A Concepta Innovation Services White Paper
June 2021

1700 Rockville Pike, Ste 400
Rockville, MD 20852
877-594-1944
www.conceptainnovation.com

Zero Trust Maturity Assessment

White Paper

By Agatha Onyewuchi
Principal Partner

Contents

Abstract

This white paper provides guidelines to help facilitate Zero Trust Architecture adoption by federal agencies, state government, and private sector organizations. It focuses on Zero Trust readiness assessments, gap analyses and maturity assessments, highlighting targeted milestone guidance and solutions for effective Zero Trust Architecture adoption.

1.1 Introduction

The National Institute of Standards and Technology (NIST) defined Zero Trust as "cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated". In essence securing your organization with Zero Trust is to "Never trust, always Verify". It is extremely important for organizations today to mature and adopt an assume breach mentality, adopting more detect and respond controls.

1.2 Executive Order on Improving the Nation's Cybersecurity

President Biden signed the cybersecurity directive on May 12, 2021, to address the increasingly sophisticated cyber threat environment, which outlined decisive steps agencies must take to modernize its approach to cybersecurity, the adoption of cloud services and use of Zero Trust Architecture.

The goal of the cybersecurity directive is not only the adoption of Zero Trust but also the use of analytics to get visibility, drive threat detection, and improve defense.

.

1.3 Why Zero Trust Methodology?

The use of cloud and mobile technologies, remote work and bring your own device (BYOD) have reinvented the security perimeter. The new perimeter now extends to every access point that hosts, stores, or accesses corporate resources and services. Traditional security models that rely only on on-premises firewalls, virtual private network (VPNs) and Identity provider lack the visibility, solution integration and coordination to deliver timely, holistic enterprise security coverage.

Zero Trust Methodology addresses the complexity of the modern environment with a security model that protects people, devices, applications, and data in any location and environment.

As seen in the recent cyber-attacks, a data breach can have far-reaching consequences, not just in financial losses to government, organizations, and individuals, but also human cost in time, in peace of mind, and a loss of the sense of control over one's environment.

1.4 Adopting Zero Trust

Effective Zero Trust implementation requires comprehensive information security and resiliency practices, which includes the use of automated enforcement of security policy to ensure compliant access decisions throughout the enterprise asset.

Organization may need to invest in both technology and skilled personnel to implement framework of controls into the security solutions and tools, and fine tune access policies to deliver the right balance between security, optimal user experience, and ultimately their modernization goals.

The implementation requirements will differ for each organization based on existing technology in the enterprise infrastructure, and security posture. Zero Trust focuses on the security and compliance of assets regardless of their physical or network location.

Zero Trust Maturity Assessment

We have found the following Zero Trust model very comprehensive and effective in helping our customers determine their Zero Trust readiness, secure their enterprise infrastructure, and plan their Zero Trust Architecture adoption. Zero Trust approach is an end-to end assessment strategy of the entire enterprise assets, extending across these crucial elements: identities, devices, applications, data, infrastructure, and networks. Zero Trust assessment requires the validation and trustworthiness of these elements.

The diagram below from Microsoft shows how Zero Trust security with a security policy enforcement engine can assess in real-time. The model grants access to data, apps, infrastructure, and networks after verifying and authenticating identities and checking the safety of the devices.

