Zero Trust as a Security Philosophy

cloud security alliance®

The permanent and official location for the CSA Zero Trust Working Group is
https://cloudsecurityalliance.org/research/working-groups/zero-trust/

Acknowledgments

Lead Author

Paul Simmonds

Contributors

Hillary Baron
Marina Bregkou
Josh Buker
Daniele Catteddu
Sean Heide
Erik Johnson
Shamun Mahmud
John Yeoh

Production

Frank Guanco
Stephen Lumpe

Table of Contents

Summary

When implemented correctly, a Zero Trust strategy or approach to information technology, and the architecture that supports it, has the potential to provide a simpler, more secure and flexible environment for an organization to do business.

This paper takes a neutral look at both vendor and technology solutions and what Zero Trust means for organizations; provides recommendations to develop a strategy and the supporting architecture that supports the organization and its workflows; and aligns IT to business goals and outcomes.

The paper looks at the origins of the term, as well as what the term means today, and gives an overview of the subject so that executives can understand the aims and objectives behind Zero Trust; while technology subject-matter experts can see where their area of expertise (or product set) contributes to the overall picture.

In principle, you can think of Zero Trust as different from other (historical) approaches in the following ways:

- Inside out, versus an outside approach; Zero Trust begins with the value and access rights for the data
- Verifying before trusting (and sharing information)
- Reduced reliance on a physical perimeter
- Both data and logical access is risk-based
- Trust decisions are based on identity

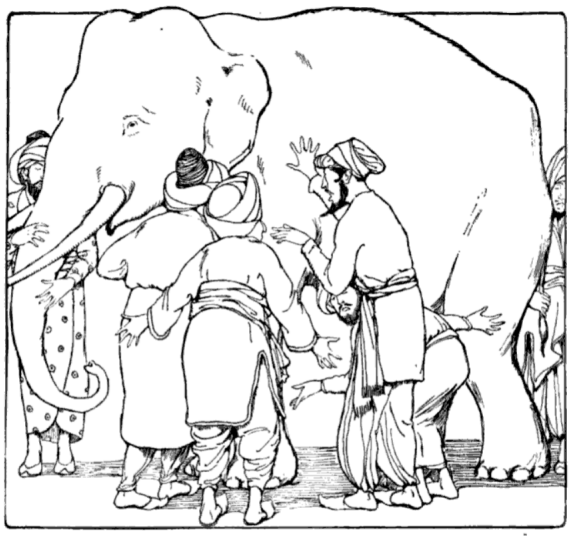
Ultimately, for most organizations, a Zero Trust approach will be just another tool in their toolbox; complementing existing security solutions, such as firewalls and VPNs. Like any other control, it may be used in conjunction with (e.g., compensating control) or in lieu of other (protective) controls.

An Introduction to Zero Trust

There is a parable dating back some 2,500 years of three blind men in a jungle who come across an elephant, the one who grabs its leg describes it as a tree, the one who grabs the tail describes it as a snake, etc.

Zero Trust is similar to the elephant and depending on your area of expertise, your role, or the product you sell, you will describe both the problem and its solutions radically differently.

"Zero Trust" has morphed into an antithesis term for the fact that the security models and solutions that have been used and, to a large extent, ingrained in the training of IT, network, and security professionals, have been failing for many years.



Public Domain, https://commons.wikimedia.org/w/index.php?curid=4581243

> Today, Zero Trust is an overarching security philosophy, dictating that any/all access requests to systems or data should be risk-based and start from a position of zero trust.

So, what is "Zero Trust"? Is it a strategy? A set of design principles, architecture, or products? This paper will argue that it's all of the above, but more importantly, it's the ***philosophy*** of how you align the requirements of today's business with a risk-based approach to IT Infrastructure, Networking, Security, and Cloud.

"Zero Trust" is also a misnomer, as the architectural response to the "problem statement" depends on implementing solutions that put trust into your IT ecosystem.

However, caveat-emptor [buyer beware], the definition of Zero Trust changes from vendor to vendor and from one security professional to the next. Perhaps this is due largely to there being no single source of standardized definition by regulatory bodies. As one of the modern-day challenges to Zero Trust, this presents the need to provide this underlying philosophy.

What should businesses be aiming to solve with a Zero Trust philosophy?

The response to a Zero Trust philosophy will be a unique architectural strategy for the organization, driven by the strategic aims of the organization and aligned with its risk appetite to deliver a flexible technological environment that meets both the current, medium, and long-term needs of that organization. This can be achieved by re-architectecting or integrating Zero Trust principles into current business practices and methodologies.

A Zero Trust approach enables an organization to be more secure and resilient. Some key advantages of when implemented properly are:

- It enables the organization to be more secure and resilient.
- A focus on business-critical assets and a tailored risk-based approach to the security of those assets.
- A vendor-neutral, technology-agnostic approach that reduces the dependency of vendors and makes the business owners responsible and accountable for providing access to information.
- Easier technology and security collaboration, especially with other organizations (Partners, JV's, Outsourced partnerships etc.).
- Simplification of the operational model for both IT and Network teams, with IT and Information Security better aligned to business needs.
- Enhances user experience by reducing friction fore end users, IT, and security teams.
- Enhances user experience by reducing friction for end users, IT, and security teams.
- Reduces both Capital Expenditure (CapEx) and Operating Expenditure (OpEx).
- Delivers a standards-based approach to operationalize Zero Trust and future-proof investments without complex re-architecture exercises.

