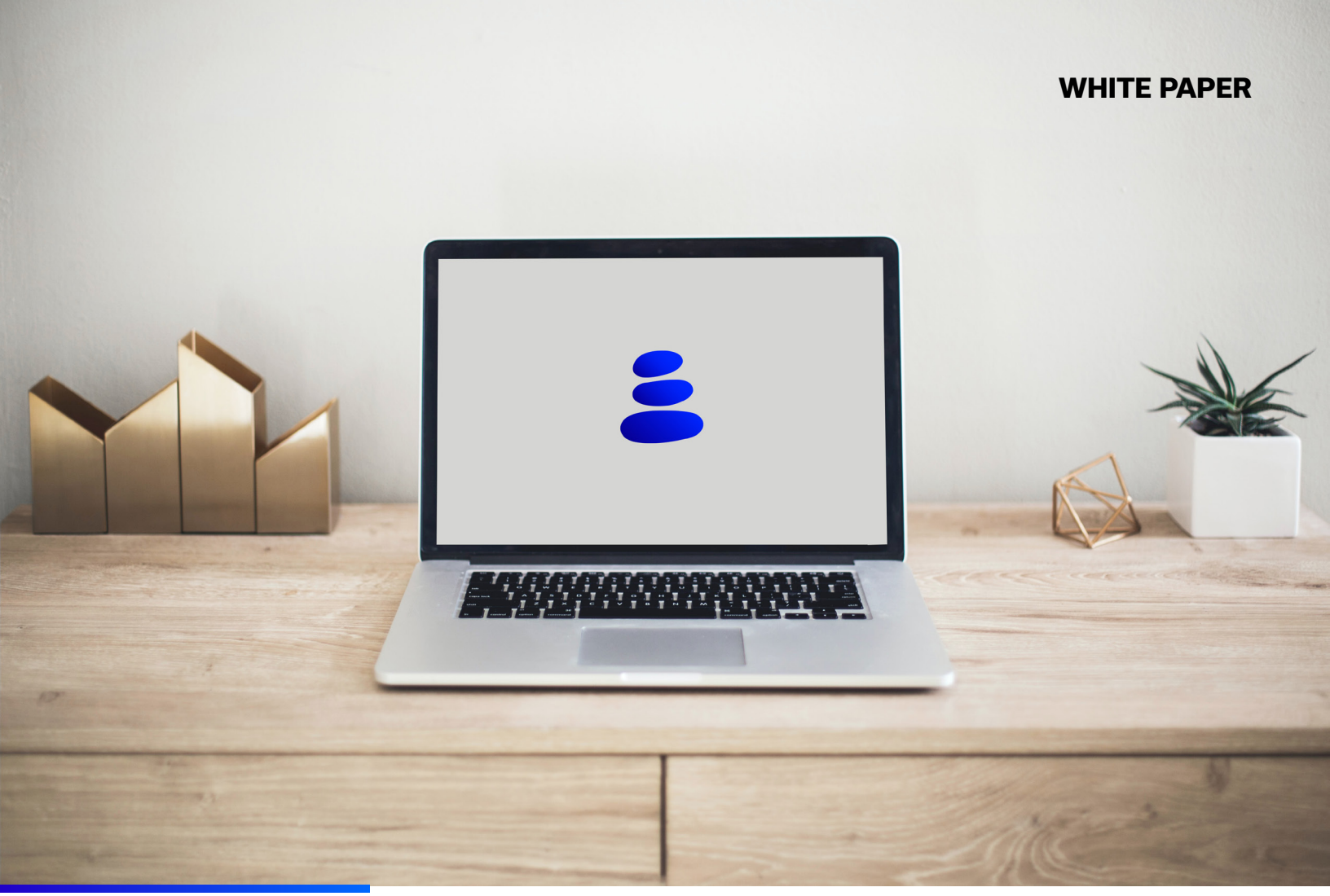
WHITE PAPER



zentry

MIGRATING TO ZERO TRUST SECURE ACCESS

NEVER TRUST, ALWAYS VERIFY

zentry

TABLE OF CONTENTS

zentry

EXECUTIVE SUMMARY

In today's enterprise, the traditional perimeter security model using firewalls and virtual private networks (VPN) is no longer sufficient to handle the challenges brought by the cloud and mobile computing. The assumption that the internal network is safe and everything inside the perimeter can be trusted no longer holds. In contrast, the Zero Trust security model eliminates the excessive trust placed on networks and locations, provides device-aware, identity-aware and policy-based secure access to applications and resources across on-premise and cloud environments. In this white paper, we will explore the transformation of security models, what elements are essential to Zero Trust secure access, and how Zentry enables Zero Trust secure access for today's modern enterprise.

