Contents

Introduction

Overview

This document is intended to provide a comprehensive end-to-end view of Zero Trust application deployment IaaS, PaaS, SaaS and network security components. It is intended to provide a High Level Design to meet least risk security requirements for

1. Identity security
2. Device security
3. Network security end-to-end across hybrid connections
4. Application Workload security
    a. IaaS security for the compute, network and storage components
    b. PaaS security
    c. SaaS security
5. Data security

Purpose and Intended users

This document is intended to provide a reference overview for the security components for technical, business and project management stakeholders who want to build a Zero Trust deployment. It is intended to serve as a reference for security component requirements and to provide an end-to-end overview of the technology interdependencies at play in delivering security.

It is a point of call to find

1. Design recommendations for security components
2. Requirements that informed the security design
3. Governance, management of risk and regulatory and corporate security compliance elements (e.g. data protection)

Approach

The approach taken is to provide a high level category of cloud security components, The aim is to map the delivery to the security requirements for the purposes of maximizing security and minimizing risk. .

The cloud technology delivery topics required to address the Zero Trust foundation components are identity, network, device, application workload and data security.

Technology Scope

In Scope: The external security of the web browsers, REST services, microservices, and platform compute, network and storage services. The security of communications between application services is in scope, as are data transport services, database storage, authentication and authorisation of end users, admins, and developers.

Technology:

1. Identity and Access Management
2. Network Security
3. Device Security (IOT, mobile, desktop)
4. Application (IaaS, PaaS and SaaS) Security
5. Data Security for end users

Also In Scope:

Secure Development and Operations
Security Monitoring and Intelligence.

While these topics are extremely important, they are not usually the primary focus of Zero Trust applications.

In summary the following technology is In Scope:

1. Application User Interfaces (person, device, application)
2. Application components
3. Authentication and authorisation services
    a. Application layer
    b. Presentation layer
    c. Session layer
    d. Transport layer
    e. Network layer
4. Network and transport communication
    a. WAF
    b. Network security groups
    c. Access Control Lists
5. Implementation and deployment environments, configuration QA

Objectives

This document aims to provide an overview security design, with a requirements traceability matrix. Specific objectives include:

1. Manage identity and access: Consistent way to manage identities and access for platform and application users.
2. Protect infrastructure, data, and application: Ensure virtual isolation and protection for compute, data and networking. Safeguard against application and network threats, exploits, and vulnerabilities. Provide secure connectivity to data at the enterprise and protect sensitive data both in transit and when stored in the cloud.
3. Optimize security operations across public and private cloud, and on premises: This provides information to provide least risk processes, methods, and tools for running security operations.
4. Provide a basis to consistently assess security practices, plans, and designs and evolve them in a timely manner to stay ahead of threats.

Roles and Responsibilities

The roles and responsibilities for security, while clearly defined, require collaboration amongst different stakeholder groups.

Security Management

The application owner has the information security management role, with overall responsibility for the end to end connectivity of the IT systems and cloud services. This provides for governance measures for regulatory compliance and risk reduction. Information Security Management must work in conjunction with cloud service administration and cloud service implementation.

Security Administration

Security Administration is a shared responsibility between Zero Trust applications participants, and monitors the security of each cloud service used (for example, managing authentication and authorisation of end users and endpoints), monitoring and reporting on correct service operations, as well as reporting on and responding to security incidents.

Security Delivery

Service delivery is responsible for the security of runtime cloud services and integration of application services on-premises and cloud. This role, while primarily the responsibility of Zero Trust applications, requires good communications across participants.

Requirements Tracking

Responses documented by Zero Trust application requirements and compliance documents are the primary source of tracking security requirements.

The responsibility matrix is documented as part of the Security Minimum Control Standards set by the organization regulatory requirements. .

The deployment security requirements source documents have different purposes and operate at different levels of the deployment. It is noted that both MCS and Policy documents cover much the same ground, with a different business and technology focus, depending on the stakeholders.

Deployment Requirements Documentation

Response to detailed requirements to be found in the application Minimum Control Standards Zero Trust application resources, which may include mapping to required control standards and/or frameworks such as the NIST Cybersecurity Framework.