Other benefits from a Zero Trust implementation are (but not limited to):

- Enhances visibility and automated real-time responses that allow defenders to keep pace with the threat.
- Enables an easier transition between on-premise and cloud solutions.
- Supports organizations in adopting multi-cloud strategies.
- Enables organizations to embrace IIoT (Industrial Internet of Things) and supports an Operational Technology (OT) strategy.

Today's Zero Trust Philosophy

If you critically examine the nature of an organization's IT infrastructure, their assets, and their data, most businesses consider any perimeter irrelevant as a viable security approach. At best, retaining the corporate intranet provides an area over which corporate IT can provide guaranteed throughput, with a coarse filter to the Internet that keeps out the "lumps," providing a network with an understood level of point-to-point throughput and quality of service.

Many organizations and governments have adopted a "cloud-first," "cloud-smart," or a hybrid Cloud strategy, and startup businesses today are unlikely to own any of their own infrastructure, with the entire business running on outsourced services using OpEx[1].

Whatever the organization's strategic approach to technology, its assets–people, systems, user devices, and data–are spread far and wide; some on systems owned and managed by the organization, but increasingly much of it outsourced (e.g., SAAS[2] and other in-the-cloud or third-party services). Thus, an organization's data, and increasingly critical data, are not held on infrastructure owned or managed by the organization, with that data usually being accessed through the Internet.

This leads us to one of the fundamental principles from the US Government National Security Agency's work on Zero Trust, which is "Assume breach"[3]!

> "Fundamentally if someone wants to get in, they're getting in"
>
> *- General Michael Hayden, former director CIA & NSA.*

For most organizations, the architectural response to most common security vulnerabilities will use elements of Zero Trust-based solutions. Whether a breach in the organization's intranet, likely making it no safer than the Internet, a breach to the service provider, a third-party breach, a breach happening to a joint-venture partner–all can be approached for management (intrusion, detection, prevention, etc.) from a Zero Trust architecture perspective.

By having granular visibility across the intangible assets, the critical data and where that data flows, and then by either designing out or mitigating the risk, an organization can better protect the identified business assets, irrespective of where they are located.

However, turning a zero trust philosophy into a viable architecture will demand a risk-based approach for the validation of all entities[4] in the transaction chain, coupled with a contextual (users, devices, network, behavior parameters, etc.) and continually evaluated view of whether the transaction is, or continues to be, valid–something referred to as "Entitlement".

1 Operational Expenditure; funded by day-to-day running cost, not requiring capital expenditure/investment
2 SAAS is Software-as-a-Service
3 NSA | Embracing a Zero Trust Security Model (U/OO/115131-21 | PP-21-0191 | February 2021 Ver. 1.0)
4 Entities are: People, Devices, Organizations, Code and Agents - Definition: Jericho Forum

Organizations are moving away from perimeter-based controls architecture to a Conjoint security control architecture, which is a combination of data-centric controls and user/identity/behavior and threat-based controls. The primary goal of the Zero Trust philosophy is to move the perimeter closer to the 'subject' and 'enterprise resource'. Acquiring and retaining skills to match this ever-changing and fast evolving landscape, and maintaining a mature security posture for the organization, are some of the ongoing challenges one faces when adopting a Zero Trust philosophy.

A Zero Trust approach presumes that a problem exists, while compliance is most often focused on prevention. This gives agencies and organizations a huge benefit because instead of being locked into a single vendor, technology leaders can now implement a whole framework. Thus, instead of a product or a service that offers just compliance, the implementation of which comes down to a parameterized architecture and check-box assumptions that risk creating a false sense of security, Zero Trust makes it possible to choose the best technologies to monitor, manage, and control access to resources wherever they reside.

A Risk-Based Approach Towards Zero Trust

Implementing any Zero Trust philosophy demands a risk-based approach across the many pillars of information security practices for an organization (Data Access Governance, Identity and Access Governance, Threat Management, IT/OT convergence, etc.). These practices encompass the domains of data security, network security, endpoint security, server security, OT security, IT security, physical security, location security, and people security.

Unfortunately, most current technology and security design assumptions have been based on the notion of binary trust. "They are trusted because they are on our Intranet," or "They are who they claim to be because they (eventually) gave a correct password," or "They passed security vetting." Risk, especially when moving to a more granular approach demanded by a Zero Trust principles, must also be variable based on:

- An understanding of the context of the entities involved
- A situational understanding of what the entity is requesting
- Continually analyzing behavior and risks tied to the entities (users, devices, identities, etc.)
- Continually assessed as the context changes

The Zero Trust model becomes even more powerful when it additionally adopts a context-aware security posture.

