cpl.thalesgroup.com

THALES

Meeting NIST Guidelines for Zero Trust Security

White Paper

Contents

3 Introduction

3 Zero Trust: Beyond "castle-and-moat"

4 A new blueprint for Zero Trust?

5 NIST Approaches to Zero Trust Architectures
5 Identity-centric
6 Network-centric
7 Cloud-based combination

7 Implementing Zero Trust with Thales SafeNet Trusted Access

8 Benefits of using Thales SafeNet Trusted Access to implement Zero Trust
8 Architecturally logical approach
8 Flexible and agile
8 Ease of deployment, management and scalability
9 Smooth and familiar user experience

9 Conclusion

9 About Thales

Introduction

Digital transformation, the proliferation of disruptive technologies and emerging trends such as 'work from home' have made the digital boundaries of corporates disappear. With boundaries diminishing, traditional perimeter security solutions have become inadequate to respond to increasing demands for access from literally everywhere.

These developments coupled with the alarming increase in data breaches and security incidents have rendered the concept of trust extinct. Hence, Zero Trust security is based on the tenet "Never Trust, Always Verify" and views trust as a vulnerability. Zero Trust security requires strict and continuous identity verification to minimize implicit trust zones. NIST recently published a blueprint for Zero Trust security which provides guidance on how to build effective Zero Trust security architectures.

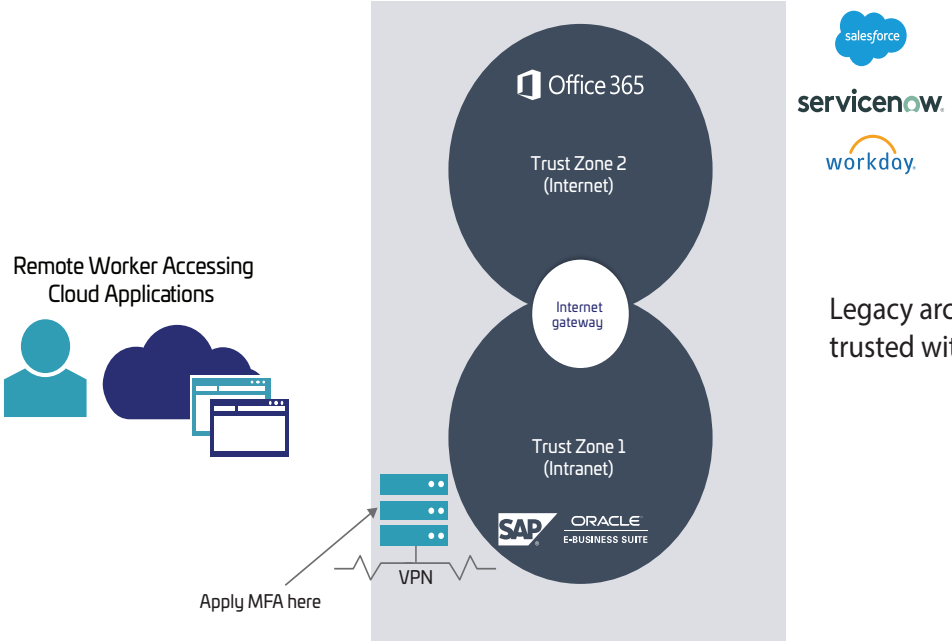
The purpose of this whitepaper is to assess the NIST Zero Trust guidelines and provide concrete guidelines on how to implement an effective identity-centric Zero Trust architecture with the goal of achieving security in a post-perimeter environment.

Zero Trust: Beyond "castle-and-moat"

Back in the 1980s, US President Reagan, when referring to the then USSR, used the term "trust but verify." Fast forward to 2020s and the digital transformation of businesses through the adoption and proliferation of technologies such as IoT, cloud delivery, and mobile adoption have led to the disintegration of the traditional IT security perimeter. In this environment, where applications are delivered from the cloud to the cloud, where users are located everywhere and where multiple devices are in use, the ability to rely on a single point of trust is untenable; all interactions are inherently risky, necessitating a "never trust, always verify" stance.

Zero Trust is a strategic initiative and principle that helps organisations prevent data breaches and protect their assets by assuming no entity is trusted. The National Institute of Standards and Technology (NIST) defines Zero Trust as "a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised."

