AIRGAP

AIRGAP INSIGHT

Modern Zero Trust Segmentation?

5 Steps to Implementation

While establishing a Zero Trust Architecture can enhance security, many organizations find the implementation challenging given the multitude of offerings available.

The zero trust security model requires that all identities, devices, and applications connected to any organization's network are continuously authenticated, authorized, and monitored to ensure adaptive policy configurations and security posture before granting any access to networks and data, regardless of where they are on-site or remote.

As more companies migrate to the cloud and SaaS, the way that companies protect data must change as well. In a traditional on-premises network architecture, companies were able to follow the "trust but verify" philosophy. However, protecting cloud data needs to take the "never trust always verify" approach. Understanding what a complete Zero Trust Architecture is and how to implement one is the first step.

Basic Tenets of Zero Trust

According to the National Institute of Standards and Technology Special Publication (NIST SP) 800-207, the basic tenants of a Zero Trust architecture include:

- All data sources and computing services are considered resources
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

The path to zero trust is an incremental process and a fundamental shift that can be accomplished in minutes not months or years. Key considerations include:

- Thinking agentless given its minimal footprint and efficiency
- Assuming breaches will occur
- Assuming an enterprise-owned environment is no different or more trustworthy than non-enterprise-owned environments
- Continuously analyzing and evaluating risk
- Continuously enacting risk mitigation protections
- Minimizing user and asset access to resources
- Continually authenticating and authorizing identity and security for each "just-in-time" access request

Zero Trust directives also generally cover the following security implementations:

- **Enhanced identity governance.** Identity governance is the process of managing the identity lifecycle from the time you first grant a user or entity access to any resource until you terminate that access. Enhanced identity governance includes restricting network access according to the principle of least privilege and requiring multi-factor authentication (MFA).
- **Micro-segmentation.** Micro-segmentation is the process of protecting resources, either in groups or individually, by placing them on a unique network segment using a switch, firewall, or another gateway device. Although this approach incorporates identity governance, it also relies on network devices to prevent unauthorized access. When using micro-segmentation to protect data, organizations need to ensure that the devices can respond to threats or changes in workflow.
- **Network infrastructure and software-defined perimeters (SDP).** An SDP approach often uses technologies like Software-Defined Networks and Intent-based networking. Under this approach, the organization deploys a gateway at the application layer that establishes a secure channel between the user and resource without expose network access.

Deployment Considerations for Zero Trust

Across Distributed Enterprise Boundaries.
Organizations typically have a headquarters with remote offices, subsidiaries through M&A, and need to support a remote workforce exiting the Covid-19 pandemic. Since remote locations and homes don’t connect directly to an enterprise local network, a company might decide to create a portal for users who need access to resources.

Multi and Hybrid Cloud Architecture.
Organizations often deploy workloads in more than one cloud services provider and host multiple applications across different clouds. A zero trust approach enables “least privilege” security for both Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) by requiring users and entities to access the resources through a portal or centralized zero trust policy enforcement controller. This provides the company more control over how users gain access to cloud resources and also ensures better visibility and insights into cloud security.

Managing Third-Party, Non-Employee Access.
To mitigate the risks associated with outsiders accessing enterprise resources, zero trust can be used to create the need-based network connectivity with real-time identity verification to perform user tasks. Using zero trust enables you to offer just-in-time access while obscuring enterprise resources.

Private Applications and Customer-Facing Services.
An organization needs to protect both internal assets and customer information. Zero trust enables enhanced security when organizations can segment these customer services from enterprise services and use application catalogs to direct customers to the needed resources.

5 Steps to a Zero Trust Architecture

It's highly likely that you already have some network infrastructure in place before starting a zero trust journey. These requirements typically include:

Autonomous Discovery and Learning

- Instant clarity all devices/applications/"things"/services
- Zero trust "least privilege" ringfencing / isolation
- Gain visibility across the entire ommunication patterns
- Autonomous network resource learning and graph
- Advance network access control with agents when entering into network premises
- Cloud agnostic

Understanding Workflows

- Identifying key workload patterns from device-to-device and device-to-application communications
- Ensuring that all privileged user accounts have access
- Ensuring that all privileged user account access is appropriately limited
- Reviewing access to make sure no one has more access than they need

Deploying Infrastructure

- Cloud-native to support scale in and scale out
- SaaS centralized management and orchestration
- Cloud-delivered for cloud-first initiatives and digital transformation
- Agentless.
- Eliminate outsourced management and add-on IT cost
- Deploying Zero Trust solutions in stages to mitigate business interruption risk
- No forklift upgrade and least disruption on existing IT workflows
- Endpoint to Enterprise integration and consistent policy

Configuring Zero Trust Technologies

- Enterprise perimeters, home and branch offices
- End-to-end risk-based policies and configuration
- High availability design and disaster recovery plan with reference deployment guidelines
- Support for different applications, services, and protocols changes

Adaptive Security Posture

- Real time incident Response
- Risk-based control against lateral threat movement
- End to end SOC operations
- SOAR Automation
- SIEM Integration on all traffic and access logs
- Report on denied requests on failed MFA, known attacker or subverted IP addresses

About Airgap

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication.

airgap.io