Context implies being able to understand the user, the device(s), the organization, the location(s), the nature of the transaction as well as how they are related to previous transactions and potentially many other factors. The continuous analysis of the behavior tied to entities with the defined boundaries of the entity taking the risk strengthens the security context.

Ideally, any system validating that the risk is within the accepted limit will also be capable of step-up authentication on transactions considered as higher risk by established policies or added security context. This evaluation can be executed as close as possible to the asset being protected.

Risk also has a temporal aspect; what may be true at a point in time will change. For example, a "hostile termination of a user" should, near instantaneously, block all current user access to both systems and data. The continuous assessment of risk should be a design characteristic of any Zero Trust principles-based approach.

Moving Towards Zero Trust Principles

When looking at what actually constitutes Zero Trust, the starting point is to understand the risk and get complete visibility and understanding of the assets and accesses, alongside understanding the holistic risk and entity risk within each of the following areas below. For each of those areas to understand how that risk can be…

- Eliminated (designed out), or
- Mitigated (compensating controls added), or
- Transferred (another party takes on the risk, e.g.; Insurance), or
- Accepted (the risk remains as a cost of doing business)

Thus, by defining the level of trust that can be placed in each risk area, this allows the understanding of the end-to-end risk of any transaction chain.

The aim should be to use components and/or architectural strategies that, as much as possible, mitigate the risk. For example, using encryption for data storage and/or encrypted protocols for data in transit, for which the keys are never shared/exposed, may mitigate many risks.

However, especially when implementing compensating controls, new strategies, tools, and architecture may be required that are specifically designed for a Zero Trust architecture.

When discussing Zero Trust within a corporate environment, the areas that warrant consideration in any risk assessment should include the following.

1. No Trust in Any Network, Including Your Own

Starting from the assumption that an Intranet is no more secure than the Internet, data transiting any network should be protected using an inherently secure protocol[5] appropriate to the data being transported.

In general, encapsulation technology (e.g., VPNs) should be avoided unless absolutely necessary. For example, as a temporary measure to support legacy systems that cannot be protected using a more modern approach The definitive alternative is to use risk-based MFA that can also extend to legacy systems and tools that cannot be protected by VPNs.

2. No Trust in the Internet

While obvious, if you do not trust your own intranet, data transiting the Internet should be assumed to be monitored, intercepted, spoofed, and generally untrustworthy, as should Internet-provided services, such as DNS.

5 An inherently secure protocol is one where the data is protected and both/all parties are appropriately authenticated.

However, the Internet is generally designed to provide very robust, standards-based, infrastructure with multiple points of entry and exit (e.g., Wired, 4G, 5G, private, and public connections).

Note that caution should be exercised trying to put private secure tunnels over the Internet when designing a Zero Trust architecture. An organization should ensure that any chosen solution does not negate many of the resiliency benefits, or result in being locked-in to requiring a single vendor solution.

3. No Trust in the Countries You Operate in

It's evident from recent and past attacks that nation-state actors and criminals operate in all countries. Thus, the infrastructure used, even when "exclusively yours," such as a private MPLS link, cloud service, or third-party managed service, should be presumed as being monitored and subvertable.

Note that most countries have the equivalent of the US Government's "National Security Letter" (NSL), gagging the disclosure of a government's request to data.

Consider ensuring that cryptographic keys are only held within your organization, or by the individual; should a legitimate request for, or illegitimate theft of, data occur, then the keys must also be obtained from the data owner.

4. No Trust in Third-Party Hardware or Code

Hardware can be compromised at the chip level[6] (chips with "undocumented features") as well as the circuit board level[7] (undocumented chips/functions).

Code, whether BIOS level[8], OS, Application or Microservices, can contain exploitable bugs and can also be malicious or subverted.

This risk can typically be mitigated by a full understanding of the entire supply chain that manufactures the hardware and firmware and would be part of a wider Third-Party Risk Management (TPRM) process, probably only undertaken by Military and Government organizations.

> - Where it is viable, fully encrypting data in transit and at rest, with the keys not residing on, or used by the server, should mitigate the risk.
> - While a code review may act as a mitigating factor, for much commercial software, a code review is prohibited, thus, when using commercial-off-the-shelf software (COTS), most organizations choose to accept the risk[9]; or add compensating controls.

6 https://cwe.mitre.org/data/definitions/1242.html

7 https://www.wired.com/story/plant-spy-chips-hardware-supermicro-cheap-proof-of-concept/

8 https://searchcloudsecurity.techtarget.com/definition/BIOS-rootkit-attack

9 Zero trust establishes the framework for minimizing risk from third parties by examining security gaps that occur during these interactions. It unifies and consolidates security policies in-house, minimizing vulnerabilities created by insufficient security practices of outside vendors.

- Best practices using open source (including open-source libraries) should include source control, business logic, and code reviews (DAST/SAST/IAST). Again they need to be risk-based and based on industry standards and frameworks such as MITRE and OWASP Top 10.

