FORTRA

Vulnerability Management: The Backbone of a Zero Trust Strategy

Introduction

Zero Trust is more than just the latest security buzzword being bantered around. It is a massive paradigm shift in how organizations approach security. With 94% of organizations using cloud computing of some variety and remote work still being common, data has moved well outside the traditional security perimeter, so security strategies must evolve.

The government has embraced the effectiveness of Zero Trust for securing data through the adoption of a Federal Zero Trust Strategy. This strategy builds upon President Biden's executive memo on improving the nation's cybersecurity to clarify how organizations should implement Zero Trust. Zero Trust as the de facto security implementation strategy is on the rise across all industries. Recent studies have found that 96% of security decision-makers believe that the adoption of Zero Trust is critical to their organization's success.

With Zero Trust, risk of unauthorized access is virtually eliminated through authenticating, authorizing, and encrypting all access and requests, in conjunction with intelligent network microsegementation to limit lateral movement.

*96% of security decision-makers believe that the adoption of Zero Trust is **critical** to their organization's success[1].*

What is Zero Trust

Zero Trust trusts no 'one' and leverages multiple authentication criteria to protect and secure data and productivity. It represents a paradigm shift required to protect today's hybrid architecture. Zero Trust security is built on these tenets:

- Assume breach
- Trust no one
- Verify everything

Zero Trust has no trusted users or assets, and everything is checked and verified before access is granted. Even when access is given, it only persists for a time before it is automatically revoked, eliminating the risks of permissions existing beyond their needed time.

While Zero Trust is built on a solid foundation of access management controls, these controls are only helpful if the platforms they run on and against are trustworthy. If attackers can exploit vulnerabilities to gain access by circumventing controls, the solution is no longer effective. To ensure that Zero Trust remains relevant, organizations need an effective vulnerability management process to identify, prioritize, and remediate vulnerabilities before attackers can leverage them and bypass the Zero Trust security architecture.

The Importance of Zero Trust

Zero Trust is increasingly important for a number of reasons. With the increase in remote work and cloud computing, confidential and regulated information is no longer just on-site but spread across numerous locations.

Keeping this data safe requires a new approach to data security. Insider Threats continue to grow, up 47% over the last two years. Organizations can no longer hide behind traditional firewalls and other perimeter defenses and assume that they are secure. In a traditional implementation, assets with access or that exist inside the perimeter are implicitly trusted.

Unfortunately, if the initial line of defense is breached, the assets on the inside are effectively defenseless, permitting attackers to rapidly pivot between resources, steal data, and take over systems free of impediments. Having Zero Trust in place reduces the impact of attacks by limiting what cybercriminals have access to, even if they gain access to your infrastructure.

Zero Trust Mindset

Zero Trust requires a fundamental shift in how organizations view their security posture. Rather than focusing on keeping cybercriminals out of their organization, they need to assume attackers are already in the network. The key focus is to limit access and loss.

By taking an "assume breach" approach, organizations focus their security control design on protecting the data and resources. This approach requires access management, monitoring, and system management working in unison. Rather than granting access based on prior verification, authentication and authorization are required to validate every request and to ensure it remains within reasonable risk levels for the requestor.

Components of Zero Trust

Adopting Zero Trust requires a collective set of solutions to provide security controls ranging from access management to monitoring and threat detection. Each component offers part of the Zero Trust architecture, creating an in-depth defense throughout the organization that applies to resources, no matter where they reside.

Essential components of Zero Trust include:

- **Identity Management** - Verifies that users are who they say they are and not someone else masquerading as them.
- **Policy Analysis** - This component analyzes access requests against the defined organizational policies and compliance rules to determine if the risk level of the request falls within reasonable levels for automatic approval.
- **Access Management** - Works with policy analysis component to automatically grant access requests of acceptable risk and remove them after a specified period.
- **Monitoring and Threat Detection** - Analyzes access requests and network behavior for abnormal usage and high-risk behavior. This works with the access management component to drive alerts and block access for accounts exhibiting risky behavior.
- **Vulnerability Management** - This software scans and analyzes existing infrastructure for vulnerabilities in software and implementation that attackers could utilize to bypass security controls. This must be part of a vulnerability management process to categorize, prioritize, and remediate vulnerabilities effectively.