Zero Trust goes beyond the "castle-and-moat" concept which dominated traditional perimeter security, recognizing that when it comes to security, trust is a vulnerability. Traditional security concepts considered all users trusted once inside a corporate network – including threat actors and malicious insiders. Trust gave them the right to move laterally and freely access or exfiltrate whatever data they were not limited to.



Legacy architectures consider users trusted within implicit trust zones

Zero Trust is a security model that requires strict identity verification and moves the decision to authenticate and authorize closer to the resource. The definition of Zero Trust indicates that its focus is on authentication, authorization, and minimizing implicit trust zones while maintaining availability and providing seamless authentication mechanisms. Access rules are as granular as possible to enforce least privileges required to perform the requested action.

To achieve its goal, Zero Trust is governed by the following foundational principles:

- Access to corporate resources is determined by a dynamic policy, enforced on a per-session basis, and updated based on information collected about the current state of client identity, application/service, and the requesting asset, including other behavioural and environmental attributes
- All communications to resources must be authenticated, authorized, and encrypted
- Authentication and authorization are agnostic to the underlying network
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets

A new blueprint for Zero Trust?

In the modern, digital landscape, where employees' mobility and customers' habits for omnipresence require access to resources anytime and from anywhere, traditional perimeter security seems inadequate to protect from sophisticated cyber-attacks.

The use of legacy security solutions, which rely on on-premises routing, to enforce authentication and authorization to the cloud hampers productivity, scalability and user experience and increases operational costs. Relying on legacy solutions leads to complexity, admin overhead and creates fog and friction for users.

The proliferation of IoT, multi-cloud platforms, and containers require the creation and management of numerous identities to authenticate them. As a result, businesses have become increasingly reliant on identities and credentials. Not surprisingly, these credentials are attractive targets for cyber criminals. Compromised credentials and identity theft are the main causes of security incidents and data breaches.

"The use of legacy security solutions, which rely on on-premises routing, to enforce authentication and authorization to the cloud hampers productivity, scalability and user experience."

Because of the expanding attack surface, regulations such as GDPR, CCPA, PCI DSS and HIPAA are based on the accountability principle and require the strong authentication and authorization of every data communication and process.

Further, the global working environment is changing. Remote working trends, fuelled by the COVID-19 pandemic, accelerates the adoption of cloud platforms, and increases the need to effectively authenticate and grant access to corporate resources based on contextual, adaptive, and dynamic decisions – at the access point.

These developments have led NIST to standardize Zero Trust architectures. NIST SP 800-207, Zero Trust Architecture, serves as a blueprint for Zero Trust and "gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture." The release of this publication will lead to greater adoption of the Zero Trust security model.

NIST Approaches to Zero Trust Architectures

NIST describes three approaches to building an effective Zero Trust security architecture.

Identity-centric

The identity-centric approach of Zero Trust architecture places identity of users, services, and devices at the heart of policy creation. Enterprise resource access policies are based on identity and assigned attributes. The primary requirement to access corporate resources is based on the access privileges granted to a given user, service or device. To cater for a more adaptive authentication, the policy enforcement may consider other factors as well, such as device used, asset status, and environmental factors.

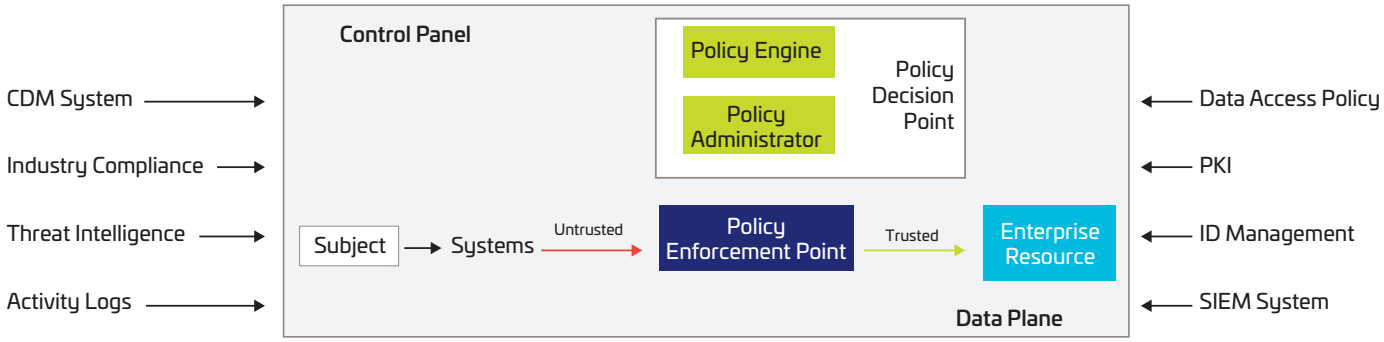


Figure 1: NIST Identity-Centric Zero Trust Architecture Approach. Source: NIST SP 800-207