5. No Trust in DevSecOps

Whether the code is in a user-utilized DevOps model or a more enlightened DevSecOps model, code development will still introduce bugs and exploits. When code is developed in-house:

- Functional requirements should describe how software is expected to function and begin as business requirements from several different places. These requirements are followed by designers, coders, testers, and many other operatives. Environment separation or "Separation of Duties", validation, and continuous monitoring for compliance should help mitigate risks.
- Software development MUST implement "Secure by Design" principles through the secure software development lifecycle (SSDLC) irrespective of the model employed (e.g., Waterfall, Agile, Spiral).

6. No Trust in System Administrators (Yours or "Theirs")

A system administrator is a high-value privileged user, which poses a significant amount of insider threat to any organization. Organizations are faced with dilemmas on managing these high-risk users who can pose a significant threat whether intentional (malicious) or unintentional (negligent). A valid administrator account can be obtained by the threat actor to move laterally in the organization and to access and control critical resources. These attacks are difficult to determine when valid credentials are used with no visibility into behavior, risk, and security context.

A system administrator generally has the ability to do (or reset) anything on a system, and however well you are able to vet your system administrators (assuming your organization even does it) there is virtually no opportunity to vet administrators employed by third parties that are your outsourcers/ cloud providers/JV Partners, and so on.

For systems that are a high-value target, you should assume that the system administrators are themselves targets for extortion, coercion, blackmail, and so on.

With Zero Trust principles, administrators like all other users of the system should be subjected to continuous validation and monitoring. Access should be granted on a "need to know" basis based on privileges, access policies, behavior, and dynamic risks, and also by determining whether these are human users or service accounts. An example could be that they should be able to administer systems (backup, manage, and configure systems) but not have access to actual data.

- Full mitigation can probably be achieved if the system does not handle unencrypted data, viable on a storage server, but unlikely on an application server or end-user device.

- Partial mitigation can be provided with Privilege Access Management (PAM) coupled with an independent change control system and code fingerprinting. PAM solutions are evolving with "just-in-time" privilege management now a reality.
- Partial mitigation may be achieved with employee monitoring (where it is legal/ethical) with integration into a wider ecosystem of logging, monitoring, and anomaly analysis tools.(e.g., SIEM, SOAR, NDR, EDR)
- Partial mitigation can be provided by selecting third-party providers' relevant security certifications or attestations (e.g., CSA STAR, ISO27001, SOC2, etc.) with a scope that covers your usage of their services.
- Partial mitigation can also be provided by utilizing vendor risk management, digital risk management, and supplier risk management tools when outsourcing services to third parties.

7. No Trust in a (Secure) Server Location or the System's Physical Security

Without exception, almost all secure server/system locations can be breached (by an insider attack, stealth, force, or a court-issued warrant) if the target has a high enough value.

- Again, full mitigation can probably be achieved if the system does not handle unencrypted data, and partial mitigation provided by selecting third-party providers with the appropriate ISO27000-family of certifications with a scope that covers your usage of their services.
- Physical security, whether of locations you manage, or locations managed in third-party environments, is often overlooked when it comes to providing security services based on Zero Trust. Physical access to the server room/Data Center and/or to the physical server can critically undermine the security of the systems.
- Social Engineering (e.g. phishing) is gaining traction, and the best line of technology defenses can be breached by HUMAN's "the weakest link in the security chain." However, it is also imperative to know that humans can provide the first, middle, and last line of defense. Security Awareness programs should be a part of the mitigation strategy as well as providing compensating controls.

8. No Trust in the Endpoint

Whereas "devices'' cover all systems, servers, and so on, "device endpoints'' specifically have a human behind them. More often than not, they travel across various networks, and in a non-Zero Trust principled approach, they bridge the hardened perimeter, meaning that infecting/subverting a device "outside" carries the infection "inside."

Endpoints have other issues too, from the ability to trick the human into clicking on malicious code, to the (now) ubiquity of home-working and the rise of BYOD with the reluctance of the actual owner to have corporate monitoring software/apps on "their" device. They are also the point at which data, even if it was encrypted, needs to be decrypted to allow the person to interact with it.

Mitigation strategies for endpoints can include:

- A "locked-down" corporate image
- Code execution restrictions, approved code (via signed code and/or corporate approved app store)
- Endpoint software/apps capable of reporting device "hygiene" attributes; such as OS version and patch level, anti-virus version, device risk score/posture, etc.
- Endpoint software/apps capable of reporting device "status" attributes, such as geolocation, device model, and thus capability (e.g., biometric capability)
- User-awareness training
- Anomaly monitoring of endpoints accessing key systems
- A DNS firewall (or DNS firewall service)
- Change management and patch management.
- Data aggregation from the endpoint into a centralized anomaly monitoring system (assuming it's a corporate-owned device).

9. No trust in Identity Ecosystems

Most (legacy) identity directory solutions are broken with one or more of the following issues:

- They only support people (not entities such as devices, service accounts, and non-human identities)
- They operate binary authentication ("User123 has passed authentication")
- They demand to be the span-of-control (you can only make it work if everything is within that system)
- They contain non-authoritative and/or stale (non-maintained) attributes
- Validation must be, directly or indirectly, with only that identity solution

An identity strategy will probably be at the heart of any Zero Trust architecture. If correctly implemented, it will enable the contextual risk-based understanding of whether a transaction is entitled to proceed with risk-based conditional access.

