Since 1996
Prescient
Solutions

Definitive Guide to Zero Trust Security

GUIDE

Until recently, cities were built with strong defenses to protect against intruders; they were surrounded by a tall, thick stone wall with gates that could be securely locked. The townspeople inside the walls were trusted. Strangers outside who requested entry were challenged to show cause to admit them.

That same defensive model was applied to information security. The corporate network perimeter was fortified. Users inside the perimeter—employees, along with trusted vendors and partners—were readily granted access to resources. Security tools focused on detecting unauthorized attempts to breach the perimeter.

This traditional perimeter-based security model no longer adequately addresses cybersecurity challenges for several reasons:

1. Perimeters aren't well defined.
Cloud computing and "bring your own device" mobile policies make it difficult to distinguish between the "us" we trust and the "them" we're wary of. Data constantly moves between systems and users in different locations, and trusted users may use untrusted devices. In addition, cloud, distributed, and mobile computing models significantly increase the number of endpoints, making it more difficult to apply security controls consistently across the network.

2. Trusted partners may be compromised.
Assessing a partner as trusted only once and granting access privileges in perpetuity makes businesses vulnerable to threats from those partners. The SolarWinds Sunburst supply chain attack in late 2020 proved that: businesses trusted that downloads from their vendor's site were safe, but in fact the SolarWinds downloads had been corrupted by malware. More than 30,000 organizations were placed at risk.

3. Employees endanger assets, either deliberately or accidentally.
Trusting employees in perpetuity also makes businesses vulnerable. Employees with a grudge, with motivation to steal intellectual property, or simply with a propensity to make errors, can all put business data at risk. In addition, security incidents that expose login ids and passwords are common. Verizon's Data Breach Investigations Report found that more than 80% of attacks relied on misused credentials or network privileges. Current information security models, including use of virtual private networks, mean that once a malicious user has used credentials to breach the network, they're likely to have significant access to all the resources inside the so-called perimeter or trust zone.

There is no way to harden the perimeter enough to resolve these challenges. Instead, the solution is to recognize that there is no such thing as safety when it comes to information security and malware. Businesses need to operate in an environment in which each and every request for access by each and every user is examined each and every time.

That results in a Zero Trust approach to information security, and in fact Zero Trust security is now the cybersecurity solution recommended by the federal government. In addition to segmenting networks and restricting user permissions, Zero Trust means access privileges are never granted on an ongoing basis; each and every request is evaluated and assessed for risk each and every time.

Seven Principles of Zero Trust

The National Institute of Standards and Technology (NIST) has defined a standard (NIST 800-207) for Zero Trust that provides comprehensive guidance for organizations implementing this security model.

The NIST model proposes seven core tenets:

1. **All data sources and computing services are resources.**
2. **All communication is secured regardless of network location.**
3. **Access to resources is granted on a per-session basis.**
4. **Access to resources is granted by dynamic policy.**
5. **The enterprise monitors and measures the security and integrity of all assets.**
6. **Resource authentication and authorization is dynamic, and controls are enforced before access is granted.**
7. **The enterprise collects information about its assets, infrastructure, and communication, and seeks to improve its security posture.**

The net effect of the seven Zero Trust principles is that the default security position denies access to assets. Controls aligned with these tenets impose continuous verification that limits security impacts if a breach occurs. It also builds an ongoing process of hardening against security threats as additional information about threats, vulnerabilities, and normal usage patterns becomes available.

Zero Trust Benefits Every Organization

The Zero Trust approach to security suits IT infrastructure that heavily relies cloud-first architectures and remote employees, so nearly every organization will benefit from applying these principles.

