ZERO TRUST SECURITYMODEL

cyber quotient
REDEFINING RISK MANAGEMENT

_cygularity
Cyber Security Redefined

Zero Trust Model

By Team Cygularity

Zero Trust is an information security model that does not implicitly trust anything inside or outside its network perimeter. Instead, it requires authentication or verification before granting access to sensitive data or protected resources. Zero Trust was coined by John Kindervag at Forrester Research in 2009. Zero Trust security provides visibility and security controls needed to secure, manage, and monitor every device, user, app, and network. The Zero Trust is also known as a Zero Trust Network or Zero Trust Architecture. Related frameworks include Google's BeyondCorp, Gartner's CARTA, and MobileIron's zero trust model.

Why is Zero Trust important?

Zero Trust is important because it is an effective way to reduce data loss and prevent data breaches, which have an average cost of $3.92 million globally according to a study conducted by Ponemon Institute and IBM. To understand why Zero Trust has risen to prominence in cybersecurity, we must first understand the issues with traditional perimeter-based network security models, and that starts with understanding how the Internet and local area networks interact.

The problem with perimeter-based security

One important thing to understand is once a single resource is connected to the Internet, all resources on the same local area network become connected too. In the past, the solution to this was to implement perimeter security, aka the castle-and-moat security approach where organizations defended their perimeter by setting up firewalls that prevented outside access to internal networks. This approach assumes every user inside a network is trustworthy and should have access. This assumption presents at least two problems:

- If a bad actor has network access, they can laterally move within the network to expose sensitive data, install malware, and cause data breaches.

- If an employee is not physically at work, they cannot access the network.

As you know, the solution to the second problem is a virtual private network, or VPN, that uses encryption to allow remote workers to access resources as if they were physically present in the network. The larger issue is there is a fundamental contradiction between the goal problems, one is about enabling outside access while the other is trying to keep bad actors out.

Zero Trust Model

By Team Cygularity

These two problems have been exacerbated by the rise of bring your own device (BYOD), software-as-a-service (SaaS), and cloud computing. Instead of the occasional employee needing to connect to the corporate network from home, every single employee has a device that is always connected, on-premise data centers have been replaced with the public cloud, and internal applications changed to SaaS solutions. In short, what was once on-premise is now largely off-premise so protecting the perimeter makes little sense. The fact is perimeter-based security frameworks are no longer an effective part of your enterprise security architecture. Not only are they susceptible to malicious insiders who launch a cyber attack from inside the network, but they are also vulnerable to outsiders. An attacker who has gained access to an internal network through phishing or other social engineering methods like spear phishing and whaling can pretend to be a trusted insider.
The answer is to stop trying to put everything behind a firewall and treat everyone as a threat until proven otherwise.

The Zero Trust approach

The Zero Trust security model follows the access control principle of least privilege where user identity is verified in real-time whenever a resource is requested. Least privilege access (usually) depends on multi-factor authentication (MFA) or two-factor authentication (such as a password and a trusted device or temporary code) and even once authenticated an individual may only access granularly-defined resources or applications as defined in an RBAC security policy.

The Zero Trust model solves all the issues inherent to a castle-and-moat access management approach:

- With no internal network, there is no longer the concept of an outside intruder or remote worker
- Individual-based authentication works across devices and on the application side across on-premises resources, SaaS applications, and public cloud (particularly when using an identity management solution like Okta or Azure Active Directory)

In short, Zero Trust starts with the assumption that everyone connected is not to be trusted until proven otherwise, allowing for far more distributed and granular control over secure access to sensitive data and internal resources than what was possible with perimeter-based security or even physical security controls.

Zero Trust Model

By Team Cygularity

The benefits of Zero Trust mean it has gained widespread acceptance and adoption, with companies like Google adopting a form of Zero Trust called BeyondCorp which assumes the internal network is as dangerous as the Internet.

What are the main principles and technologies behind Zero Trust?

The philosophy behind Zero Trust assumes there are bad actors within and outside of your internal network, so no user or machine should be implicitly trusted.

Principle of least privilege

Another principle of Zero Trust security is the principle of least privilege (PLOP). PLOP is the practice of limiting access rights for users, accounts, and computing processes to only those needed to do the job at hand.

Regardless of how technically competent or trustworthy a user is, the principle of least privilege should be used to prevent data breaches, as 80% of data breaches involve privileged credentials according to The Forrester Wave: Privileged Identity Management, Q4 2018. PLOP has the additional benefit of reducing the risk of privilege escalation.

Micro-segmentation

Alongside PLOP, Zero Trust utilizes micro-segmentation, the practice of breaking up security perimeters into small zones to maintain separate access to separate parts of the network. For example, a network of resources living in a single data center that utilizes micro-segmentation may contain dozens of separate, secure zones each equiring re-authentication and a different level of access. This means a person or program with access to one zone will not be able to access additional zones without authenticating again, reducing the risk of lateral movement attacks.

Multi-factor authentication

Multi-factor authentication is another core value of Zero Trust. MFA simply means requiring more than one piece of evidence to authenticate a user. This means that if an attacker exposes the password to a sensitive zone, they won't be able to authenticate without additional information such as biometrics or a one-time password. A commonly seen application of MFA is the 2-factor authorization (2FA) used on social media accounts like Facebook and Twitter. In addition to entering a password, users who enable 2FA must enter a code sent to their mobile device, thus providing two pieces of identity authentication.