The features of such an identity system should encompass:

- Trusted (signed) attributes of any entity for which your locus-of-control is authoritative
- The ability to consume trusted attributes from entities outside traditional network boundaries.
- The ability to analyze access behavior along with telemetry from multiple entities like devices, applications accessed, privileges, locations, time, and many more.
- Risk-based scoring of the level of immutability between entity and attribute.

Either separately, or as an integrated solution, an entitlement/authorization engine will:

- Hold the rules by which access is granted to a transaction
- Consume attributes, in context, together with their risk-scores
- Take attribute feeds from devices involved in the transaction (e.g., GPS from a smart device)
- Take device, data and intelligence feeds from other systems, both internal and external (e.g., geolocation services, or inter-bank IP-Address threat data)
- Support step-up authentication, and extend to legacy systems and tools (e.g. PowerShell) that are not generally covered by identity verification tools
- Support continuing real-time monitoring and analysis of behavior, risks and deviations in transactions
- Take additional inputs from systems providing continuous monitoring and behavior anomaly detection
- Utilize (port-based) Network Access Control[10] to enable access to certain restricted networks (probably for highly-sensitive access).
- Enable risk based conditional access to improve user experience - that is, trigger step-up authentication only when the risk changes, tied to behavior, baselines and other signals such as device used, geo-location, etc

It is likely, over time, that entitlement solutions will migrate from central control and be located closer to, or part of, systems and applications, to obtain better integration with the application that is being transacted with. This enables entitlement "shims" to be implemented identically whether in-house, at a third-party or when using cloud services.

10 802.1X-2020 - Port-Based Network Access Control - https://ieeexplore.ieee.org/document/9018454

Cloud and Zero Trust

The risk analysis required for a Zero Trust architecture has large similarities and overlap with the risk analysis required for (third-party hosted) cloud implementations; whether SaaS, IaaS, or PaaS, as the system, applications and data are all operating in an environment over which there is minimal control and restricted visibility.

This enables organizations to leverage many of the same methodologies when analyzing Zero Trust architectural risk as they should do when analyzing cloud-risk, such as:

- The ENISA[11] work on Cloud Risk[12]
- The CSA Cloud Controls Matrix (CCM)

Though, while these may aid in highlighting the risks, many of the solutions to mitigate the identified risks are likely to be different.

Architectural differences

A cloud environment is designed for the cloud service provider (CSP) to have full control over their components of the "shared-responsibility model" (see Figure 1), as well as visibility into the network and network traffic.