Certain environments may gain the most benefit, including:

- hybrid and multi-cloud environments where data is frequently transferred between sites
- industries facing a high risk of ransomware, such as healthcare, education, utilities, and other public-facing services
- organizations vulnerable to supply chain attacks, particularly through processes that automatically receive data or application updates

Applying Zero Trust Principles

Making Zero Trust work requires understanding the context of all aspects of data and its usage. This context allows the creation of security policies that can be used continuously to authorize connections on demand. Policies must be enforced through constant monitoring and validation of access requests against the policy's requirements. In turn, this means there must be total real-time visibility into user and application attributes, including descriptive and behavioral data that allows access requests to be compared to normal usage patterns. Granting access is conditional, based on assessment of risk. When access is granted, the least privilege needed to satisfy the request is given. This limits the scope of any breach by limiting the attacker's access.

Zero Trust also requires the ability to rapidly and automatically detect, respond to, and resolve security incidents. There is a range of response actions that can include modifying or deleting access privileges for users, redesigning network segments, and other measures. Finally, data must be collected and analyzed to allow continuous improvement of security postures. Policies and practices can be adjusted to increase security and enable faster decisions.

Layers of Zero Trust Protection

In a Zero Trust environment, protection is extended across multiple layers, including identity, endpoints, applications, network, infrastructure, and data. Technology is used to evaluate every access request and grant it only if it satisfies current policies.

Implementing the Zero Trust framework requires deploying advanced technologies for authentication and identity protection, along with endpoint security, email security, and data encryption. It requires real-time analysis capabilities plus high levels of automation to distribute policies, patches, and other updates.

Zero Trust uses these tools to implement protections across multiple aspects of the organization's IT:

- **Identities:** Zero Trust requires strong authentication. User credentials must be tightly controlled and strongly authenticated using multi-factor authentication. Users are granted the least level of privilege required, and authentication periodically times out and the access rights are reassessed.

- **Endpoints:** Zero Trust requires visibility into all devices and their compliance status before granting access. Devices, even those connected to the corporate network through an approved provisioning process, are treated as potentially compromised.

- **Applications:** Zero Trust can prevent shadow IT usage and control access to applications through real-time analytics that monitor and limit user access. Workloads, particularly those in the cloud, need granular security monitoring and access management tailored to individual needs.

- **Data:** Zero Trust classifies and protects data through encryption and access restrictions rather than through perimeter boundaries. Data must be evaluated to identify the most sensitive data sets, understand data flows, and restrict access to legitimate business needs. Policies securing data must be consistently applied across the entire infrastructure, including desktops and servers, phones, tablets, and other devices, databases and applications, and clouds.

- **Infrastructure:** Zero Trust leverages telemetry data to detect abnormal behavior and other signs of attack. All levels of infrastructure including containers, microservices, and underlying operating systems and firmware layers must be examined.

- **Network:** Zero Trust eliminates the idea of a trusted internal network; it applies encryption, limits access, and uses microsegmentation to protect resources no matter where they reside. This prevents attackers from moving through the network and limits the impact of a breach.

IDENTITY

ENDPOINTS

APPLICATIONS

DATA

INFRASTRUCTURE

NETWORK

In addition to the controls at each level, Zero Trust requires a high level of automation.

Zero Trust Implementation Phases

A complete Zero Trust implementation touches nearly every aspect of an organization's IT security strategy.

Due to the extent and scope of this work, full implementation is likely to be a multi-year project passing through these phases:

1. Goal setting.
Create a vision for what Zero Trust means for the organization. Get management buy-in and commitment to see the project through to the end. Tie the project to business priorities, including agility, measurability, risk reduction, and accountability. Promote the business case by emphasizing benefits, including reduced risk, particularly in partner relationships; support for work-from-anywhere; reduced IT security costs through streamlining the security stack; and providing a more agile security and compliance response.

2. Analysis.
Identify resources, access points, and the associated risk exposures. Identify gaps in visibility, in identity management, and in other elements of Zero Trust.

3. Deploy Zero Trust technology.
Due to lengthy implementations, define sub-initiatives with specific timeframes and milestones and benefits that can be measured for each initiative. The sub-initiatives may be focused by IT aspect to protect (such as identity or network), by a Zero Trust tenet (such as collecting data and using analytics), or by the specific benefit desired.

