access and security, same protection and experience for remote and local users
- Lightweight, high-performance access gateways front-end applications and resources both on-premise and in the cloud
- Application-level secure access connections use low latency, high throughput end-to-end TLS encryption
- Device validation and multi-factor authentication (MFA) are used to minimize attack surfaces
- Single sign-on (SSO) and federation minimize the need for repeat authentication, improving the user experience
- Flexible and extensible policy engine governs access per application and per resource
- Simple, secure transient authentication for privileged user access to IT infrastructure
- Reporting, analytics and visualization for feeding intelligence back into access policies
- Software-based service eliminates monolithic hardware and enables zero trust secure access on a pay-as-you-go basis

SCALABLE ZERO-TRUST ARCHITECTURE

Zentry is built as a modular set of components to facilitate adjustment to a variety of applications, resources and environments. The modular nature of the solution also allows for new components to be built and leveraged as they become available. Components interact in an automated manner driven either by orchestration or the Zentry admin interface.



zentry

The Zentry zero-trust secure access architecture consists of the following components

ACCESS GATEWAY

The Zentry Access Gateway is a high-performance access proxy that communicates with all other components and ensures that secure access to applications and resources is fully authenticated and authorized using device validation and authentication via MFA, SSO and policy enforcement. On supported platforms with hardware acceleration, the Zentry access gateway delivers improved performance for TLS encryption and compression. Supported functionality includes:

- Device validation
- User authentication with MFA, federation, SAML and OIDC
- Access proxy with load balancing and application health checks
- End-to-end encryption with support TLS 1.2 and TLS 1.3

POLICY ENGINE

Built on open standards, the Zentry Policy Engine provides flexible and fine-grained access policy controls on a per-application and per-resource basis. The access gateway queries the Zentry Policy Engine for attributes such as user, role, group, target application/resource, time, source IP, client location and other criteria. Zentry Policy Engine examines authorization context and policy definitions to generate least privilege access profiles and keep applications, resources and corporate data safe. Extensible and based on open frameworks, Zentry Policy Engine supports REST APIs for interfacing with external data.

SERVICES BROKER

Zentry Services Broker is a collection of intelligent emulation proxies that webify resources such as desktops (RDP and VNC), SSH, Telnet and legacy web applications that require a specific client version. Zentry Services Broker provides uniform and clientless access to these resources through an HTML5 browser. Configured in conjunction with Zentry Access Gateway, Zentry Services Broker leverages access control policies as defined Zentry Policy Engine. The services broker is highly scalable, and supports the following resources:

- Windows, Linux, Mac desktops
- Citrix XenApp/XenDesktop, VMware Horizon
- SSH, Telnet, FTP
- Legacy web applications, internal web applications
- Public web applications

TRANSIENT AUTHENTICATION

Zentry Transient Authentication is an SSO technology that generates temporary credentials for seamless access to Zentry protected mission-critical network infrastructure. Along with Zentry Services Broker, transient authentication can provide privileged user access to IT infrastructure including routers, switches and firewalls. Transient authentication eliminates unneeded root privileges, reduces the risk of root credentials being stolen and streamlines the user experience. Transient authentication also eliminates labor-intensive administrative tasks for infrastructure credential rotation and management.

REPORTING & ANALYTICS

Zentry Reporting & Analytics provides a centralized mechanism to analyze, search and visualize data at scale on application usage, application metrics, user metrics, compliance reporting, logs and more. Reporting and analytics works with every Zentry component to gather information and present it in easily created custom dashboards. Reporting and analytics is used for monitoring and alerting; in addition, debugging and troubleshooting information can also be sent to Zentry Reporting & Analytics to visualize events for a specific resource and the overall environment.

DEVICE IDENTITY

When only managed devices can be granted access to all resources, Zentry Device Identity comes into play. Device Identity provides a registration service to allow users to register their devices with Zentry. Once registered, PKI is used to bind the device signature (does not require any agent installation on the device) to device certificates which can then be validated by the Zentry Access Gateway device validation during user's login.

DEPLOYMENT MODELS

Private Clouds (hypervisors, 64-bit only)	Public Clouds (marketplaces)
VMWare ESXi 4.1 or later	Amazon AWS
XenServer 5.6 or later	Microsoft Azure
Open Xen 4.0 or later	VMware Cloud on AWS
KVM 1.1.1-1.8.1. or later	Aliyun (Alibaba Cloud)

SPECIFICATIONS

Feature	Description
Encryption	TLS 1.2, TLS 1.3
Cipher Suites	RSA, ECC
Authentication	AD, LDAP, RADIUS
Federation	SAML, OIDC

Sample Supported Features	Description
Identity Provider (IdP)	Azure AD, Google G-suite, Okta
Multi-Factor Authentication (MFA)	RSA, DUO
Zentry Web Services supported protocols	HTTPS, RDP, VNC, SSH, Telnet, FTP
Zentry Web Services supported desktops (physical or virtual)	Windows, Linux, Mac, Citrix XenApp/XenDesktop, VMware Horizon
Zentry Device Identity	CRL, OCSP, blacklisting, whitelisting

zentry

Zentry provides next-generation secure access solutions that improve security, productivity, visibility, and usability. Zentry empowers modern enterprises by delivering Zero Trust secure access from any device to any application or resource located on-premise or in the cloud. Learn more at www.zentrysecurity.com.

Zentry Security, Inc.
1371 McCarthy Blvd.
Milpitas, CA 95035

1-866-4-ZENTRY
(408) 240-8754

info@zentrysecurity.com
www.zentrysecurity.com