What is Zero Trust?

NEVER TRUST, ALWAYS VERIFY

Ominous sounding yes. But necessary…absolutely.

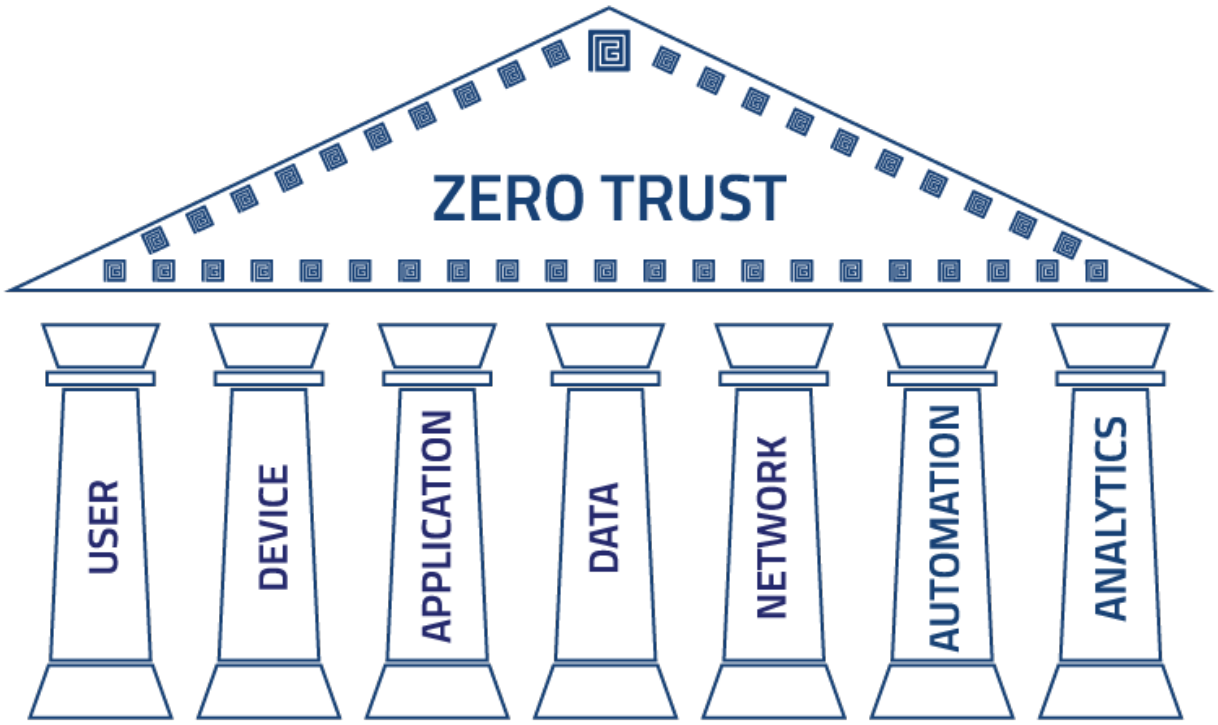
Organisations should not automatically trust anything inside or outside their perimeters…

and instead …

Must verify anything and everything trying to connect to their systems before granting access.

ENTER PKI. PKI is one of, if not the most secure way to establish Zero Trust.

Seven Pillars of Zero Trust



User- User Identification, authentication, and access control

Device- Validation of user and autonomous devices to ensure trustworthiness and level of risk

Zero Trust

Application and Workload- systems, Services and applications are protected against unauthorised access

Data- Data classification to ensure it is only accessed by those with permission

Network- Defining network access to stop unauthorised access by people or things

Automation- Automates security and network operational processes across the ZTA by orchestrating functions between similar and disparate security systems and applications

Analytics- Real time User and system analytics between all Zero Trust components

Goal of Zero Trust

Eliminate need for trust

Prevent vulnerability exploitation

Create a more secure system

How do we use it?

- **Gain Visibility and Context**

  Use Zero Trust to gain visibility and context for all traffic across users, devices, locations and applications, plus zoning capabilities for visibility into internal traffic

- **Identify business processes and risks**

  Use Zero Trust to identify your business processes, users, data, data flows, and associated risks, and set policy rules that can be updated automatically, based on associated risks, with every iteration

- **Adding authentication methods**

  Adding authentication and other verification methods will increase your ability to verify users correctly

Data Breaches

The available attack surface is growing exponentially due to accelerated digital transformation.

Rapid Increase

- Remote workers
- BYOD
- Partner access
- Cloud migration

According to a McAfee survey:

- Average enterprise employee uses 36 Software as a Service apps
- Average enterprise uses over 1900 cloud services
- Means protection of a perimeter does not protect the organisation
- Protection of the end point is essential
- What about more secure environments? Some don't Allow SaaS at all.
- Even more important in perimeter protected environments
- Need to be able to halt transiting across the network from a single breach point.