Data Classification and Sensitivity Requirements

The overview deployment policy for data security must be developed in accord with organization regulatory requirements. .

Identity and Access Management

Identity and Access Management covers device, network, application and data functions.

The following measures provide the major activities for identity management. The compliance with these requirements is documented in the compliance statement for Minimum Control Standards for Security.

1. Identity Lifecycle Management – management of accounts, users, user groups and roles. This is managed by both Cloud Service Providers for IaaS and PaaS services and application owners for PaaS and SaaS services and micro services. The principle of Least Privilege is applied for end users and application APIs.
2. Role Based Access Control – controlling access to resources based on system and user roles. The application IDAM provides role-based access controls to manage container images. Fine grained access management is enabled by Role Based Access Control (RBAC) to application containers and Cloud Service Providers resources.
3. Privileged Account Management (PAM) – a set of additional controls for privileged access accounts, usually a combination of User ID and Server Side Password, and SSH keypair. Administrator/developer privileged access management enables monitoring of role access.
4. Multi Factor Authentication (MFA) – additional levels of authentication for higher security. Multi Factor Authentication (MFA) is enabled to provide at least two-factor authentication for the root Cloud Service Providers account.
5. Authentication and Authorization – ensure application users and applications are securely identified and have appropriate access privileges. API access control via authentication and authorization for securing domains
6. Audit and compliance – Zero Trust application deployment of Vulnerability and Penetration Testing is to be scheduled in collaboration with the application owner..
7. Security Gateways: Ensure gateways are effectively monitoring, logging and reporting on access by users and applications. Endpoint protection services are currently being evaluated.
8. Encryption: Ensure transport and application level security is appropriate for end user access with industry standard encryption algorithms
9. Token security: Ensure tokens for end user access are managed securely with industry standard tokens that are stored inside the Cloud Service Providers perimeter in an encrypted database protected by RSA 2048 public/private keypair with the private key stored in an encrypted key vault/secrets store.

Infrastructure Security

This section provides an overview of how Cloud Service Providers IaaS handles network security, secure connectivity, and secure compute infrastructure, as detailed in the Cloud Platform Design document and includes Cloud Service Providers online security resources for Infrastructure Architecture, Analysis and Design.

Cloud Service Providers Network Security Groups (NSGs) provide allow and deny rules at the instance level, while Access Control Lists (ACL) provide allow and deny rules to allow traffic to and from subnets.

Gateways, such as application network gateways and Cloud Service Providers network gateways are set up at

the subnet level to allow external network access. Routing rules to control which VPC/VNET subnets can communicate directly with external networks, whether these external networks are other VPCs/VNETs, private deployment networks, or the Internet.

Application access to infrastructure generally uses the Role Based Access Control built into Cloud Service Provider platforms. Users, groups and applications are assigned to a role which is assigned a set of common access privileges, such as read, read and write, read, write and assign, as appropriate. Access Control Lists applied at the network level are used to allow or deny access to subnets and VPCs/VNETs services. This mechanism ensures correct identity management access security across technology roles.

It also covers the physical data protection measures for securing inbound and outbound traffic flows, for data in transit, including APIs connected to external systems.

Encrypted transport TLS 1.2/1.3 communications links provide both for HTTP traffic, external provider APIs, as well as enterprise gateways to on premises applications.

Network Security

The following topics are key to ensuring security at the network layer.

Logging and Monitoring

Continuous logging and monitoring diagnostics and risk mitigation with endpoint, application and data threat prevention and detection. Possible and probable threat vector identification and use of policy facilitates positive identification of threat actors prior to allowing access.

Industry Compliance

Application of measures to ensure network deployment meets policies for internal and external devices, applications and people interacting with enterprise infrastructure.

Threat intelligence

Manual and automated access to industry and threat intelligence sources and databases.

Network Log Analysis

Systems to aggregate network traffic logs, resource access, security and performance information in near real-time. Cloud Service Providers make this log analysis readily available.

Network resource access policies

Combination of firewalls, security groups, identity access management policy rules and attributes relating to classification and sensitivity of enterprise resources.