THE FALL OF THE WALL

The perimeter model

The traditional perimeter security model uses a "castle and moat" approach. It resembles a castle built with walls and surrounded by a moat, with points of entry and exit. Anything inside the wall is trusted, while anything outside the castle is presumably dangerous and untrusted. Anyone who can pass through the drawbridge has the access to resources inside the castle. This model usually uses firewalls as the walls and moat to secure the perimeter, and VPNs as the drawbridge to allow access to internal resources.

However, this perimeter security model is problematic. The model, which assumes that internal networks are safe and that everything inside the perimeter is trustworthy, is flawed. When the perimeter is breached by phishing, malware or man-in-the-middle attacks, external malicious attackers can move laterally within internal networks, have access to resources, and can steal confidential business data. Malicious insiders are another major reason for security breaches. The Verizon 2019 Data Breach Investigations report says that 34% of all breaches were caused by insiders[1]. Studies also show insider threats are becoming more frequent, and the cost of insider attacks keeps rising.

As enterprises adopt cloud and mobile technologies more broadly, the network perimeter can become increasingly difficult to enforce. Today's workforce requires anywhere access from any device. Users work from at the office, from home, and on the go, blurring the line between local and remote access. Applications and resources are deployed and distributed across on-premise and cloud environments. As a result, the growing number of mobile devices and cloud applications has significantly increased the security attack surface.

Traditional VPNs, as extensions of the network perimeter, often require heavy and monolithic gateway and client software. Layer-3 connectivity that allows full access to the internal network expands the security attack surface and therefore results in security vulnerabilities including lateral movement and data leakage. In addition, VPN client software installation, configuration, upgrade and troubleshooting often imposes a heavy burden on both users and IT administrators.

[1] Verizon Data Breach Investigations Report (DBIR), Verizon, 2019, https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings

zentry

WHAT IS ZERO TRUST?

Evolution

Zero Trust is a security framework which eliminates excessive trust on everything inside or outside of the network perimeter. Created by Forrester Research analyst John Kindervag in 2009, Zero Trust was originally based on a network design that leveraged micro-segmentation to enforce granular control and limit lateral movement.

In 2014, Google unveiled BeyondCorp[2], its Zero Trust initiative that implements secure access for its employees based on devices, users, access control and encryption. The security landscape shifted from network access to resource access. Since then, it has served as reference model for many enterprises seeking to implement a Zero Trust security model at scale.

In 2017, Gartner rebranded its Adaptive Security Architecture to Continuous Adaptive Risk and Trust Assessment (CARTA)[3]. Using Zero Trust as a foundation, CARTA emphasizes adaptive risk assessment on an ongoing basis. In 2018, Forrester Research published their Zero Trust eXtended (ZTX) Ecosystem report, which extends their original model beyond network micro-segmentation[4]. The ZTX Ecosystem includes networks, devices, people, data, workloads, orchestration, visibility and analytics.

Elimination of trusted networks

Zero Trust eliminates excessive trust on networks and locations. Regardless of local or remote access, every single request is fully authenticated, authorized and encrypted based on device, user identity and access control policy.

Reduction of attack surfaces

Devices are verified before any access is granted. Multi-factor authentication (MFA) is often used with single sign-on (SSO) in the authentication process to reduce threats. Users are granted least-privilege access for their tasks, based on their roles, attributes and usage patterns. All access is encrypted, thanks to today's efficient cryptographic technologies.

VPN vs. Zero Trust secure access

Zero Trust provides next-generation secure access to enterprise applications and resources from anywhere without the need for traditional VPNs. It reduces IT burdens and maintenance costs associated with VPN client software. Compared to traditional VPN Layer-3 connectivity, Zero Trust fine-grained access control improves security by limiting lateral movements and preventing data leakages. A consistent user experience between local and remote access maximizes ease of use and minimizes end-user training costs.

