netskope

White Paper

Zero Trust Leading Practice

EXECUTIVE SUMMARY

Many people think that digital transformation is just a trend. It is an economic disruption impacting the innovation and organizational development rhythm. Companies want to stay relevant, bring products and services to market faster, be agile, and have the ability to reinvent themselves at the right opportunity.

The massive growth of cloud computing and the explosion of mobile devices has created a habit out of users continuously craving access to the information from any place, any device, and at any time.

A legacy mindset is a hindrance to today's business. Companies are going to market with new business models, interacting with thousands of third-party relationships, which eventually creates a different view of how we should build for the future. Today, trust is observant, contextual, and adaptive, not black or white (block or allow) as in the past. No entity can assume implicit trust, and the components used to establish trust have to be assessed at all times. This is ultimately what zero trust is all about. A more systematic and secure approach to information access.

The current legacy technology ecosystem is dissolving and openness in thinking is vital. Digital transformation can't happen overnight or on its own. It requires security and IT transformation as a support mechanism. We need to rethink how we provide secure access to information through transparency because that is the only thing that keeps our users happy with a strong sense of loyalty.

Zero trust concepts, when applied correctly, can deliver exactly that.

The massive growth of cloud computing and the explosion of mobile devices has created a habit out of users continuously craving access to the information from any place, any device, and at any time.

INTRODUCTION

The exponential growth of cloud computing has not only enabled businesses to consolidate their hosting patterns and reinvent how they go to market It has also brought speed to execution that traditional IT teams struggled to address with legacy technologies. While we can summarize the past as "perimeter-based network architecture," today we are so much more open and diverse.

Cloud is "a business enabler" however, and it expanded the threat landscape in ways we have almost forgotten. This trend of "cloud evolution" changed how we assess trust in the context of business risk. Today, trust is observant, contextual, and adaptive, not black or white (block or allow) as in the past. No entity can assume implicit trust, and the components used to establish trust have to be assessed at all times. This is ultimately what zero trust is all about. A more systematic and secure approach to information access.

While many organizations drive outcomes through standardized approaches on endpoints, business leaders are considering end-user desires more than ever before. As a result, the operational aspect of these devices is becoming harder to manage, as there are more types of devices to support. Other companies are moving away from maintaining and operating endpoints, instead of letting users bring any kind of endpoint to the business environment and focusing on addressing the security of information.

Ultimately, what businesses want is to enable their users to be innovative, productive, safe, and secure, regardless of what type of device they use, what time they're working, or where they're working from. That requires keeping architectural and business openness in mind. Zero trust focuses on:

- Secure access of resources regardless of network location, user, or device
- Enforcing rigorous access controls, and inspecting, monitoring, and logging network traffic at all times

Zero trust continuously assesses all aspects of entity behavior during a network connection and provides adaptive access controls based on designated parameters and levels of acceptable business risk.

Purpose and Scope

The purpose of this document is to provide an understanding of principal components and implementation steps of pragmatic zero trust concepts.

The scope of this paper focuses on access to enterprise resources, behavioral analysis, and observations.

Audience

This document is intended for a diverse audience including security, system, and network architects, as well as security program leaders, who are responsible for the technical aspects of building, operating, and securing enterprise resources and assets. While technically oriented, the assumption is that readers will have a basic understanding of security, networking, and IT systems.

Zero trust continuously assesses all aspects of entity behavior during a network connection and provides adaptive access controls based on designated parameters and levels of acceptable business risk.

PRINCIPLES

Principles are general rules and guidelines that should be understandable, robust, complete, independent, and are not intended to state the obvious. They inform and support how an organization sets about fulfilling its mission and are designed to be enduring and seldom amended. Each principle should make a statement that aids the decision-making process in the enterprise.

Here are several high-level principles that provide guidance when implementing a zero trust strategy that every architect needs to be open to considering:

- Everyone in the organization must understand the business **CONTEXT**.
  - Business (information) assets must have defined criticality (typically derived by the Business Continuity Plan and business process it supports) and sensitivity (usually acquired by the company's information classification policy and the necessary integrity requirements of the data and business process).
- There must be **NO** implicit trust between entities.
  - All entities must be continuously verified and assessed throughout the network interaction.
- Trust is not binary but a continuum.
  - There are different levels of trust dependent on business context and acceptable risk appetite.
- Access is granted to the individual enterprise resource **ONLY**.
  - There is **NO** network access but only resource (application, services, etc.) access.
  - Avoid "trust zones" and instead leverage individual sessions.
- Assume all networks are the same
  - Assume the idea of equalizing the intranet and internet.