Network-centric

The network-centric approach of Zero Trust architecture is based on network micro-segmentation of corporate resources protected by a gateway security component. To implement this approach, the enterprise should use infrastructure devices such as intelligent switches (or routers), Next Generation Firewalls (NGFW) or Software Defined Networks (SDN) to act as policy enforcement protecting each resource or group of related resources.

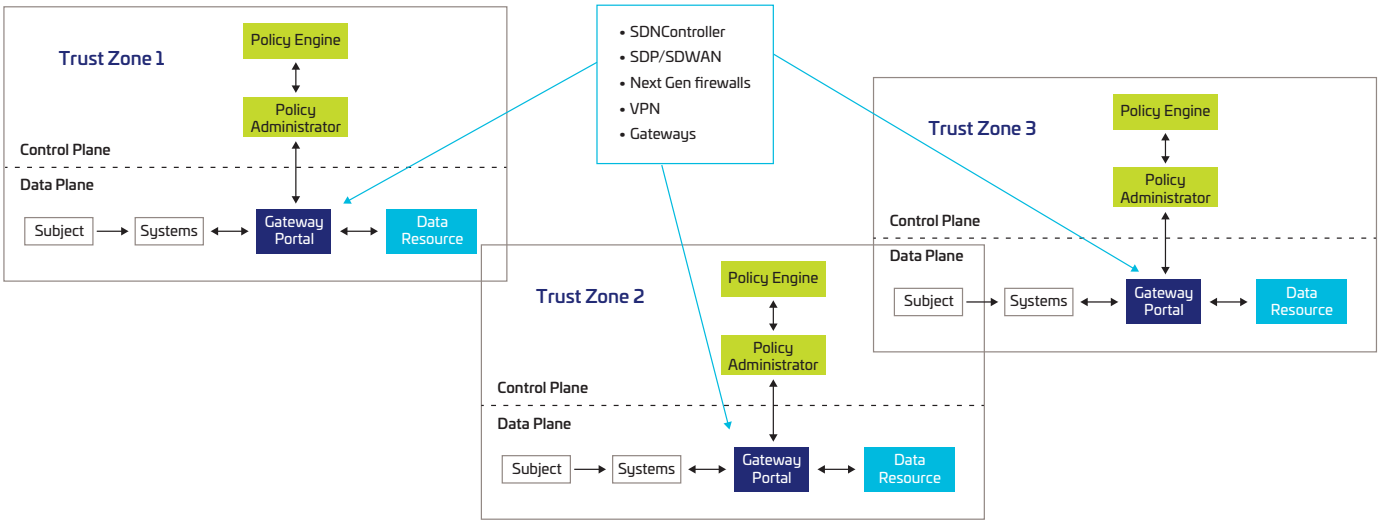


Figure 2: NIST Network-Centric Zero Trust Architecture Approach. Adapted from NIST SP 800-207.

A network-centric approach focuses on segmenting the traditional perimeter into sub-zones. Users are considered trusted once inside a zone. While reducing risk to a degree, the network-centric approach is not risk free since it assumes an entity is trusted once inside the zone. For this reason, this approach would require additional security measures and strong identity governance.

Identity-centric	Network-centric
Relying on a strong identity trust model allows fast adoption of new technologies	Complex to configure, troubleshoot and manage given the multitude of network security zones
Identity trust is a self-reinforcing model: the more you assess/ control identities across systems, the more knowledge you gain and the stronger the trust becomes	Single point of vulnerability: Once users are in the zone, they are free to roam with limited control and visibility on what they do
Identity-trust assessment becomes easily pervasive and can be consumed by new services to make simple security decisions	May not be able to support cloud apps in a trust zone
	Letting non-employees inside these zones is bad practice but difficult to avoid (e.g. contractors)

Table 1: Comparison of identity-centric and network-centric Zero Trust approaches

Cloud-based combination

A cloud-based combined Zero Trust architecture approach leverages cloud-based Access Management and Software at the Service Edge (SASE). The cloud-based Access Management solution protects and enforces the identities of cloud applications and services, while SASE components, such as Software Defined Networks (SDNs) or Next Generation Firewalls (NGFW) protect on-premises resources and monitor network traffic.