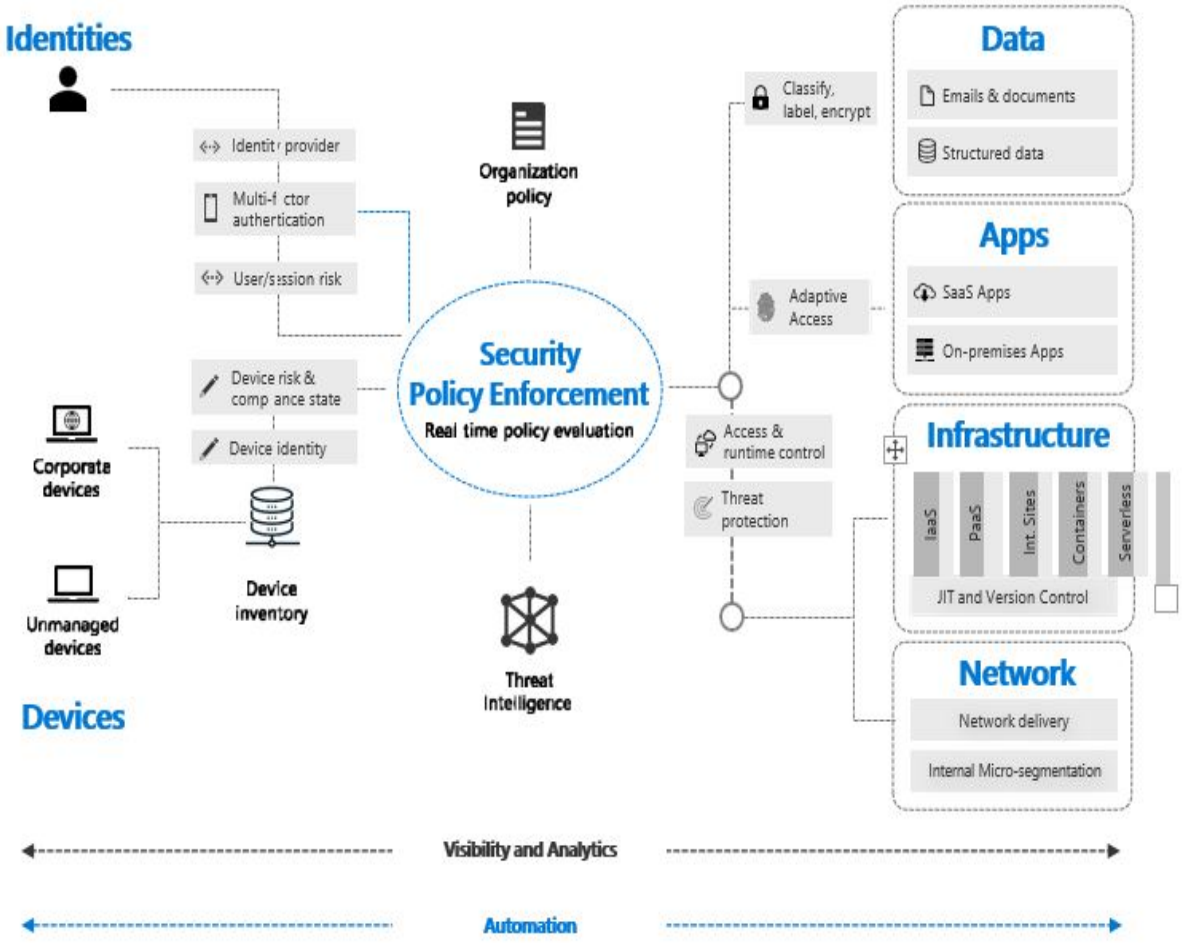

Figure 1 Zero Trust across Enterprise Assets
Source: Microsoft Corp.

2.1 Identities

Identity and Access management (IAM) is a foundational and critical cybersecurity capability. Majority of organization face challenges in the areas of identity federation, Identity governance, user provisioning and de-provisioning, entitlement management, limited visibility of identity risks, etc. As employees and partners collaborate and access organizational resources from anywhere, on virtually any device, it quickly becomes clear that the approach to securing the enterprise needs to be adapted to the new reality.

Identity Governance for federal agencies entails evaluating the available frameworks, which include PIV/CAC cards, Trusted Internet Connection (TIC 3.0), and Continuous Diagnostics and Mitigation (CDM) and aligning to requirements for Zero Trust architecture.

The identity Zero Trust security model is a powerful, flexible, and granular way to control access to data, for people, services, and or within the Internet of Things (IoT) devices. Robust Identity process should verify the identity with strong authentication, least privilege access principles, etc. Microsoft advocates an "assume breach" which means minimizing lateral movement within the network, verifying encryption of all sessions and use of analytics to get visibility and drive threat detection, and improve defense.