---

[2] R. Ward and B. Beyer, BeyondCorp: A New Approach to Enterprise Security, Google, 2014

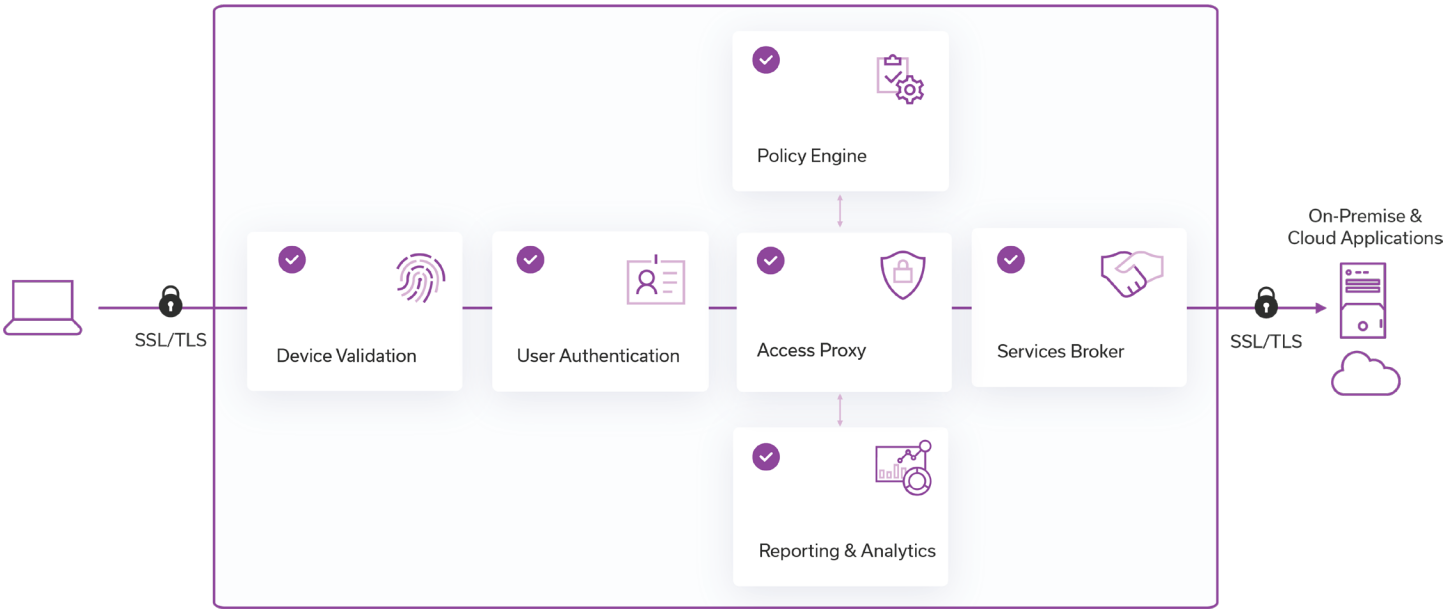
[3] N. MacDonald and F. Gaehtgens, Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, Gartner, 2017

[4] C. Cunningham, The Forrester WaveTM: Zero Trust eXtended (ZTX) Ecosystem, Forrester, 2018

zentry

ESSENTIAL ZERO TRUST ELEMENTS

Based on the “never trust, always verify” principle, the Zero Trust security model evolves beyond network security into next-generation secure access. It provides device-aware, identity-aware and policy-based access to applications and resources across on-premise and cloud environments with end-to-end encryption. Essential elements are shown in the following diagram.



Device Identity

Uniquely identify all managed devices using device fingerprinting, such as certificates. Manage device certificate creation, revocation and renewal.

User Identity

A single sign-on (SSO) system with multi-factor authentication (MFA). Supports AD, LADAP and Radius, as well as federation SAML and OIDC.

Access Gateway

High-performance application proxy, enforces end-to-end encryption, provides load balancing, application health checks at scale. It delegates requests to emulation proxy or web applications based on access control provided by the policy engine.