Zero Trust Model

By Team Cygularity

Access control

In addition to controls on user access, Zero Trust also requires strict controls on physical device access. Zero Trust monitors how many devices and IP addresses are trying to access a network, ensuring every device is authorized.

Other technologies used

In addition, Zero Trust security may rely on SIEM, IAM, orchestration, analytics, encryption, scoring, and file system permissions.

How to implement Zero Trust

A Zero Trust approach ensures that you grant the least privilege necessary based on verifying who is requesting access, the context of the request, and the risk of the access environment. By implementing Zero Trust, you minimize your attack surface, improve audit and compliance monitoring, and reduce cybersecurity risk. Zero Trust implementing Zero Trust relies on these six tenets.

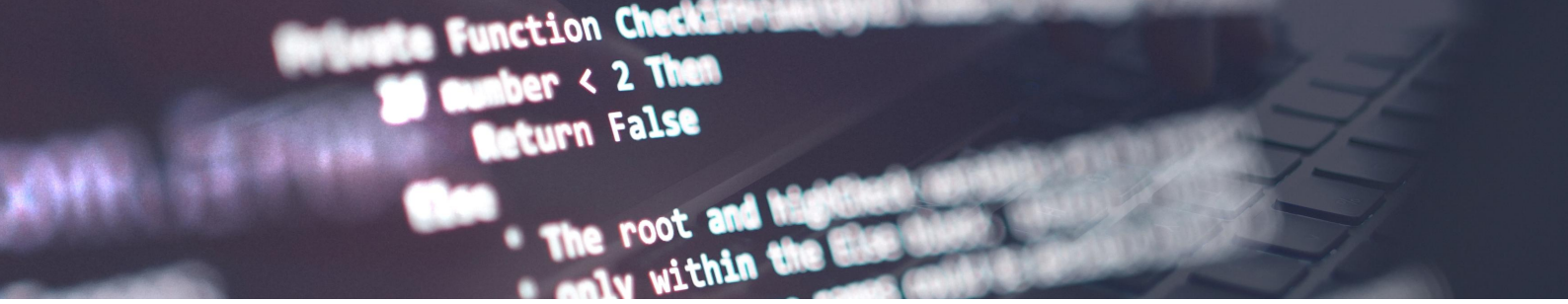
1***. Don't trust, verify***

Identity doesn't include only people but workloads, services, programs, and machines. Properly verifying identity should leverage enterprise directory identities, eliminating local accounts, and decreasing the overall number of accounts and passwords. This is why many organizations have invested in identity management solutions like Auth0, Active Directory, or Okta.

The most important part is to have HR-vetted directory identities that automatically disable once an employee is no longer with the company. In addition, you should apply multi-factor authentication (MFA) everywhere. During login, password checkout, at privilege escalation, effectively any time there is a new request. You must know who someone is when they are being granted access.

2. ***Contextualize requests***

For every request, you must understand why the person or process is performing a privileged activity. To do this, you must understand the context behind the request for access, and review and approve it if the request makes sense based on the context provided. Individuals should only have the level of privilege needed to perform a certain task and only for the amount of time needed to perform the task.



Zero Trust Model

By Team Cygularity

3. ***Secure your admin environment***

Access to privileged resources should be done through a clean source. This means preventing direct access from user workstations that also have access to the Internet and email, which can be easily infected with malware.

4. ***Grant least privilege***

There are six common ways to implement the principle of least privilege:

Group-based access management: Managing individual user access for hundreds or thousands of employees while adhering to the principle of least privilege is almost impossible. This is why identity access management (IAM) tools exist. IAM tools grant users access based on groups or job roles, then manage privileges based on groups rather than individuals.

Working hours-based access management: For employees who work consistent schedules, you can restrict access to the individual's working hours. For example, if a staff member only works 8:00 am to 5:00 pm Monday to Friday, they shoul not be able to use their keycard at 4:00 am on Sunday morning.

Location-based access management: For critical systems, you may only want people to access it from your office building.

Machine-based access management: Like location-based access management, you may only want critical systems to be accessible from certain machines.

One-time use access management: Use password safe where a single-use password for privileged accounts is checked out until the action is completed and then it is checked back in.

Just-in-time access management: Elevate privileges on an as-needed basis for a specific application when needed then revert back to a standard account once the task is complete.

Zero Trust Model

By Team Cygularity

5. Audit everything

Keep an audit trail of everything that happens during a privileged session, this is not only useful for computer forensics but also allows you to attribute actions to a specific user. For systems containing sensitive data, you may opt to keep a video recording of the session that can be reviewed or used as evidence.

6. Use adaptive controls

Zero trust controls need to be adaptive to the risk-context. Even if the request comes from an authenticated user, if it is in a risky location you may opt to ask for even more verification before permitting access. Adaptive controls should not only notify you of risky activity in real-time but also help you actively respond to incidents by cutting off sessions.

cyber quotient

Redefining Risk Management

Contact Us
amitabh@cygularity.com
+60 1111 320221
www.cygularity.com