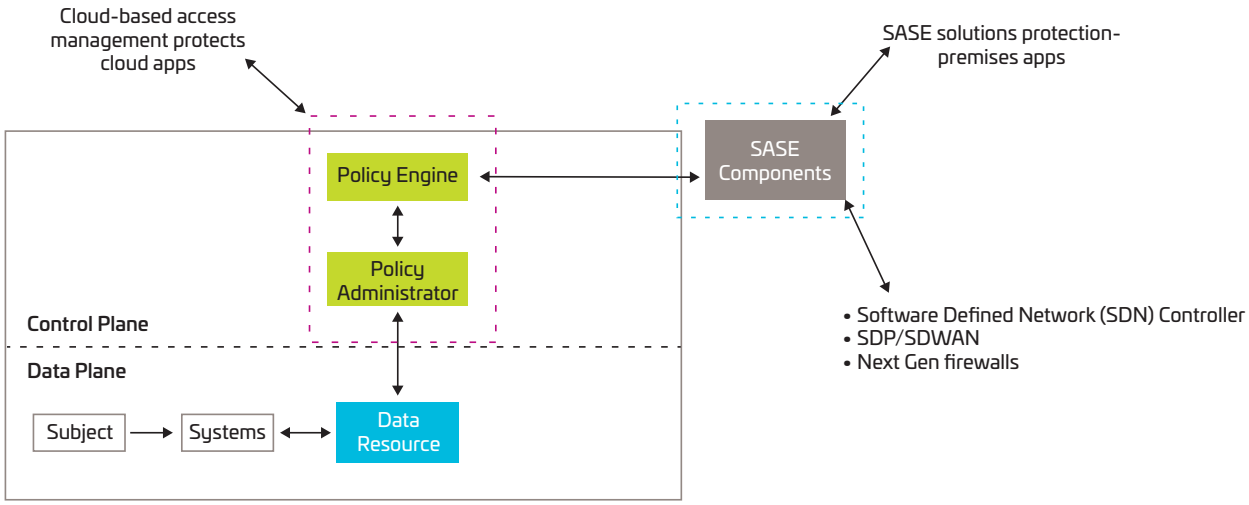


Figure 3: Combined, cloud based Zero Trust architecture approach.

Implementing Zero Trust with Thales SafeNet Trusted Access

The modern enterprise security perimeter is no longer a physical location; it is a set of access points dispersed in and delivered from the cloud. Identities are now the new perimeter and should be at the core of access decisions. The identity of any resource, user, device, or service, provides the key context for the application of access policies.

Identity is the cornerstone for Zero Trust security for application and data assets that an enterprise wants to ultimately protect. The greatest challenge is to employ a comprehensive Zero Trust security solution that covers identities and data end-to-end. With its cloud-based access management and authentication solutions, Thales addresses crucial Zero Trust security needs of enterprises holistically.

SafeNet Trusted Access is the starting point for effective Zero Trust security implementations, meeting Zero Trust principles:

