Zero Trust

Fairfield, NJ | New York, NY | Shrewsbury, NJ | Boston, MA | Chicago, IL

Table of Contents

Introduction

The explosion of cloud computing, mobile device usage, and the Internet of Things (IoT) have blurred traditional network boundaries. Perimeter defenses were once effective, but the increase in remote workforces and sophisticated Cyberattacks, such as ransomware, phishing, and advanced persistent threats (APTs), has made them less reliable.

To safeguard a modern digital enterprise, organizations need a comprehensive strategy for secure "anytime, anywhere" access to their corporate resources (e.g., applications, legacy systems, data, and devices) regardless of where they are located.

Although adopting Zero Trust Architecture, though is not mandatory, has become essential in light of the growing sophistication of data breaches and security threats. Skilled Cybercriminals are increasingly using Artificial Intelligence (AI) to bypass traditional security measures and exploit human vulnerabilities, making the need for Zero Trust even more critical.

This white paper provides valuable insights and expert analysis on a new security approach known as Zero Trust. This approach focuses on continuous verification and enforcement of least privilege access, and it is gaining traction. The benefits of implementing Zero Trust architecture include improved security posture, reduced risk of data breaches, and enhanced compliance.

History

The term "Zero Trust" was coined by Forrester Research analyst John Kindervag in 2010. Kindervag's new Cybersecurity strategy assumes that no user or device is inherently trustworthy, as opposed to the widely accepted concept of "trust but verify". This shift reflects the changing threat landscape, where breaches can come from within the network, often through compromised accounts or malware. Since its introduction, Zero Trust has evolved from a specialized idea into a widely adopted security approach, especially as Cyber threats have become more complex (see Figure 1.0).

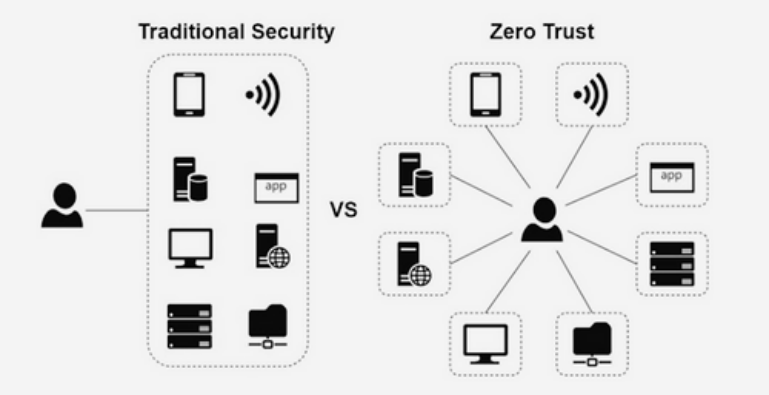

Figure 1.0 – Traditional Security vs. Zero Trust Security

What is it?

Microsoft defines Zero Trust Architecture (ZTA) as an approach to security that assumes a breach and verifies each request as though it originates from an open network. Instead of trusting everything behind the corporate firewall, Zero Trust teaches us to “never trust, always verify.”

Implementation of zero trust requires every access request to be fully authenticated, authorized, and encrypted based on the user’s role, location, and device before access is granted.

Micro-segmentation involves dividing the network into smaller, isolated segments, and least-privilege access principles, which restrict user permissions to only what is necessary, are applied to minimize lateral movements. Rich intelligence and analytics detect and respond to anomalies in real-time.