Application Security

This section addresses application vulnerabilities and the effectiveness of application security measures.

It references the application security detailed in Application Security Design, as well as identifying the infrastructure and data security touchpoints, such as caches, keystore connections, and managing the performance implications of encrypting and decrypting data and communications.

The application platform plays a strong role in application security by providing a layer of abstraction for ensuring users are directed to identity management mechanisms before allowing access to protected resources.

In addition services are applied on the Cloud Service Providers platform to address common threats and vulnerabilities. Anti-malware, patching updates, managing known vulnerabilities and Security Information Event Management (SIEM) logging and audits are also part of the infrastructure security function. The Cloud Service Providers offer platform and network security monitoring and logging, and this can be integrated with existing application deployment security monitoring and logging.

Data Security

Data security concerns the discovery, classification and protection of data & information assets including protection of data at rest and in transit, and de-identification.

Database security as part of the application and application security architecture is referenced in this section, as are corporate information security principles.

Data security and data protection starts by clearly understanding the data, and the organizational, industry and regulatory requirements for protecting it, and the application's data classification, for example

1. Public - and thus does not need a large protection focus
2. Proprietary or confidential to either the organization or its applications
3. Regulated data, such as personally identifiable information (PII)

Examples of private data include:

1. Personally Identifiable Information (PII), such as name, address, phone number, email, etc.
2. Technically Identifiable Personal Information, such as geolocation data, device IDs, usage based identifiers, static IP address, when linked to an individual

Personal and technically identifiable information is encrypted in the application databases using available encryption mechanisms..

Zero Trust applications require access to data classification systems to understand what data must be encrypted in transit and at rest. Encryption of data is planned for best practice to protect data where required based on the sensitivity of the data or on the applicable organization or regulatory requirements. Details on best practice are found in Section 10.

Secure Operations

The objective is to securely acquire, develop, deploy, operate and maintain cloud services, applications and infrastructure. DevOps extends the application software development lifecycle (SDLC) by taking the approach that increasing automation in promoting applications to production can mitigate risks due to disconnects between developers, quality assurance (QA), testers, and operations personnel. Native cloud deployments and DevOps together provide a rapid response mechanism for application changes to be deployed using Continuous Integration, Delivery and Deployment. These considerations have to be in view of existing application deployment capabilities.

Operations security is an extension of application security. The focus of secure coding includes:

1. Input validation
2. Output encoding
3. Session management
4. Credential and password handling

Embedding security in an operational framework takes advantage of the increased agility and standardization of application deployment. Secure operations can be viewed as an extension of application security that is natively designed to utilize cloud infrastructure, platform virtualization and automation.

While scripted deployment of code, configuration and toolsets provides faster and more consistent software lifecycles, all the principles of application security are even more relevant, particularly determination of what must be manually tested to avoid unintentional results from increasing automation.

Application security design and principles are respected and are the basis of security testing. Network security has to be considered as an integral part of application security.

Container Security

Containers

Containers are virtual portable software packaging that provides shared environments for developers. They are a unit of software that can be deployed, with a self-contained operating system, able to be readily scaled.

They are sometimes described as a lightweight Virtual Machine, and are the basis of 'serverless' computing microservices.

Namespaces restrict what a process can access and utilize on the host. Processes are 'forked' by the operating system kernel within a 'namespace'.

A container is a subsetting of operating system capabilities by OS process.

The main OS constructs for containers:

Cgroup: Control Groups provide a mechanism for aggregating/partitioning sets of tasks, and all their future children, into hierarchical groups with specialized behaviour.

Namespace: wraps a global system resource in an abstraction that makes it appear to the processes within the namespace that they have their own isolated instance of the global resource

Container Orchestration

Container orchestration is inbuilt into the container platform, and describes the management of containers from development to production, to provide applications and services that perform on the available virtual infrastructure.

