Whitepaper

Implementing a Zero Trust Security Framework

Introduction

With the proliferation of distributed IT environments and the Internet of Things (IoT), organizations can no longer simply secure their digital perimeters — a clearly delineated perimeter often no longer exists. While IT environments had already grown increasingly complex, the recent and rapid expansion of endpoints and networks enabling new work models has resulted in a complex ecosystem that's difficult to secure.

Outdated approaches to security assumed that anything within the corporate network could be trusted. This is simply no longer true, due to factors including:


The need for remote access


Bring Your Own Device (BYOD)


IoT


Multi- and hybrid cloud approaches


Increased collaboration


The need for business resilience

Increased complexity in organizations' IT infrastructure has created an increased attack surface with gaps in visibility and multiple disparate point solutions that make managing security an unwieldy task. As a result of this expanded edge, security protocols are seeing a necessary shift from location to identity as the trust broker.

Network access control comprising identity-based permissions and IT access is a critical component to a reliable approach to security. The Zero Trust framework, built on the principles of least privilege and — as its name suggests — zero implicit trust, is an approach organizations can take to methodically and comprehensively integrate identity-based access policies across the entire business or operations based on their unique requirements.

Insight Cloud + Data Center Transformation (CDCT) is helping organizations of all sizes strengthen their security postures and protect their users, data, and endpoints leveraging Zero Trust methodology and our partnerships with leading providers of security technologies. This whitepaper is intended to help organizations interested in adopting a Zero Trust methodology understand the necessity and benefits of such an approach and the strategic and technical support available from Insight to assist in identifying and implementing appropriate solutions.

Zero Trust: The answer for ever-expanding perimeters

The basic tenets of Zero Trust

The Zero Trust methodology lays the groundwork for a highly defensible IT environment, considering all endpoints to be untrusted until proven otherwise — requiring identity verification, among other factors, to elevate trust and provide access to networks and resources accordingly. These key modes of operation are necessitated by the basic principles that trust is not binary or permanent, and that operations must be performed in a zero-trusting way to maintain the highest level of security.

A Zero Trust approach:

Establishes trust in every access request, regardless of where it comes from

Secures access across all applications and networks

Extends trust to support a modern enterprise across the distributed network

In addition to better access security, a Zero Trust approach also supports modern enterprise models with BYOD, cloud apps, hybrid cloud/on-premises environments, and more.

To simplify the Zero Trust conversation, the implementation of appropriate security solutions is broken down into three main areas of application: the workforce, workloads, and the workplace.

Workforce

Users and devices accessing enterprise applications

Workloads

Applications, services, microservices, etc., accessing databases, servers, etc.

Workplace

IoT devices, endpoints, and control systems accessing the network

Workforce

The first area to address in the Zero Trust framework is the workforce. The workforce is made up of enterprise users and the devices from which they access enterprise applications, whether in the cloud or in physical data centers. Zero Trust principles applied to the workforce ensure that only verified users and secured devices can access enterprise applications.

There are three key components to minimizing your attack surface by verifying trust: improving device visibility, assessing device security posture, and enabling continuous risk assessment. With these capabilities enabled, organizations can protect their data while delivering seamless access to critical applications and networks across their workforce.

The right secure access solutions will allow your organization to:

- Verify user identities with Multi-Factor Authentication (MFA)
- Gain device visibility and establish trust
- Enforce access policies with adaptive access controls

Workloads

The next facet of the enterprise environment addressed in a Zero Trust discussion is its workloads. Zero Trust security for workloads means verifying trust for your applications, services, and microservices communicating with databases, containers, and servers across your enterprise environment — whether on-premises, in the cloud, or across hybrid infrastructures.

Effective technologies for securing your workloads should reduce risk with minimal burden to your IT resources with features that allow you to:

- Gain visibility across your environment
- Identify individual workloads
- Program and enforce policies
- Contain breaches
- Maintain compliance
- Continuously monitor activity
- Automatically respond to compromises

Workplace

Finally, Zero Trust protocols should also encompass the workplace, focusing on secure access for any and all endpoints and IoT devices connecting to the enterprise network, from guest laptops to badge scanners and point-of-sale devices. Specific access protocols must be in place, as many of the devices within the workplace will require access to the same applications and workloads as your users, but will not require — and should not have — full network access.

Implementing appropriate network security solutions enables users to securely connect to enterprise networks while restricting access from non-compliant devices. The secure network access solutions you choose should enable you to:

- Grant the appropriate level of network access to users and devices with network authentication and authorization
- Classify and segment users, devices, and applications
- Contain infected endpoints
- Revoke network access as needed

Implementing Zero Trust with Insight

Industry-leading solutions and support services from Insight and our partners make it possible to start implementing Zero Trust methodologies at any stage of security strategy development. And there are benefits to taking this approach, even beyond the crucial component of stronger security. With a stronger security environment and unified security solutions, organizations can benefit from more efficient operations, improved security costs, and a more user-friendly and streamlined technology environment.

Operations

One of the key issues with a traditional approach to security is complexity. Zero Trust can provide IT and security teams with control and visibility over users, devices, access level, and ongoing activity. When understood and implemented correctly, Zero Trust reduces both complexity and resource fatigue — two main factors in risk to operations.

Finance

Adopting a Zero Trust approach may seem daunting due to perceptions around the cost to rearchitect and design. However, organizations can see long-term benefits through the reduction of point solutions, centralized security policy management, and the use of behavioral analytics to assist in the constant evaluation of user and device risk to the business. Zero Trust provides a focused security solution environment and reduced resource activity to manage the constant barrage of alerts and potential incidents that security professionals deal with daily.

Technology

One of the most important aspects of a well-architected Zero Trust framework is simple, centralized policy management. The more complex an environment is, the more likely it is to have gaps that introduce risk. Ideally, technologies supporting Zero Trust should deliver integrations that streamline the IT environment, support Machine Learning (ML) and user behavior analytics, offer continuous activity monitoring, and allow for automated remediation measures.[1]

Summary

As an organization with deep industry partnerships with world-class OEMs and solution providers, Insight is pleased to help clients evaluate and implement best-fit security solutions based on their unique organizational needs to create a Zero Trust environment with innovative, comprehensive, and user-friendly technologies.

A Zero Trust approach enabled and supported by Insight's professional resources allows organizations to:

- Prevent data breaches before they happen by enabling policy-based controls for every access attempt to enterprise applications, workloads, and networks
- Gain visibility into who and what is accessing applications, workloads, and the network to identify risks and indicators of a breach of trust
- Reduce the overall attack surface, contain breaches, and stop lateral movement by enforcing granular controls and segmenting networks and workloads

Many organizations are beginning to see the necessity of a Zero Trust approach yet struggle with where and how to begin implementation. Insight's goal is to support our clients, joining them at any stage of their security strategy evolution and working with them to identify best-fit solutions and next steps in accordance with a Zero Trust framework and organizational needs. Insight CDCT empowers that effort through vendor partnerships and professional services delivery, providing organizations with all the components of a comprehensive, effective security approach to create optimal client outcomes.

For more information on how to implement a Zero Trust methodology as part of your organization's security strategy, contact us at: insightCDCT.com/contact-us

---

1 Rowell, E. (2021, March 5). Zero Trust: What's Driving Its Adoption in Enterprise Environments? Insight.

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com