4. Optimize protection to cover entire IT infrastructure and resources.
Evaluate progress toward implementation milestones. Determine appropriate threat detection thresholds to minimize false positives; integrate additional context from additional sources such as legacy and credential systems.

Zero Trust in Practice: Microsoft Azure Example

Fortunately, most businesses already have access to security tools that provide the capabilities required by Zero Trust, and deploying Zero Trust requires expanding and extending how the tools are utilized, rather than building a new Zero Trust security architecture from scratch.

For example, Microsoft 365 and Microsoft Azure have Zero Trust capabilities built in. Businesses that use these products can leverage those capabilities to gain Zero Trust's end-to-end visibility and protection without disrupting their end users.

In Microsoft Azure, the Zero Trust approach looks like the following:

- **Identity.** Azure Active Directory provides identity and conditional access controls. This capability extends beyond the Microsoft environment to other SaaS and on-premises applications. Using Azure AD enables strong authentication with multi-factor authentication across all applications. Azure AD provides support for conditional access though policies that assess risk levels (such as login from an unusual location or unusual time of day) and decide whether to grant or block access after satisfying additional authentication checks.

- **Endpoints.** Microsoft Endpoint Manager allows you to verify that all endpoints attempting to connect to your resources satisfy your security and compliance policies, even when you don't manage the endpoint (such as a mobile device). Extended Detection and Response management controls allow you to detect breaches on the endpoint and ensure the endpoint is returned to a trustworthy state before it can access resources.

- **Applications.** Microsoft Endpoint Manager can enforce policies on applications, including web browsers, enabling controls such as preventing the copying of data. Microsoft Cloud App Security can find and restrict Shadow IT usage as well as apply policies to control which data cloud applications can access and share.

- **Network.** Microsoft Azure supports network segmentation, with Azure Network Security Groups controlling access between networks, subnets, and the public internet. The Azure Firewall and Azure Web Application Firewall manage access to the network. All data is encrypted in transit, whether internal or across the firewall to the outside world. Azure DDoS Protection guards against DDoS attacks. Microsoft Defender and Azure Sentinel make it possible to detect and respond to an attack.

- **Infrastructure**. Azure Security Center and Log Analytics simplify infrastructure management to ensure that policies and controls are applied across all deployed systems and services.

- **Data.** Microsoft Purview Information Protection provides automated discovery, along with labeling data and associating policies with labels to automatically manage data in compliant ways, including encryption and preventing third-party app access.

Get Zero Trust Benefits with Support from Prescient Solutions

Implementing Zero Trust security offers a business many benefits, not strictly limited to improved security.

These benefits include:

- reduced risk
- increased support for remote work
- reduced security costs through a streamlined security stack
- more agile security and compliance response
- improved network performance due to reduced traffic on subnets
- faster network problem resolution due to enhanced logging
- reduced manual effort due to high levels of automation

Achieving the benefits by implementing Zero Trust takes time. There is no one-time replacement of existing infrastructure. Instead, there is an ongoing series of incremental changes to implement Zero Trust principles through process changes and new technology. These changes take time to spread throughout the entire organization.

Prescient Solutions, a Microsoft Gold Partner with certified expertise in cybersecurity, assists clients through each phase of the Zero Trust process, from analysis through deployment. Prescient Solutions supports blended Zero Trust/conventional security infrastructure until the complete set of assets is protected by the Zero Trust solution.

Contact Prescient Solutions to learn more about Zero Trust and why you should trust Prescient Solutions to implement a cost-effective, highly protective information security solution for your business.

Prescient Headquarters
1515 Woodfield Rd, Suite 880
Schaumburg, IL 60173
Phone: (847) 240-3900

About Prescient Solutions

Prescient Solutions has been providing managed services both on site and remotely to small, medium and large enterprises and government agencies for over 25 years. With certifications in key technologies spanning hardware, software, network, security, and other specializations, our team has the insight and experience to address the technical challenges that are holding back your IT team and your business. For more information about Prescient Solutions, or to request a complimentary IT consultation, all 888-343-6040, or visit www.PrescientSolutions.com.