Assumptions

It is imperative to understand that certain conditions will be assumed, such as:

- The organization is willing and able to do what is necessary.
- The organization has business leadership support.
- The necessary resources exist or will be allocated to the organization.
- Technology capabilities are available to the organization.

DERIVING CONTEXT

Using zero trust principles represents a holistic and strategic approach to building a security program. A strategy must drive the policy that is applied based on a specific business context. It is imperative to understand that zero trust is not a band-aid or a product. Implementation should start with a coarse-grained approach, with the policy becoming more granular as more understanding of user needs, business requirements, and business impact develops.

The traditional thinking of applying controls through the concept of "Allow/Block" will not work anymore and will leave an organization with significant risk exposure. Organizations must use a risk lens to assess any type of resource access, which is highly dependent on context.

The quality of the context is extracted from several components that must be taken into consideration during any session interrogation, before connecting to its final destination. These components are:

- Data
- Identity
- Endpoint
- Application (resource)
- Network
- Visibility & Analytics
- Automation & Orchestration

Continuous Assessment

The continuous assessment of these components provides the contextual output used for a risk acceptance calculation that drives the control set influencing the dynamic policy adaptation before or during resource access.

Data

The business is always evolving, but the lifecycle of data stays the same. Data is the soul of any business and it should be treated that way.

While many organizations avoid or find it challenging to do the typical classification of their data, it is imperative to align to the first principle of zero trust, "Understanding the business context," and complete the following steps:

- Understand the data
  - Discovery (the business must understand the location of data)
  - Classification (the business must define its relative value, then analyze, contextualize, and organize it as such)

  - Map to confidentiality (derived from sensitivity), integrity (derived from sensitivity), and availability (derived from BCP / business-critical process)
    - » If this is unknown or undetermined, assign these categories (confidentiality, integrity, and availability) to a default rating. These details enable a policy to be applied in the first instance, which can then be further refined over time.
  - Identify data owners and data custodians.
- Protect the data
  - Inspection (inspect all data, e.g., SSL decrypt)
  - Governance (define rules and guidelines)
  - Control (apply technical control sets)

Identity

There are many users within any organization, but no user is the same. They all require a level of access to specific resources, and associated controls must be applied appropriately. It is crucial to follow full identity lifecycle management, starting with provisioning through management and governance to deprovisioning, when that identity is not needed anymore. Deprovisioning is a step where many organizations fail because of a lack of proper process.

Breach avoidance and avoidance of data corruption are primary outcomes derived from good identity governance and access management programs. If the right users have the proper access to the correct data at the right times, the risk of breach and corruption impacting a company's operations, and customers, is minimized. Identity governance and access management programs must be able to address the following:

- Access Management
  - User profile mapping
  - Provisioning, deprovisioning, and transfers
- Credential Assessment
  - Authentication & authorization
  - SSO & MFA
  - Privilege access
- Governance
  - Access governance
  - Request and approval process
  - Reconciliation and error processes

Endpoint

Times have changed since organizations required "only" company-managed devices. Today, users demand a variety of devices to do their jobs, so many organizations have started to accept BYOD (bring your own device). A healthy inventory of devices is essential for a managed set of devices, as they all have to be identified, isolated, and secured by implementing policy-based controls. However, businesses have to provide secure access to resources beyond just a company-provided device.

Enter untrusted or unmanaged devices. There is an increasing need for companies to allow access from third-parties, which in turn, will result in access from untrusted endpoints, in addition to the previously mentioned BYOD.

An organization must take endpoints (trusted or untrusted/managed or unmanaged) into account when they are defining their zero trust access policy. This is not a one-size-fits-all policy either, hence the need to understand the user and business context. In some scenarios, unmanaged devices will be afforded the same application (and subsequently data) access, as managed devices. In some cases, they will not—more on this in the section on risk scoring.

Application

With a proliferation of cloud and SaaS applications and services, business and operating models have changed. One of the essential aspects of security is to lock down access to resources, in this case, applications, to a minimum. Here, zero trust becomes extremely powerful as users no longer need to connect to networks, but instead, connect to a specific application or a service utilizing individual isolated sessions.