Container basic security measures

1. Provide Identity Management for applications and application end users.
2. Limiting number of processes to enhance security
3. Restrict memory usage to enhance security
4. Ensure no root privileges for containers on host
5. Environment variables security
6. Secrets management using a secure keystore
7. Ensure filesystem/image processes are restricted to only what is needed by container for operations

Operations Security Monitoring and Intelligence

While this is not a functional part of Zero Trust applications, participants can be aware that these measures are critical to success in the prevention of security incidents.

Logging the following activities:

1. Sign-in activities – Information about the usage of managed applications and user sign-in activities
2. Audit logs - System activity information about users and group management, managed applications and directory activities

Operations reporting provides a view of access to resources such as:

1. User access to resources
2. User access context
3. Users with changed access rights.

A joint effort can ensure that application processes are in place for log forwarding and incident reporting.

Governance, Risk and Compliance

Maintaining the application policy, audit and compliance measures, meeting corporate policies, solution-specific regulations and governing laws is covered in this section.

Compliance is part of the application requirements, and there are many references to aspects of compliance in

the Application Architecture Definition documents.

Compliance categories require links to data and infrastructure security as well as identity management, application and DevOps security.

The level of compliance has to be linked to the way security logging, monitoring and reporting is handled.

Current major cloud security standards include:

1. High-level IT management systems standards such as ISO/IEC 27001 and its associated cloud service specific standards ISO/IEC 27017 (for Security) and ISO/IEC 27018 (for Protection of Personal Data)
2. Security standards specific to certain aspects of cloud computing including ISO/IEC 27033 (for Networking), ISO/IEC 27034 (for application security), ISO/IEC 19086 (Cloud service SLAs)
3. Security Technology standards which detail specific technologies used to implement security controls, such as OASIS KMIP (Key Management), FIPS 140-2 (approved cryptographic modules). Security assertions from external systems such as JWT and SAML tokens may become the subject of future implementation standards

As there is an ongoing major architecture shift from an enterprise data centre, to a hybrid cloud deployment, Zero Trust application requires an updatable Minimum Control Standard set that applies also to external service suppliers, Cloud Service Providers, SAAS, PaaS and IaaS third party providers.

Cryptography

Cryptographic algorithms protect inbound and outbound traffic to the Cloud Service Providers and on premises application deployment using TLS at the transport layer for applications, and network overlay network security as well as measures such as IPSec VPN at the network layer to secure site to site communications.

Cryptographic functions to ensure the following security aspects

1. Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
2. Authentication: The process of proving the identity of the sender.
3. Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
4. Non-repudiation: A mechanism to prove that the sender really sent this message.
5. Key exchange: The method by which cryptographic keys are shared between sender and receiver.

Use of the following cryptographic architecture patterns ensures compliance with regulations for confidential information at rest and in motion.

There are three types of cryptographic functions currently in use:

1. Secret Key Cryptography (SKC): Use of a single key for both encryption and decryption; also called symmetric encryption. Primarily used for privacy and confidentiality.
2. Public Key Cryptography (PKC): Use of one key for encryption and another for decryption; also called asymmetric encryption. Primarily used for authentication, non-repudiation, and key exchange.
3. Hash Functions: Use of a mathematical transformation to irreversibly "encrypt" information, providing a

digital fingerprint. Primarily used for message integrity.

Secret Keys in Common Usage

The Zero Trust application Cloud Service Providers deployment makes us of the main secret key cryptography algorithms in use today:

Public key cryptography algorithms that are in use today for key exchange or digital signatures include:

RSA: RSA uses a variable encryption block and a variable key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors.

Elliptic Curve Cryptography (ECC): Examples of this type of encryption are Diffie-Hellman elliptic curve and NSA Suite B. This is A PKC algorithm based upon elliptic curves. ECC can offer levels of security with small keys comparable to RSA and other PKC methods. It was designed for devices with limited compute power and/or memory, such as smartcards and PDAs.

Note: Public Key Cryptography Standards (PKCS) is a set of interoperable standards and guidelines for public key cryptography, designed by RSA Data Security Inc. It covers topics such as passwords, certificates, tokens and keys. It is not an official standard.

Quantum Safe Cryptography is still under development by standards bodies such as NIST.