Zero Trust and PKI

- PKI provides the credentials that allow for that secure identification
- PKI Provides strong user and Device Authentication
- PKI key in NIST Zero Trust Architecture Approach. See SP800-207

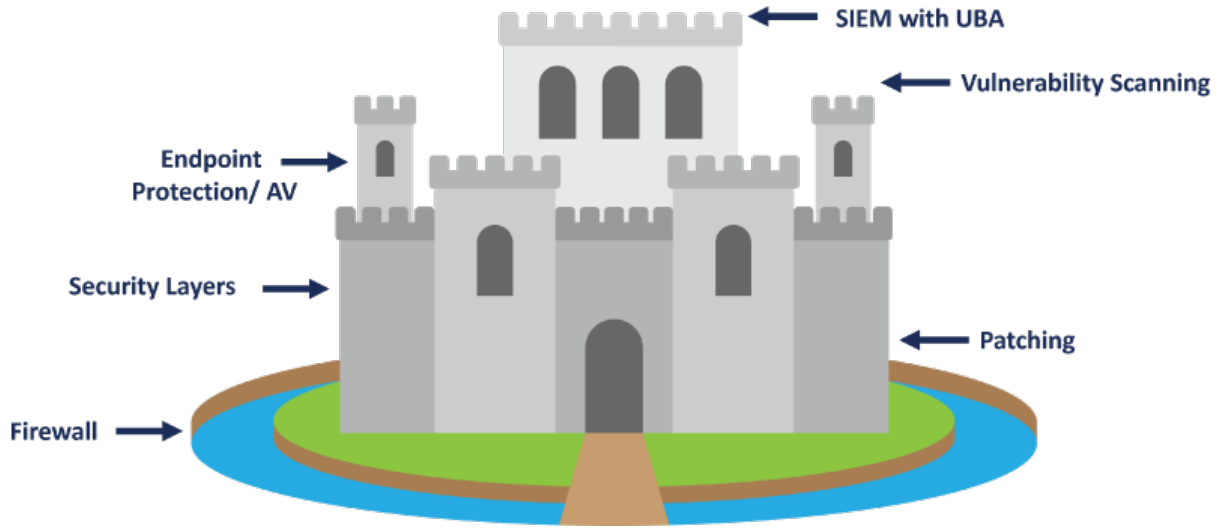
Identity and Certificate provisioning must be automated. This:

- Maintains security
- Avoids impacts to productivity and user experience

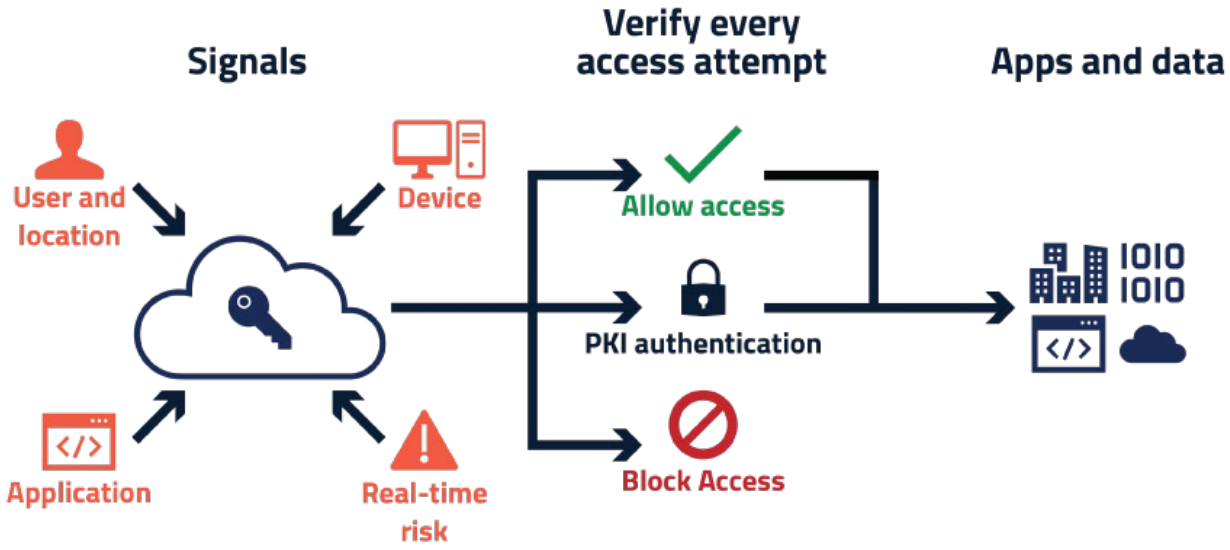
Cogito Group

Zero Trust

Old Approach



New Approach



Cogito Group

Zero Trust

Relies On?

- Zero trust improves security by making identity the new perimeter
- Zero trust relies on strong identity verification of people, devices, and services
- PKI uses encrypted public and private keys to ensure secure connections between users, devices and applications.
- Identity verification often needs Identity and Access Management (IdAM)
- A key control of IdAM is Public Key Infrastructure (PKI)

Identity and Certificate provisioning must be automated. This:

- Maintains security
- Avoids impacts to productivity and user experience

Use Cases

Authenticate

To identify the device and user making the request

Seamless

Allow access seamlessly

Encrypt

To prevent eavesdropping

Sign

Ensure data is not altered such as logs to aid in forensic analysis

In Practice

Verify **Validate** **Limit access and privilege**

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.