Services Broker

A set of emulation proxies webify resources including desktops, SSH, Telnet and legacy web applications, and provide uniform access. Access policies are defined by the policy engine.

Policy Engine

Provide flexible and fine-grained access control to applications and resources on a per-request basis. Authorization is based on attributes, such as device, user, group, role, target resource, IP, location, time, etc.

Reporting & Analytics

A centralized mechanism to analyze, search and visualize data at scale on application usage, application metrics, user metrics, compliance reporting, audit logs, application logs and more.

zentry

MIGRATION TO ZERO TRUST WITH ZENTRY

Zentry allows IT to provide users with Zero Trust secure access to any application or resource on any devices with zen-like ease-of-use, and may be customized based on individual enterprise requirements. Founded on over years of accumulated experience in access proxy, policy-based access control, TLS encryption and AAA, Zentry is 100% focused on delivering Zero Trust secure access solutions to enterprise customers.

HOW ZENTRY WORKS

Zentry integrates all of the essential elements required to enable a Zero Trust security model.

Access Gateway

A high performance access proxy that communicates with all Zentry components, and ensures that secure access is fully authenticated, authorized, encrypted using device validation, user authentication with MFA, SSO, and policy enforcement. It delivers the following capabilities:

- Device validation
- User authentication with MFA and SSO/federation
- Access proxy, load balancing and application health checks
- End-to-end encryption

Policy Engine

Built on open standards, the policy engine provides flexible and fine-grained policy controls for access on a per-resource basis.

Service Broker

A set of emulation proxies webify resources such as desktops, SSH, Telnet and legacy web applications.

Transient Authentication

A password-less single sign-on function that uses automatically generated temporary credentials for seamless access to IT infrastructure. Along with Zentry's service broker, transient authentication can provide privileged user access to mission-critical IT infrastructure including routers, switches and firewalls.

Reporting & Analytics

A centralized way to monitor and analyze data on applications, users, infrastructure, logs and more.

Device Identity

A registration service that allows users to register devices with Zentry. Once registered, PKI is used to bind the device signature to device certificates which can then be validated by the Zentry access gateway prior to users logging on.

zentry

KEY USE CASES

Remote working

Zentry helps enterprises enable next-generation secure access for remote working, replacing traditional VPN with improved security, ease-of-use and productivity.

Resource protection

Zentry is also suitable for resource protection. It protects internet facing websites and resources from unrestricted access by enforcing user authentication, authorization and access control policies designed to safeguard enterprise digital assets.

Privileged user access

Zentry modernizes privileged user access by combining SSO, MFA and a password-less transient authentication mechanism for seamless access to back-end IT infrastructures.

KEY ZENTRY ATTRIBUTES

- Clientless, consistent user experience
- High-performance access gateway and policy engine
- Flexible, scalable and reliable architecture
- End-to-end encryption (TLS 1.3), with high-throughput, low-latency TLS processing
- REST API for 3rd-party integrations (IdP, MFA, etc), open, flexible and extensible
- Password-less transient authentication for privileged access management
- Self-service admin portal with centralized controller for subscription, configuration and orchestration

THE ZERO TRUST JOURNEY

Zentry provides an ideal starting point for enterprises to begin a journey to Zero Trust. The first step is to define a project scope. You need to identify the systems and data you wish to protect the most in your enterprise (for example: finance, DevOps, etc.). Next, prioritize use cases and analyze workflows. Zentry makes it simple to implement Zero Trust for a select set of applications, assess the results, then implement more broadly across the organization over time.

CONCLUSION

The security landscape is shifting from a traditional perimeter model to a new Zero Trust security model. Zero Trust security evolves beyond network segmentation into next-generation secure access. Zentry, based on “never trust, always verify” principles, provides identity-aware, policy-based secure access solutions with enhanced security, improved productivity and ease of use. It is an ideal starting point for the Zero Trust journey.

Zentry can assist you in learning more about Zero Trust solutions and keep you informed on future developments, so that you can make the most informed decision about your company’s Zero Trust secure access requirements. Learn more on our Zentry product page, our Zentry solution page, or start a free 30-trial of the Zentry product today.

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

1-844-2-ZENTRY
(408) 240-8754

info@zentrysecurity.com
www.zentrysecurity.com