Any organization should have a clear understanding of the following from the application agreements:

- Application type
- Hosting model
- Confidentiality, integrity, and availability of the application (derived from the data it accesses, stored or processed, or business process it supports)
- Transaction flows - upstream and downstream
- Third-party access requirements
- The output of an application risk assessment

Network

Legacy perimeter is disappearing, connectivity is ubiquitous, and security has become distributed. It is vital to understand transaction flows and interactions between two or more points. Network isolation and micro-segmentation to more localized segments are some tactics to minimize lateral movement but they also allow for more granular controls over resource access.

Networking teams already understand the topology, content delivery, and quality of service through performance monitoring and optimization, but zero trust introduces more dynamic changes within network architecture where adjustments are necessary.

Endpoints and users do not access networks anymore. Still, they have direct connectivity to an individual service, application, or workload (this is the power of zero trust, as we can now shrink our attack surface significantly), so it is crucial to apply the following concepts:

- Adopt the security posture of "Default Deny"
- Avoid "trust zones"
- Session isolation
- Micro-segmentation

Visibility and Analytics

Gaining visibility into transactions between the components mentioned above with contextual detail and the ability to correlate and analyze them, is an absolute must. As a result, we can further understand the interaction, quality, and performance of a built ecosystem, enabling us to enhance and realize new fine-grained policies, thus the adoption of controls. Capabilities must be aligned to specific outcomes and purposes, such as helping with the speed of detection and response to threats where the IR team is the biggest consumer, focusing on threat hunting, forensic investigation, compliance activities, etc.

Mature zero trust programs must be able to:

- Inspect all traffic (deep packet inspection, looking beyond just network telemetry)
- Correlate data between multiple and distinct sources with security information and event management (SIEM)
- Identify anomalous behavior with user-environment behavior analytics (UEBA)
- Provide a holistic view of the environment

Automation and Orchestration

One of the significant challenges for many organizations today is the availability of quality resources. Security is one of the most impacted verticals, where capacity disadvantage takes its place. Individuals can't provide enough speed and scale to address such complexities within the ecosystem. Increasing complexity necessitates the use of automation.

Automation and orchestration bring unparalleled ability to deliver a more efficient and effective security program. It is all about the right process at the right time. With automation, organizations can speed up the identification and resolution of specific threats with a level of precision humans can't compete with.

Risk Scoring and Access Policy Definition

Determining access to resources, such as applications, services, or data, is managed by the application of controls that are defined through policies. These policies then enforce the access rules that are determined by the risk appetite of the organization. The policy definition, and consequently, which controls are applied, should be driven by a set of criteria that assesses each of the components discussed earlier.

Organizations can take two approaches:

- For each attribute, assess each possible implementation scenario and define a rule that will enable (or restrict) a level of access, and apply these cumulatively.
- Establish a risk model that applies a weighting to the implementation scenarios of all attributes and defines access policies based on the aggregate of that score.

For example, for approach one, in the case of unmanaged devices, the organization may decide that unmanaged devices can only get access to applications that process, store, or access data that is low in confidentiality classification and integrity rating. Furthermore, the user context can be included in this policy decision, e.g., an internal user coming from an unmanaged device may be able to access applications that process, store, or access data that is higher in confidentiality classification and integrity rating. Still, they cannot access the most critical applications or data.

Each permutation can drive a different policy definition, thus a different control set is applied.

Sample permutations are listed below, but the organization needs to document and assess this themselves so that it fits how the organization operates and aligns to their existing standards and practices:

- **User:** Internal permanent, internal contractor, third-party
- **Data Confidentiality rating:** Highly Confidential, Confidential, Private, Public
- **Data Integrity rating:** Very High, High, Medium, Low
- **Data Availability rating:** Highly Available, 0-4 hours, 4-24 hours, 24hours +
- **Endpoint:** Managed, Unmanaged
- **Application:** Critical, Important, Minor

As it relates to the concept of continuous assessment, throughout a user session, these components should be assessed and verified at all times. Should a change be noted, then action should be taken. Perhaps terminate the session, force re-authentication, or perform a set-up authentication.

An example may be that the session now appears to be originating from an unmanaged device, where it was previously thought to be a managed device. It could also be that the user is now trying to access data that is higher in confidentiality than what was initially assessed.

CONCLUSION

Most current security architectures were developed to address a technology ecosystem that is no longer relevant. A new mindset is required for new ways of operating and enabling your business. Security architecture has to focus on clearly understanding business risk, its context, and applying adaptive controls to address a new set of challenges while enabling users and businesses to move forward fast.

It is imperative to implement an appropriate balance between security, privacy, and user experience.

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything, visit netskope.com.