Simplifying Zero Trust with Cisco Secure

Abstract

With the proliferation of distributed IT environments and the Internet of Things (IoT), organizations can no longer simply secure their digital perimeters, as 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. 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.

Together, Insight and Cisco are helping organizations of all sizes strengthen their security posture and protect their users, data, and endpoints using the Zero Trust methodology and Cisco's portfolio of Zero Trust security solutions. This whitepaper is intended to help organizations interested in adopting a Zero Trust methodology understand the necessity and benefits of such an approach, the Cisco® solutions available to accomplish a Zero Trust environment, and the strategic and technical support available from Insight to assist in identifying and implementing these solutions.

Problem statement

Outdated approaches to security assumed that anything within the corporate network could be trusted.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, and the necessity of 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.

Background

Cisco and Insight are leaders in helping clients secure their networks and other IT infrastructures. For more than 20 years, Insight's team of experienced IT professionals has played an integral role in identifying, delivering, and supporting innovative Cisco solutions for transformative outcomes for clients worldwide.

As a long-standing Cisco partner, Insight is pleased to recommend the Cisco security portfolio to many of our clients seeking to implement a Zero Trust methodology, thanks to its innovative, comprehensive, and user-friendly offerings.

Cisco has developed a strong approach to Zero Trust that builds in automation, reporting, logging, visibility, and analytics to meet known client and market challenges. In fact, Cisco is leading the industry in Zero Trust solutions, having consistently been part of the Forrester Wave™ for the past three years.

In "The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers," Forrester states, "Organizations that have a well-constructed security apparatus in place and are moving to a more mobile workforce should consider bolstering those capabilities with the ease of use Cisco now provides."[1]

Cisco's delivery of Zero Trust solutions enables clients to begin with their current-state environment wherever they are on the path to achieving a comprehensive Zero Trust architecture, aligning with Insight's methodology of joining clients at any stage of the IT modernization journey to visualize end-state goals and deliver strategic and technical support for every next step.

Solution

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** Ensure only the right users and secure devices can access applications	 **Workloads** Secure all connections within your apps, across multicloud	 **Workplace** Secure all user and device connections across your network, including IoT
Who or what	People & their devices (laptop, mobile, tablet)	Apps, services, microservices	IT endpoints & servers, IoT devices, Industrial Control Systems (ICS)
Trust verification	Accessing applications	Communicating with other systems	Accessing the network
From	Anywhere	On-premises, hybrid cloud, public cloud	On-premises, hybrid cloud, public cloud

Workforce

The first area to address in the Zero Trust framework is the workforce. The workforce is made up of the enterprise's 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.

Cisco Secure Access delivers three critical capabilities to help organizations minimize their attack surface by verifying trust: improving device visibility, assessing device security posture, and enabling continuous risk assessment.[2] With these capabilities enabled, organizations can protect their data while delivering seamless access to critical applications and networks across their workforce.

Organizations leveraging Cisco Secure Access can easily, efficiently, and cost-effectively:

- Verify users' identities with Multi-Factor Authentication (MFA)
- Gain device visibility and establish trust with endpoint health and management status
- Enforce access policies for every app with adaptive and role-based access controls[3]

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.

Cisco Secure Workload, formerly Tetration®, allows clients to automate and implement a secure model for microsegmentation based on application behavior and telemetry, creating a proactive security environment that can detect and remediate suspicious or compromising activity automatically.[4]

With Secure Workload, organizations are empowered to reduce risk with minimal burden to internal resources by:

- Gaining visibility by identifying workloads and enforcing policies
- Containing breaches and maintaining compliance
- Continuously monitoring and responding to indicators of compromise[5]

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 do not require — and should not have — full network access.

Implementing appropriate network security solutions from Cisco (spanning offerings including Cisco Secure Firewall, Cisco Secure Network Analytics, Cisco Identity Services Engine (ISE), and Cisco Software-Defined Access (SD-Access) from Cisco DNA™) enables users to securely connect to enterprise networks while restricting access from non-compliant devices. With secure network access solutions from Cisco, organizations are empowered to simply:

- Grant the right level of network access to users and devices with network authentication and authorization
- Dynamically classify and segment users, devices, and applications on the network
- Contain infected endpoints and revoke network access by continuously monitoring and responding to threats[6]

To achieve the most thorough Zero Trust environment possible, certain organizations may find, depending on their requirements, that additional Cisco Secure solutions such as Secure Endpoint (formerly AMP for Endpoints), Secure Network Analytics (formerly StealthWatch®), and Cisco Umbrella® — an offering for flexible, unified, cloud-delivered security — can aid in filling out a holistic Zero Trust approach.

The benefits of Zero Trust with Cisco and Insight

Industry-leading solutions from Cisco and support services from Insight 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.[7]

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.[8]

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. Cisco technologies supporting Zero Trust 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.[9]

Conclusion

In summary, a Zero Trust approach enabled with Cisco Secure solutions 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, or 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. Cisco Secure's Zero Trust portfolio empowers that effort, delivering the components of a comprehensive security approach and helping us create optimal client outcomes together.

References

[1] The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2020, September 24, 2020.
[2] Duo. (2020). The Essential Guide to Device Trust in the Enterprise. Duo.com.
[3] Cisco Zero Trust Solution Overview. (2019, Aug. 5). Cisco.com.
[4] Cisco Secure Workload – Tetration. Cisco.
[5] Cisco Zero Trust Solution Overview. (2019, Aug. 5). Cisco.com.
[6] Cisco Zero Trust Solution Overview. (2019, Aug. 5). Cisco.com.
[7] Rowell, E. (2021, March 5). Zero Trust: What's Driving Its Adoption in Enterprise Environments? Insight.
[8] Rowell, E. (2021, March 5). Zero Trust: What's Driving Its Adoption in Enterprise Environments? Insight.
[9] Rowell, E. (2021, March 5). Zero Trust: What's Driving Its Adoption in Enterprise Environments? Insight.