Vulnerability Management is the Cornerstone of Zero Trust

Zero Trust cannot exist without vulnerability management. It is crucial for creating a hardened environment in which to implement a Zero Trust. Without building this foundation, the controls that support Zero Trust are no longer reliable, and the premise of Zero Trust is defeated.

Trust is a Vulnerability

It is important to remember that anytime an entity is trusted and granted access to a resource, it creates an inherent vulnerability. There is always the risk that the entity is not who they claim to be, such as through stolen credentials, or that they may be a legitimate user, but they may misuse the access they are granted. This includes both malicious and accidental misuse, such as accidentally deleting a file or making an unwarranted edit; this action can impact others in the organization.

While granting no access and trusting no one results in perfectly hardened security, it also prevents anyone from productively working. Organizations have to balance their security and productivity needs. Zero Trust is intended to help balance this vulnerability by only granting access for short periods and then re-assessing whether the access is still appropriate when requested in the future.

"Zero Trust cannot exist without vulnerability management. It is crucial for creating a hardened environment in which to implement a Zero Trust strategy. "

Building Foundations

Vulnerability management focuses on the infrastructure side of vulnerabilities rather than those resulting from access. These vulnerabilities are equally critical as they help build the foundation for a secure enterprise where Zero Trust will operate. It identifies failures in patching and configuration that cybercriminals can leverage to gain access or escalate privileges. Access checks and the trust-but-verify approach may be circumvented if systems or applications have vulnerabilities that bypass authentication.

By leveraging vulnerability management, organizations identify vulnerabilities in servers and endpoints before cybercriminals. Since time is a limited resource, organizations must prioritize the vulnerabilities and address the highest risk ones first. This helps to manage defenders' time more efficiently while blocking the most likely flaws attackers would otherwise use to get in.

Vulnerabilities in Controls

Vulnerabilities do not only live in endpoints and servers. Even the security controls that help to protect the organization can have vulnerabilities. If these control systems are compromised, such as an access management solution, the control is no longer viable, and Zero Trust breaks. Zero Trust is only as reliable as the systems that provide the controls to operate it. Vulnerabilities in the core infrastructure undercut the design foundation of Zero Trust.

To avoid this happening, vulnerabilities related to any of the core aspects of Zero Trust need to receive expedited attention. When prioritizing identified vulnerabilities, this should be factored into the risk adding additional weight and preference for these vulnerabilities over others.

Vulnerability Scanning for Zero Trust

Many choices exist when selecting a vulnerability management solution, and not all of them are made equally. Determining the right-fit solution for your organization requires more than just picking the first option discovered. When assessing options, you need to consider your organization's overall architecture and needs.

Most modern organizations will require a flexible solution to handle their hybrid infrastructure without excessive configuration and deliver quality results. Quality results go beyond the findings and include reporting that provides valuable insights that staff can ingest and use to remediate.

Flexible Delivery

Most organizations considering a Zero Trust architecture often use a hybrid IT architecture of on-premise, cloud solutions, and remote systems. To effectively scan this mix of assets, it takes a combination of agentless and agent-based scanners. Each type of scanner has advantages and disadvantages as they fulfill different needs.

Agent-based Scanning

This type of scanning is vital for remote workforces and dynamic environments such as the cloud, where the ephemeral nature of assets would require constant discovery by agentless scanning. Agent-based scanning does not create excessive network traffic and allows for in-depth assessment of even BYOD devices. Agent-based scanning does have limitations in that the agents are not designed for every system, so it may not include some devices such as routers, switches, and firewalls.

Agentless Scanning

This type of scanning does not require anything installed on an endpoint but instead uses discovery to identify network-connected assets. Because nothing is installed, it is device agnostic and can assess almost any device on the network. The challenges of agentless scanning are most specific to remote assets, as discovery becomes complex. For remote users, if they are not connected to a VPN at the time of the scan, scanners will miss their device.

There will be blind spots for vulnerability scanning that only utilizes one variation of scanning. Lack of complete visibility will result in unknown and unmanaged vulnerabilities. When considering a Zero Trust architecture, this can be a critical problem that could undermine overall security for the organization. A vulnerability scanner should offer both agent-based and agentless scanning for the best coverage.