11 ENISA is the European Union Agency for Cybersecurity

12 https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

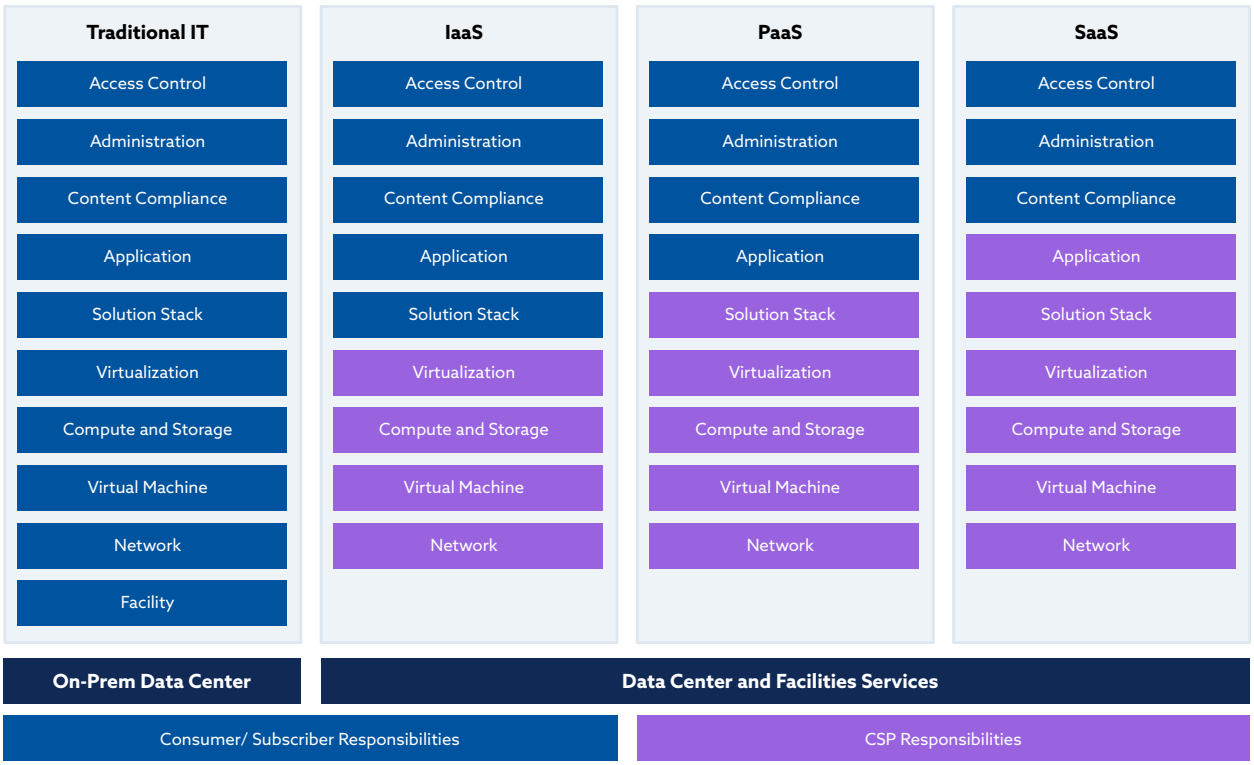


Figure 1: SEQ Figure, Shared Responsibility Model for cloud

Most organizations using cloud-based infrastructure will therefore adopt a shared responsibility model that requires trust of the CSP, relying on external certification to assure themselves that the risk is suitably mitigated while implementing tools and processes to gain visibility to the components they are responsible for in the model.

Where a CSP provides the provision for the relevant monitoring and logging of parts of the model managed by them, but relating to the client, then organizations may want to ingest such data into their own tools by way of further mitigation of the risks involved in using cloud services.

Zero Trust tools in a cloud environment

Where organizations are running a hybrid provision of services, on-premise, third-party, cloud, etc., then they should ensure that the Zero Trust philosophy they adopt, and particularly the tools and services used to support their architecture, will extend into any third-party services, cloud services, or cloud infrastructure they use.

Data in a third-party environment

For data at rest and data in transit, similar risks and mitigating solutions apply for both Zero Trust and the cloud. However, where a cloud service (most typically SAAS) processes the data, then the mitigation controls become more difficult.

Where cloud or Zero Trust may not be appropriate

Moving to a Zero Trust architecture within an organization, where there is no longer a reliance on the perimeter as a security boundary, should imply that it is now architecturally irrelevant where many systems and applications are physically hosted. However, there will be other operational, security, and design constraints to consider. Examples are:

- An industrial control system will probably need to be on the same physical network as the equipment that it controls, with appropriate segregation, redundancy, and network quality-of-service provisions.
- High-risk (and/or high value) systems and applications may need to be under the direct control of the organization's staff that can be vetted, with real-time monitoring and management controls.

Critical to integrating cloud solutions into a Zero Trust risk-based architecture is the ability to gain (potentially real-time) insight into those aspects of a cloud solution that need to be trusted and cannot be designed out - often quoted as the need to "trust but verify."

Risk reduction via cloud-delivered Zero Trust

Cloud services are no longer solely used to host the applications that need to be protected with a zero trust approach; in addition, cloud services have arisen to provide secure Zero Trust access to those resources. These cloud-delivered Zero Trust solutions benefit from the same fundamental advantages of cloud-based application hosting - resilience, flexibility, elasticity, scalability, visibility, transparent user experience, etc. External attack surface reduction, elimination of single points of failure, separate control and data plane, prevention of unauthorized lateral movement, and reduction of vulnerability to automated attacks are a few of the potential risk mitigations offered by a cloud-based approach to Zero Trust access.

Conclusion

Most organizations regard their IT and security teams as inhibiting or adding friction to business processes. The outdated perimeter model has been responsible for many of the problems, requiring complex gateways and interfaces to transit the perimeter, which in turn demanded conformity of authentication against corporate identity silos for people and devices.

In today's business world, no organization is an island. Collaboration and frictionless connectivity to the data and systems needed to provide services in a timely and cost-effective manner are demanded by the board, business leaders, and shareholders.

Aligning Zero Trustzero trust strategy to business risk, maturity and strategy

Zero Trust presents an enormous opportunity for organizations embarking on their digital transformation journey.

The advent of Zero Trust should be regarded as an opportunity to better align IT with an organization's business strategy. The whole purpose of modern networked computing is to facilitate collaboration, both with others that are part of the organization, but more importantly with entities that are not part of the organization, whether on the intranet, through the Internet, or as part of an outsourced service.

Implementing Zero Trust is about organizational and cultural transformation; it is neither a technology, security, or an identity issue. It's about the strategic alignment of the business roadmap and strategy with the relevant technology to support it.

Management intent and support will play a significant role in overcoming cultural barriers as Zero Trust brings about a fundamental change in the way organizations work and operate. The concept of "trust no one" is easy to understand but poses significant challenges to all internal and external stakeholders to implement, manage, and maintain at the strategic, tactical, and operational level.

Therefore, the implementation of Zero Trust must be driven and owned by the business areas, who need to define their critical systems, the entitlement rules to interact with those systems, together with the risk they are prepared to accept.

While not for the faint-hearted, adopting a Zero Trust philosophy and architecture enables the delivery of the capability an organization requires in a cost-effective, frictionless manner with an understood level of risk, aligned to business needs.

Appendix 1
Zero Trust Strategies and High-Level Methodology

When developing a Zero Trust strategy it is important to keep in mind that the aim is to align any IT and Security strategy with the business strategy.