In an ideal zero-trust environment, the following is required:

- User Identities are verified and secured with multifactor authentication (MFA) MFA requires users to provide a combination of two or more pieces of evidence, or “factors”, to verify their identity. MFA factors consist of knowledge (something you know) and ownership (something you have). Examples of MFA include but are not limited to, one-time passwords (OTP), hard tokens, fingerprints, and facial recognition. The added use of biometrics enables strong authentication for user-backed identities
- Devices are managed and verified as healthy and secure. Device health validation is mandatory. All device types and operating systems must adhere to a minimum health state as a condition of access to any organizational resource (see Figure 2.0)
- Least privilege access is enforced. Limit access to only the applications, services, and infrastructure required to perform a particular job function. The use of Identity and Access Management (IAM) tools can help automate this process. Broad access solutions that lack segmentation must be removed

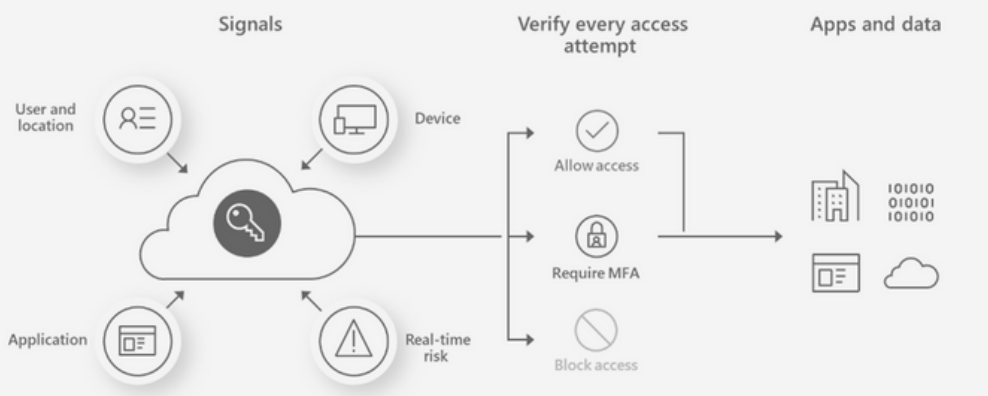

Figure 2.0 – Zero Trust Verification

Challenges

Implementing Zero trust architecture may also present several challenges for organizations, including, but not limited to:

- **Costs:** Implementing Zero Trust architecture requires additional manpower and changes to existing network infrastructure, which can be expensive. The associated costs of purchasing new tools and hiring additional employees may only be feasible for some organizations, particularly larger ones
- **Slows Application Performance:** Since every user, device, and application must be authenticated and authorized before receiving access to data or applications, there are many complaints about slowed application performance
- **Cultural Resistance:** Employees and management may view the increased security measures as obstacles to productivity. Implementing zero-trust architecture also requires a cultural shift in mindset
- **Complexity:** Evolving interdependencies and complexities of security control systems may pose challenges for IT departments to manage
- **Legacy Systems:** Outdated infrastructure may not be poised to integrate with zero-trust systems
- **Supply Chain:** Authentication and authorization of every third-party user within the digital supply chain may be difficult and not feasible

Overcoming Challenges

- To manage costs, organizations can implement Zero Trust in phases, starting with critical areas and gradually expanding
- To address performance concerns, invest in optimized security tools and regularly monitor their impact on system performance
- Cultural resistance can be mitigated by engaging employees early, providing training, and clearly communicating the benefits of Zero Trust
- For legacy systems, consider hybrid solutions that integrate Zero Trust principles where possible while planning for longer-term infrastructure upgrades

How to Get Started - A Roadmap

The following zero-trust guidelines can help organizations implement a zero-trust Cybersecurity framework:

1. Continuously Define and Refine the Attack Surface: Defining the attack surface requires focusing on the areas organizations need to safeguard. To do this, they must conduct a crown jewel assessment to identify their most critical digital assets that require the highest level of security

How to Get Started - A Roadmap

The four most prominent areas at risk of attack:

- **Sensitive Data:** Customer and employee data that includes personally identifiable information (PII), such as social security numbers, addresses, phone numbers, etc.
- **Critical Applications:** Applications that are required to support the organization's most crucial business processes
- **Physical Assets:** The growing number of Internet of Things (IoT) connected devices (e.g., laptops, HVAC, physical access solutions) continues to create a larger surface area for hackers to exploit vulnerabilities
- **Corporate Services:** Elements of the organization's infrastructure used to support the day-to-day operations of employees

2. Implement Controls Around Network Traffic: The flow of traffic in an organization's network varies depending on the dependencies of each system being used. For example, several systems may need access to a database holding customer, product, or service information. Requests don't simply "go into the system"; instead, they are redirected through a database that stores sensitive data and architecture. Understanding these details will help organizations determine which network controls to deploy and where to place them. Technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and AI-driven anomaly detection can be crucial for monitoring and controlling network traffic.

3. Architect a Zero-Trust Network: Zero-trust networks are designed around the organization's specific protection surface. There will never be a one-size-fits-all solution. Implementing a next-generation firewall (NGFW) is typically a good starting point. This tool helps in segmenting areas of the network. Segmentation is essential because it can prevent Cyber-attacks from spreading across a network and into unprotected devices. It can also limit how far an attack can spread and stop harmful traffic from reaching vulnerable devices. For example, if a network is segmented, attackers can only access the initial section they breach, giving IT time to respond.

Additionally, introducing multi-factor authentication (MFA) will be critical in ensuring that users are thoroughly vetted prior to obtaining access to organizational data and assets.

4. Create a Zero Trust Policy: Zero trust policies aim to prevent unauthorized access and make access control as granular as possible. Zero Trust policies should be designed around key principles such as:

- Who is trying to access the resource?
- What are they trying to access?
- When is the request occurring?
- Where is the user and resource located?
- Why is the data being accessed?
- How should access be provided?

How to Get Started - A Roadmap

Examples of zero trust policies include, but are not limited to:

- Strong user IDs
- Verified device IDs
- Identifying which application is being used to access a protected resource
- Being sensitive to the time at which a connection occurs

Network Access Control (NAC) systems can be used to help implement these policies by segmenting the company network and its most sensitive assets.

5. Monitor Your Network: Implementing continuous monitoring tools will help organizations take swift actions in response to potential intruders or nefarious activities. Monitoring the network provides valuable insights for optimizing network performance – without compromising security.

Conclusion

Adopting a Zero-Trust architecture is not just a technical task, but a strategic necessity in today's Cyber threat landscape. The shift to a Zero-Trust model requires organizations to transform their approach to security—moving from a perimeter-based strategy to one that assumes a breach and continually verifies every access request.

The urgency to adopt Zero Trust has never been greater as Cyber threats become more advanced, and the attack surface continues to expand with the proliferation of remote work, IoT, and cloud computing. The 2023 Verizon Data Breach Investigations Report highlighted that human error accounts for 74% of data breaches, emphasizing that Cybersecurity is only as strong as its weakest link.

To protect your organization's most valuable assets, it's crucial to start your Zero Trust journey now. Begin by assessing your current security posture, identifying critical assets, and implementing Zero Trust principles in phases. By prioritizing this transition and promoting a culture of continuous security awareness, your organization can stay ahead of emerging threats and build a resilient defense against future attacks.

The time to act is now—adopt Zero Trust and safeguard your digital enterprise against the ever-evolving Cyber threat landscape.

Who We Are

Founded in 2001, DLA is a specialized boutique financial advisory firm that provides customized services and solutions to optimize businesses' financial, operational, IT, and Cyber processes, while minimizing risk and driving growth and innovation. With advanced expertise that spans accounting advisory, internal audit and forensic accounting, valuation, litigation, and post-closing dispute support as well as risk and IT and Cyber advisory, our team of accounting, finance, and technology professionals provide creative strategies that address your most pressing priorities and challenges. DLA is headquartered in Fairfield, New Jersey, with offices in Shrewsbury, New Jersey, Boston, Chicago, and New York City.

About DLA, LLC

Founded in 2001, DLA LLC is an accounting advisory and capital markets organization focused on a comprehensive internal audit, accounting advisory, and corporate finance choice for employees, the office of the CFO, audit committees, and public accounting firms and law firms on behalf of their clients. DLA LLC is headquartered in Fairfield, New Jersey, with offices in Shrewsbury, New Jersey, Boston, Chicago, and New York City.

dla@dlallc.com | 973-575-1565 | www.dlallc.com