Current Hash Functions

Hash algorithms that are in common use today include:

Message Digest (MD) algorithms: A series of byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message.
MD5 (RFC 1321): Developed by Rivest after potential weaknesses were reported in MD4; this scheme is similar to MD4 but is slower because more manipulation is made to the original data. MD5 has been implemented in a large number of products although several weaknesses in the algorithm were demonstrated by German cryptographer Hans Dobbertin in 1996 ("Cryptanalysis of MD5 Compress").

Secure Hash Algorithm (SHA): Algorithm for NIST's Secure Hash Standard (SHS), described in FIPS 180-4.
SHA-1 produces a 160-bit hash value and was originally published as FIPS PUB 180-1 and RFC 3174. It was deprecated by NIST as of the end of 2013.
SHA-2, originally described in FIPS PUB 180-2 and eventually replaced by FIPS PUB 180-3 (and FIPS PUB 180-4), comprises five algorithms in the SHS: SHA-1 plus SHA-224, SHA-256, SHA-384, and SHA-512 which can produce hash values that are 224, 256, 384, or 512 bits in length, respectively.
SHA-3 is the current SHS algorithm. Although there had not been any successful attacks on SHA-2, NIST decided that having an alternative to SHA-2 using a different algorithm would be prudent.

Transport Layer TLS/SSL.

TLS/SSL encryption provides guarantees of integrity during transmission. The private key used to generate the cipher key must be sufficiently strong for the anticipated lifetime of the private key and corresponding certificate. The current best practice is to select a key of at least 2048 bits. In addition, the private key must be stored in a Key Vault as per application architecture.

After the initial certificate handshake, a common practice is to use an ephemeral (temporary) shared secret key exchange such as the Elliptic Curve Diffie-Hellman (ECDHE) Diffie-Hellman for forward secrecy with an appropriate length for the generated temporary key

Strong TLS 1.3 is currently using the ECC with SHA 2 (e.g. SHA-256 and SHA-384 algorithms) as a signature to prove ownership of a private key. (ECDSA with SHA-1 is now deprecated).

Application inbound traffic is routed through a WAF protected application gateway subnet, encrypted using TLS/SSL to protect data during transmission. TLS/SSL provides authentication of the server certificates to the client application.

Application outbound traffic to third parties uses an Cloud Service Providers Network Security Group (NSG) whitelist.

TLS 1.3 is used to secure transport. It is not sufficient as the sole source of encryption for data security, as transport layer vulnerabilities persist.

Network Layer

Network encrypted communications are used for inbound and outbound traffic across network segments and provider boundaries, including public internet.

Development, Test and Production environments inbound and outbound traffic best practice is to use authentication to and from network endpoints.

Network segmentation to be applied wherever possible, as this isolates resources from the flow on effects of a data breach when network incursion occurs.

Best practice Domain Name System (DNS) traffic management, domain certification and network layer firewalls are essential. Consider DNS Security Extensions (DNSSEC), a security protocol created to mitigate DNS hijacking. DNSSEC protects against attacks by digitally signing data to help ensure its validity. With DNSSEC enabled, the signing happens at every level in the DNS lookup process.

In Summary

Zero Trust security provides an assurance that every measure has been taken to ensure safety of information technology application deployments, in the context of the current threat landscape, and the requirement to update older application deployments to mitigate the risk of known cyber security application vulnerabilities, as well as zero day threats.

Basic data encryption requires at least the encryption of data prior to storage, and automatic decryption of data when reading from storage.

It is recommended that identity management, network, device and application security measures are aligned with application data classification requirements..

Zero Trust applications have to request sufficient visibility of application data classification policy to ensure that the appropriate level of identity and network security is applied.

Data being transported in or out of the application infrastructure, both in the cloud and on premises, must be secured at both the transport and network layers.

Data must be protected as follows:

1. Field level encryption of data
2. Encryption using TLS 1.3 for external communications
3. Endpoint protection with good coding practices
4. Network security augmented with SDN, IPSec or SSL VPN communications

The development of an application security architecture based on reference architectures such as this document is a cost effective insurance policy against data breaches, reduces damage from emerging types of ransomware threat, and provides a repeatable model of best practice.