It is also key to critically think about what having "no limitations" (or at least minimal controls) would enable your business to do. This is akin to the Google/BeyondCorp model of *"We treat every network in the world as untrusted, whether it's physically inside our building, [or] whether you're at a Starbucks"*; therefore, it follows that the reverse is true and everyone should be able to use our organization's network as if they were in Starbucks.

Such a change in thinking can enable (not an exhaustive list);

- Widespread use of bring-your-own-device (BYOD).
- External consultants, joint ventures, partners, etc. being able to use their own corporate laptop when working and connecting to your systems.
- Partners and outsourced services being able to connect their own infrastructure onto your organization's network.
- The use of public 5G mobile networks.
- The adoption of a "diverse Internet" strategy, leveraging multiple lower-cost public connections to the Internet.
- The widespread use of IIoT and IoT[13] devices (many probably utilizing 5G mobile networks).
- The adoption of ICS/Industry 4.0
- M&A - accelerate time to value without having to interconnect disparate corporate networks.
- Application transformation - migrate apps from datacenter to cloud, or consolidate datacenters, without disrupting user experience.

Some organizations may choose to implement their zero trust strategy alongside an IPv6 strategy; thus, enabling all people, devices and organizations to directly connect to your systems (whether hosted internally or externally), all using the same security/access model. It also potentially enables a more robust global Internet strategy, as organizations with multiple sites can leverage a local Internet connection either standalone or in conjunction with a corporate WAN link to provide global connectivity and resilience.

13 IIoT = Industrial Internet of Things, IoT = Internet of Things (generally more consumer focused)

Critical Systems

Every organization has a set of critical systems and an associated set of data flows that the organization relies upon to conduct business. Identifying those systems in conjunction with the business itself allows a zero trust architecture to be developed (hopefully with common components) that allows a set of "entitlement" rules to be developed by which each system will allow access.

Entitlement/Authorization

Entitlement[14] or the rules that define the how, and by whom, resources can be accessed at an acceptable level of risk (remembering that risk is bidirectional and always asymmetric), should be driven by trusted attributes and other supplementary sources of inferred trust; facilitating the ability to derive context, and from that an entitlement decision.

Properly implemented, entitlement should continue into the application itself; for example, there is an acceptable level of risk to let the device/person view their bank account, but not to transfer any money; and for this some level of step-up authentication may be required.

Entitlement, context and risk-based access can also enable more frictionless access to systems and data for all users.

For all elements used in an entitlement decision it is critical to factor in who/what is truly authoritative for the attribute/data you are consuming to make the decision.

Context

Context comes in two forms; asserted context and inferred context.

- Asserted Context is typically the digitally signed join of two entities - here is my assertion that I am a corporate laptop, signed by the corporation that owns it, asserted by the laptop. (The join of "device" and "organization"); or I am John Doe, full time staff at Acme Corp. (the join of "person" and "organization").
- Inferred context is what can be gathered, usually by observation - this laptop's IP is based in Russia, or the last time this user tried to access this system they were geolocated to Corporate HQ, but ten minutes later they are in Bulgaria.

Understanding context, and having systems in place that can provide the attributes to enable an entitlement system/engine to derive contextual access decisions will be critical to success.

14 See also: CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 - Domain 12: Identity, Entitlement, and Access Management (cloudsecurityalliance.org/download/securityguidance-v4)

Governance and oversight

Any Zero Trust initiative within an organization must have an appropriate governance model, oversight board, steering committee and executive sponsorship. Implementing a Zero Trust model has the potential to disrupt every network, system, and way of working and thus the governance must be in place to ensure the business fully understands and is "on-board" with the changes.

Appendix 2
Building Your Roadmap Towards Zero Trust

The board and senior management understand the language of dollars and risk. It is imperative that the organization deploys personnel who can translate the technical language and advantages of a Zero Trust journey into a business one.

In building a roadmap to Zero Trust the key steps should be as follows:

1. Ensure business leaders understand the need and benefits of implementing a Zero Trust philosophy - most businesses will appoint a business-led steering committee.
2. Understanding of the current environment can be a good starting point; assessment is key in understanding the "as is" posture of an organization.
3. Work with the business to understand their short, medium- and longer-term strategic roadmaps for their business areas. These need to be aligned with the security vision, mission, and culture of the organization.
4. Work with the business to determine the critical systems and assets for the business; and with the business owners for those systems to understand the risk and the future strategic plan for those systems/assets.
5. Map and understand the service architecture and data flows.
6. Map and identify the entities involved (people, devices, organizations, code, and agents).
7. Challenge business assumptions about what could be possible and evangelize what Zero Trust could enable (remember: business leaders have been brought up in a "perimeterized" mind-set too).
8. Run risk-workshops (joint IT, Security and Business) to define the acceptable risk thresholds for the key systems and assets.
9. Publish the results into a set of requirements for all key systems together with an overview of the high-level technology strategy.
10. Work with Zero Trust architects to define a set of technology solutions to deliver on the strategy.
11. Review with the business and iterate as required.
12. Develop a roadmap to get from where you are today, to where you want to be tomorrow
13. Implement an appropriate Zero Trust Maturity Model to validate your maturity at each phase of the roadmap.