Quality of Identification

As with scanning methods, accuracy of results is crucial to further success of a security program. False positive and false negative test results will undermine the efficacy of an organization's vulnerability management program. Unreliable testing and missing checks can muddy a security practitioner's understanding of flaws on a device. Further, inflexible data management and reporting will hinder the ability for defenders to efficiently address critical issues.

Having a wide breadth of accurate data is crucial for hardening security as attackers also use vulnerability scanning. Knowing the types of results an attacker will see helps to keep one step ahead of threat and plan appropriate mitigation.

Actionable Reporting

Zero Trust requires a fundamental shift in how organizations view their security posture. Rather than focusing on keeping cybercriminals out of their organization, they need to assume attackers are already in the network. The key focus is to limit access and loss.

By taking an "assume breach" approach, organizations focus their security control design on protecting the data and resources. This approach requires access management, monitoring, and system management working in unison. Rather than granting access based on prior verification, authentication and authorization are required to validate every request and to ensure it remains within reasonable risk levels for the requestor.

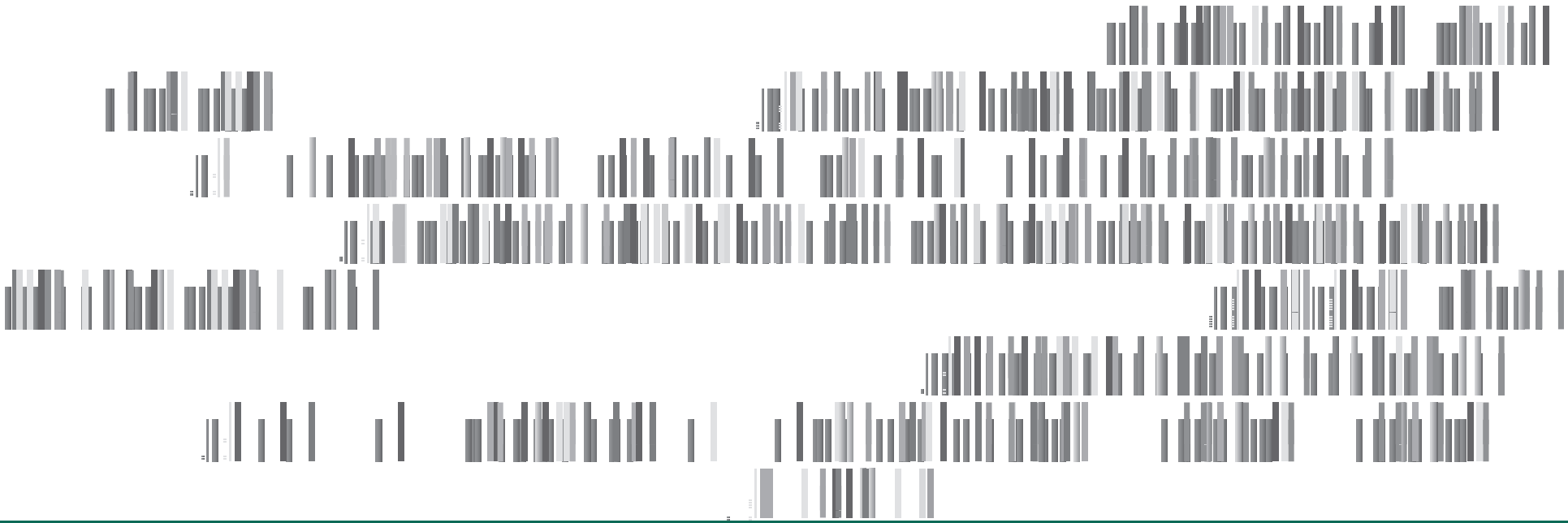
The Right Security Partner

The vulnerability management vendor you choose must meet all of the aforementioned needs, providing a scalable, easy to use, and highly accurate solution that will kickstart your team's Zero Trust Strategy.

Frontline Vulnerability Manager is designed to provide fast, high quality improvement in your network security, so you can build your Zero Trust program on a solid foundation.

Learn more and request a free trial.

[1] Microsoft 2021 Zero Trust Adoption Report



About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-be-gd-1022-r1-79d