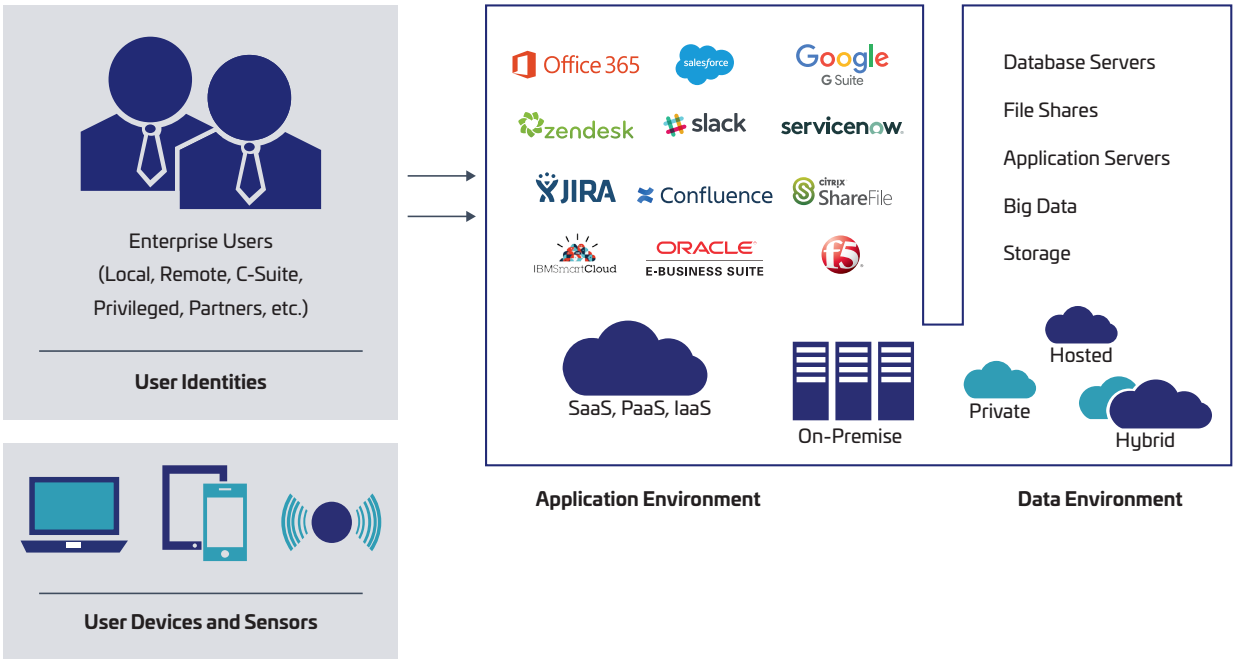
- Access decisions are enforced dynamically at the application access point, irrespective of where the app resides, where users reside, what device users use and network routing
- Access decisions are aided by updated inputs from third party network security vendor technologies such as VPNs, WAMs, WAFs, SASE etc.
- Access decisions adhering to a 'default deny' stance are continuously reassessed even if Single Sign On (SSO) features are enabled.

Benefits of using Thales SafeNet Trusted Access to implement Zero Trust

There are several benefits to using SafeNet Trusted Access to implement an identity-centric Zero Trust architecture:

Architecturally logical approach

Legacy perimeter solutions control traffic through a central, on-premises hub, which is not effective for traffic generated or routed to the cloud and could create a bottleneck and a single-point of access failure. SafeNet Trusted Access was born and lives in the cloud. Hence, it is not dependent on on-premises infrastructure and can control access in the cloud avoiding bottlenecks. In addition, since all authentication and access decisions are continuously enforced at every access point, SafeNet Trusted Access enables security throughout dispersed network environments, enabling the implementation of Zero Trust approaches.



Flexible and agile

One of the core strengths of SafeNet Trusted Access is its policy engine, which allows for setting access policies that are extremely flexible. Security policies cater for the creation of very granular and specific rules to constantly reassess users during an open session, rather than only for certain events such as authentication time-outs. If the level of risk changes, SafeNet Trusted Access forces the user to re-authenticate or step up to a stronger form of authentication. Policies can be set per application, apply to network ranges, operating systems, and user collections and geolocations. Authentication rules can be established as dynamic and as context specific as needed adapting to changes in a dynamic cloud environment.

Ease of deployment, management and scalability

SafeNet Trusted Access offers a simple and scalable way to enable 'work from home' or 'work from anywhere'. While SASE solutions are still evolving and legacy solutions are not adequate to accommodate modern Zero Trust requirements, the SafeNet Trusted Access platform is readily available, established and proven. With identity-centric Zero Trust being consumed by all technologies and services, SafeNet Trusted Access offers a future-proof, adaptive solution to safeguard corporate resources wherever they are.

Smooth and familiar user experience

The ability to integrate seamlessly into a broad range of applications and services is key to ensuring a standardized unified access framework, as well as a consistent authentication experience for end users. SafeNet Trusted Access offers consistent application access across all login scenarios and applies unified network routes for all applications, whether they are cloud based or protected behind VPNs or internet proxies. Finally, to cope with the increasing 'work from home' requirements, SafeNet Trusted Access can enable BYOD schemes without compromising security.

Conclusion

In the traditional "castle & moat" security concept, bad actors were considered trusted once inside corporate networks and were free to roam unencumbered. Zero trust security concepts allow organizations to grow securely in the cloud and adjust to borderless and dispersed environments. SafeNet Trusted Access meets these needs by ensuring a 'trust no one, verify everywhere' stance through its ability to continuously protect applications and services at the access point, regardless of the underlying network deployed, the location of the app, the location of the user or the end device being used.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <