Verify Zero Trust Security Whitepaper

Contents

Introduction

This document describes information related to Zero Trust and how it can be used to secure the enterprise.

Executive Summary

Zero Trust represents a model that assumes no user, device, or application, whether outside or inside the network, can be deemed safe, and that each must be validated before it is allowed access to network assets.

This concept has gained more importance in virtualization and the rapid movement of on-prem resources to public, private, and hybrid clouds.

The term Zero Trust was created by Forrester in 2010 with the release of their Zero Trust Network Architecture Report.

It is important to understand that Zero Trust must start as a strategy at the business level to protect vital business interests and initiatives.

Zero Trust Pillars

What is Zero Trust?

Zero Trust is a strategic approach that encompasses various technologies to help achieve more practical security for today's infrastructures. It is a security architecture and enterprise methodology designed to effectively orchestrate today's combination of technologies, practices, and policies.

It represents an evolution in our approach to security and delivers a comprehensive, interoperable, and holistic solution approach that incorporates multiple vendors' products and services.

Zero Trust is based on many established technologies such as network segmentation, multifactor authentication, and network access control.

Why is Zero Trust Important

Zero trust helps protect the enterprise from unauthorized users, breaches, and cyberattacks. You can continuously verify the identity of users and devices and allow them only the permissions they need to do their work to minimize the risk of a security event.

Market research has shown that the global Zero trust security market size is expected to grow from an estimated value of USD 27 Billion in 2022 to around USD 60 Billion by 2027/2028, at a Compound Annual Growth Rate of around 17% at that time.

Motives:

- Heightened frequency of Target-Based Cyberattacks.
- Growth in Regulations for Data Protection and Information Security.
- Greater Need to Reduce Business and Organizational Risks.
- As more services are migrated to the cloud, centralized data deployment surpasses data boundaries and magnifies security risks.

- The need to confirm the identity of the user throughout the entire access process and not just initially.

A single ransomware attack costs $5 million. Cybercriminals do not discriminate when they target businesses.

Recent CIO and CISO surveys show that Zero Trust is one of the Top 5 priorities. CISOs say a shift to remote work, a labor shortage, and a large spike in cybersecurity attacks demand their existing systems in the enterprise be secured.

Traditional vs Zero Trust Model

Traditional environments are where security has been added after the environment was built. Normally, they are flat networks where defences are built around the edge of the network to prevent attacks from the Internet.

Zero Trust is generally recognized to focus on the need to protect the systems and data of an organization on multiple levels with a mixture of encryption, secure computer protocols, dynamic workload, and data-level authentication and authorization, and does not rely solely on an external network boundary.

The traditional perimeter-centric security architecture is less effective as workloads are increasingly delivered from the cloud, and mobile endpoints become the norm for application and data access.

Zero Trust Architectural Framework

A Zero Trust Architectural Framework deals with the restriction of access to systems, applications, and data resources to those users and devices that specifically need access and have been validated. They must be continuously authenticated to their identity and security posture to ensure proper authorization for each resource to provide access.

The framework is to provide a road map to migrate and deploy zero trust security concepts to an enterprise environment and is based on NIST Special Publication 800-207.

An effective Zero Trust Architectural framework coordinates and integrates across these seven main core components.

- Zero Trust Networks are an important characteristic of a Zero Trust strategy which refers to the ability to segment networks or isolate network assets and maintain control of communications between them. Also, it secures trusted connections to extend the workplace for remote use.
- Zero Trust Workforce encompasses methods to limit and enforce user access, which includes technologies to authenticate users and continuously monitor and govern their access privileges. This access is secured by technologies such as DNS, multifactor authentication, and network encryption.
- Zero Trust Devices addresses the need to isolate, secure and manage all network-connected devices, which have grown with the addition of mobility and the Internet of Things, to create an immense vulnerability for attackers to exploit.
- Zero Trust Workloads secure the front-to-back application stacks that run critical business processes. Focuses to secure east/west traffic between applications, data, and services in a data center to better protect critical applications.
- Zero Trust Data refers to methodologies to classify and categorize data, combined with technology solutions to secure and manage data, which includes encryption of data.
- Visibility and analytics refer to technologies that provide the awareness for automation and orchestration and enable administrators to not only see but also understand the activity in their environments, which include the presence of real-time threats.
- Automation and orchestration encompass tools and technologies such as machine learning algorithms

and artificial intelligence to automatically classify network and data center assets, and to suggest and apply segmentation and security measures, policies, and rules to be automatically put into effect; therefore, reduce the burden on security teams and accelerate attack mitigation.

Zero Trust and Segmentation

Every network-based resource must be secured and segmented with the principle of least privilege. This is best accomplished via an asset management system that controls credentials and access for every purpose.

The need for Zero Trust segmentation includes brand protection, limited attack surface, improved network stability, and enablement of quick service deployment.

To assist in further achieving protection for individual resources, micro-segmentation can be used. Scalable Group Tags (SGTs) can be used where a tag value is inserted in the Ethernet frame to uniquely identify a resource. Furthermore, infrastructure devices encompass intelligent switches, routers, or next-generation firewalls that can be used as gateway devices to protect each resource.

Visibility, Analytics, and Automation

It is important to have complete visibility into all the assets of the organization and any activities associated with those assets. This is the foundation of Zero Trust.

To provide dynamic policy and trust decisions, there needs to be a continuous gathering of analytics. Our Zero Trust architectural approach focuses on the core logical components of an SDN strategy with a Policy Engine and Policy Administrator to form a Control Plane to restrict access to resources via Policy Enforcement Point(s) in a Data Plane.

The capabilities needed for Zero Trust Architecture to provide greater network context, learning, and assurance to securely accomplish its mission:

- Granular micro-segmentation of access to users, devices, applications, workloads, and data.
- Enforcement of security policies everywhere that work is performed, which includes LANs, WANs, data centers, clouds, and the edge.
- Comprehensive identity management – to extend identity and access management to include, the identities of users, devices, applications, workloads, and data which become new micro-perimeters via software-defined access.
- Integrated threat defense that leverages global threat intelligence and feeds.
- Fully automated, agile control of the network of your organization to securely function at the desired scale, performance, and reliability required to accomplish the objective.

Steps to Zero Trust

The key to comprehensive Zero Trust security is to extend the security throughout the entire network environment, whether it be the LAN, Data Center, Cloud edge, or Cloud. Compliance is of course mandatory.

This security must include total visibility of the network environment of your organization. Key steps to comprehensive Zero Trust center around:

- Identify devices and sensitive data. Perform identification and classification of devices, sensitive data, and workloads.
- Understand the Flows of Your Sensitive Data.
- Architect Your Zero Trust segmentation policy. Each network-based asset must be secured and

segmented appropriately with the principle of least privilege and strictly enforced, granular controls so users have access only to the resources needed to perform their job.
- Implement policies and posture. This can be performed with platforms such as Cisco DNAC or ISE.
- Continuously monitor the Zero trust environment. Implement security analytics to real-time monitor and analyze security incidents and quickly identify malicious activity. Continuously inspect and log all traffic both internally and externally.

Achieve Trusted Access

To achieve comprehensive Zero Trust security, organizations must extend their Zero Trust approach across their entire workforce, workplace, and workloads.

- Zero Trust Workforce - Users and devices must be authenticated and authorized and access and privileges continuously are monitored and governed to protect resources.
- Zero Trust Workplace - Access must be controlled across the entire workplace, which includes the cloud and edge.
- Zero Trust Workloads - Granular access control must be enforced across entire application stacks, which include between containers, hypervisors, and microservices in the cloud as well as traditional agency data centers.

Cisco, a Forrester-recognized Zero Trust Leader, is a strong advocate of Zero Trust enablement throughout your entire network – both on-prem and in the cloud. You can not only leverage your Cisco networking infrastructure as a critical foundation of your Zero Trust Architecture, but you can also learn about other key Cisco Zero Trust security capabilities that can help your organization on your Zero Trust journey.

Cisco Secure Portfolio

These can be used to build a successful Zero Trust framework:

- Frictionless, secure access for users, devices, and applications through **Cisco Duo**
- Flexible cloud security through **Cisco Umbrella**
- Intelligent packet inspection through **Cisco Secure Firewall**
- Advanced Malware protection via **Secure Endpoint** (formerly AMP)
- Secure VPN and Remote Access through **Cisco AnyConnect**
- Holistic workload protection through **Cisco Secure Analytics** (formerly Stealthwatch)
- Protected network segmentation with the **Cisco Identity Services Engine** (ISE)
- Application visibility and micro-segmentation via **Cisco Secure Workload**
- Integrated security platform via **Cisco SecureX**
- Unified SASE solution with as-a-service subscription via **Cisco Secure Connect**
- Expert guidance from the **Cisco Zero Trust Strategy Service**
- Support and End-to-End services via **Consulting, Advisory, and Solution Services**

Summary

One of the simplest ways to think about Zero Trust is to “Never Trust AND Always Verify.” This applies to every network connection, every session, and every request for access to critical applications, workloads, and data.

Zero trust security frameworks create localized micro-perimeter defenses around each resource in the network of the organization. If correctly designed, the frameworks can protect assets regardless of where they are located.

An efficient way to reduce risk is to control access to privileged and shared data and adopt the principle of least privilege. This security model enables orchestration through APIs, as well as integration with workflow automation platforms which provide visibility into users and applications.

Successfully implemented, Zero Trust can help ensure secure and seamless operations across the entire information technology environment of an organization and result in continual trusted access to the critical workloads, applications, and data, of an organization, in order to enhance the missions of your organization.