Fundamental principles

- Zero Trust is not a "project," nor is it a product; it's a journey of continuous evolution.
- All assumptions need to be challenged. The 4 "Ws" and 1 "H": What, Why, Where, When, and How can be helpful; ask why you need this and the benefit it brings.

- Keep it really simple, complexity costs, rarely works or scales and is certainly not conducive to a frictionless business environment
- Remember, Humans are often the first, middle and last line of defense. Zero -trust is not about "technology only".
- Remember to start small and take incremental steps.
- Remember your Zero Trust strategy should constantly provide a "return on value" and "assurance" to the business owners.
- Do the basics well, and select "quick wins"?
- Plan to upgrade/enhance systems at their natural refresh time where possible
- The final goal should and always be to reduce residual business risk to an acceptable level.
- Have a separate strategy for legacy, don't let the legacy problem drive your strategy.

Remember that there is no such thing as a Zero Trust solution; your strategy will be unique, comprising multiple solutions, and should be a continual evolution of IT, Networking and Security to better support business-led computing.

The challenges of a Zero Trust philosophy

Unless your organization is starting from a "green-field"; or you have the level of business mandate to "rip-and-replace" virtually every system and network component, the challenge of an established organization to move to a fully Zero Trust architecture should not be underestimated.

Mistakes

- Trying to shore-up (or worse, replicate) an existing perimeter-based model using Zero Trust components.
- Thinking of Zero Trust as a "Network" or "Intranet" or "Security" problem.
- Trying to "boil the ocean" and verify everything - a risk-based approach is essential.
- Using VPN technology for anything other than a transition tool for specific legacy use cases.

Trust

- The challenge is identifying effective and efficient solutions for establishing trust[15] with entities that are not under your direct control.
- The opposite of this is to get trapped by the "locus-of-control" problem – "we can only make this work because everything is in a system under our control."

15 Botsman, Rachel. "Who Can You Trust? How Technology Brought Us Together – and Why It Could Drive Us Apart" Penguin Books Limited, 2017, 5 October 2017 ISBN-10: 9780241296189 ISBN-13: 978-0241296189

Identity

- For most organizations, federation promises much and delivers a nightmare of complexity and custom technological solutions. Instead, look at solutions that simply allow consuming trusted (signed) attributes that can be consumed by the entitlement engine.
- Understand the attributes of an entity for which your organization is truly authoritative, and understand from where (and how) you will consume those attributes.

Legacy

- Legacy can mean legacy! It's often not viable to fix and you need a workaround to mitigate the risk of operating legacy (and probably vulnerable) systems in a Zero Trust environment.
- Proceed with caution, have a plan and an agreed upgrade path for a Zero Trust compliant solution.
- Segmentation and micro-segmentation of flat networks is a path strewn with risk, and while it may be viable to segregate legacy systems, only do it when absolutely necessary - and have a plan for removing it.

Cloud

- Cloud migration is both an opportunity and a risk.
- Avoid the "lift and shift" of an on-premises (perimeterized and managed in-house) solution and architecture simply to replicate the architecture in cloud hosting, especially in the name of Zero Trustzero trust. Cloud requires a cloud specific architecture that dovetails with your zero trust architecture and ideally finding Zero Trust solutions flexible enough to comprehensively integrate with both cloud and on-premise solutions, as well as hybrid and multi-cloud deployments.

Monitoring and observability

- TLSv1.3 and other properly encrypted protocols are not conducive to monitoring, where possible instrument the end-points, the application and the data–not the network or network gateways.
- Avoid encapsulating traffic, especially using VPNs, as it limits the ability to derive context and thus understand risk.
- Adopt threat modeling approaches to idenjtify instrumentation requirements.

Privacy

- Many current approaches to Zero Trust appear to the end user as a violation of privacy, where the right to gain access is granted only by agreeing to be monitored, or access only allowed by installing a corporate app/program on their Bring Your Own Device (BYOD).

Interoperation and vendor lock-in

- Leverage standards wherever possible to ensure interoperation not only with your own disparate systems, but also with the collaborating external parties.
- Critically assess vendor solutions for the level of interoperability they offer to avoid the "locus-of-control" trap.

Appendix 3

Zero Trust Architecture and Other Frameworks

- NIST SP 800-207 - Zero Trust Architecture
  https://csrc.nist.gov/publications/detail/sp/800-207/final
- CISA - Zero Trust Maturity Model (Draft)
  https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf
- NCSC - Zero Trust architecture design principles
  https://www.ncsc.gov.uk/collection/zero trust-architecture
- Cloud Security Alliance work on Software Defined Perimeters (SDP)
- SDP Spec v1 Final
  https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-and-zero trust/
- SDP Architecture Guide
  https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/
- Cloud Security Alliance - Cloud Controls Matrix (CCM)
  https://cloudsecurityalliance.org/research/cloud-controls-matrix/
- Earning Trust in the 21st Century - CSA DC Chapter
  https://cloudsecurityalliance.org/artifacts/earning-trust-in-the-21st-century/
- ENISA - Cloud Computing Risk Assessment
  https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/@@download/fullReport