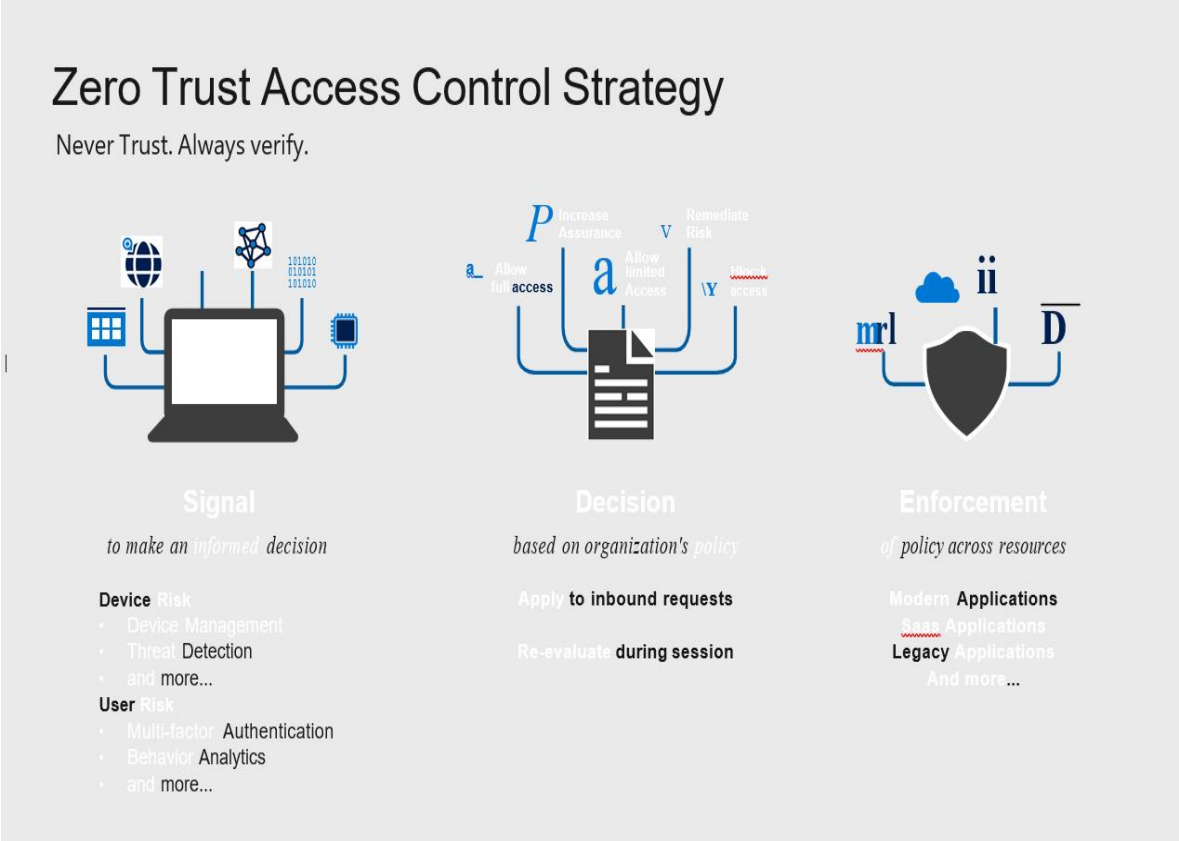

Figure 2 Zero Trust Access Control Strategy
Source: Microsoft Corp.

2.2 Devices

Devices including mobile devices are leading assets within modern workplaces. Organizations are challenged with device security-ensuring devices process, modify and store sensitive data securely. The Device Zero Trust security assesses data flow to different endpoints from IoT, mobile, BYOD, partner, and on-premises to cloud technologies, wherever the endpoints are connected, whether the corporate network, home, or public internet. Ensuring device health and compliance for secure access.

2.3 Applications

The Application Zero Trust security will assess Applications and application programming interface (API) such as legacy on-premises, Software as a service (SaaS) and or migrated apps to the Cloud. Ensuring the use of policy-based access controls for apps; policy-based session controls (such as preventing data exfiltration, protect on download, preventing uploads, blocking malware, etc.) Application-level security is important, therefore controls and technologies should be implemented to ensure appropriate permissions, discover shadow IT, validate secure configuration, and real-time analytics.

2.4 Data

Data flow control regulates where information can travel within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Zero Trust Data security focuses on data classification and protection. Ensuring data encryption at rest or in transit, and monitoring of sensitive data to minimize exposure from malicious or accidental exfiltration.

2.5 Infrastructure

The use of legacy infrastructure and software usually involves a greater maintenance cost, and the systems are exposed to more cybersecurity dangers. Modernization is vital for managing those risks and improving efficiency and the effectiveness of enterprise assets.

Infrastructure—whether on-premises servers, cloud-based virtual machines (VMs), containers, or micro-services represents a critical threat vector. Zero Trust security assess configuration version, access to privileged resources, threat detection tools, and use of telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.

2.6 Network

Network Zero Trust assessment requires a holistic approach of ongoing processes and practices to ensure the protection of the underlying infrastructure. All enterprise data is accessed over network infrastructure; therefore, all networking controls provide critical functionality to enhance visibility and help prevent attackers from moving laterally across the network. Zero Trust security assessment focuses on network segmentation, real-time threat protection, end-to-end encryption, monitoring, analytics, and TIC policy enforcement security capabilities.

3.0 Conclusion

Zero Trust Architecture is a multifaceted journey that requires definitive goals, outcomes, and architectures. Organizations should undertake incremental implementation of zero trust principles, process changes, and technology solutions that protect critical enterprise assets.

4.0 About Concepta Innovation Services

Founded in 2018, Concepta Innovation Services, is a women-owned minority small business, and a Microsoft Partner. We conduct Zero Trust assessment readiness to help organizations identify activities already in existence, and activities required to implement an effective Zero Trust journey, focusing on solutions with the most security impact.

We offer Zero Trust deployment solutions to customers to fit their unique business, compliance, and technical requirements. We integrate elements of Zero Trust in our Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) design and deployment in a shared multi-tenant or dedicated single tenant cloud environment through cloud providers such as Microsoft Azure, and Amazon Web Services, etc.

5.0 Acronyms

NIST	National Institute of Standards and Technology
BYOD	Bring your own device
IAM	Identity and Access management
IoT	Internet of Things
API	Application programming interface
VMs	Virtual machines
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a service
PIV Card	Personal Identity Verification
CAC	Common Access Card

Keywords
Zero Trust; Executive Order, cybersecurity; IT modernization; zero trust maturity assessment; security assessments; identity and access management; Cloud technologies; system; enterprise assets; critical assets; analytics.

References

Executive Order on Improving the Nation's Cybersecurity
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

NIST Special Publication (SP) 800- 207: Zero Trust Architecture:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Microsoft Zero Trust Business Plan:
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4JAsW

NIST Special Publication (SP) 800-53 Rev.5:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf