Fálaina Zero Trust Security

A practical approach to implement Zero Trust with Identity & Data Security

Sivachanthiran Belasamy
Founder & CEO

3 Jan 2022

fálaina

THE NEXT GENERATION IDENTITY AND ACCESS GOVERNANCE PLATFORM

Fálaina Zero Trust Security

A practical approach to implement Zero Trust with Fálaina Identity and Data Security solution

Ever-expanding attack surfaces are making conventional castle-and-moat cybersecurity models ineffective against continually evolving cyberthreats. Further, with trends like working from anywhere, digital transformations & cloud initiatives, and billions of newly connected endpoint devices, it is even harder to defend against this rising tide of threats.

Enter the notion of Zero Trust, based on the principle of “Never Trust, Always Verify”. Zero Trust is a security model based on the principle of maintaining strict access controls and not trusting anyone by default, even if these employees and non-employees are already inside your network. Zero Trust is gaining traction in enterprises where the defined perimeter is greying/ fading but every user, device, and network is inherently trusted.

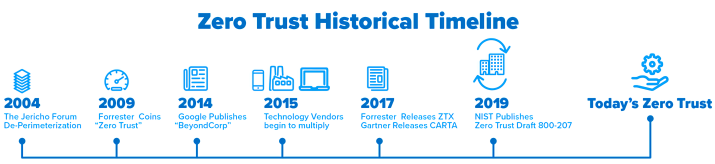
Adopting Zero Trust is a journey. It typically requires a shift in mindset driven by broader transformation efforts, along with an experienced guide who can help organisations take a holistic approach to cybersecurity in advance, rather than approaching it as an afterthought.

This involves establishing strong foundational capabilities across the five fundamental pillars of users, workloads, data, networks, and devices, and supporting them further with complete visibility, automation, and orchestration.

History of Zero Trust

It was in 2003 that the Jericho Forum, a security consortium, defined some of the earliest work on what we now call Zero-Trust. This is with the basic principle that we shouldn’t trust anyone or anything just because it’s inside the organisation’s perimeter.

Forrester later established the Zero-Trust model in 2011, which centred around the guiding principle “Never Trust, Always Verify”, and the recognition that perimeter firewalls are no longer sufficient to protect business secrets and assets.



Several organisations, such as Google and Microsoft, established methodologies to implement and operationalise it, but it has yet to be widely adopted till today. Now, the time has come to embrace Zero-Trust and learn the lessons from others who have been on this journey.

Other Zero Trust Terminologies:

- Zero Trust Network Access (ZTNA) - IT security solution that provides secure remote access to an organisation's applications, data, and services based on clearly defined access control policies.
- Zero Trust Architecture (ZTA) - an architecture based on the principle that nothing can be trusted. Under this philosophy, no device, user, or application attempting to interact with your architecture can be assumed to be secure.

fálaina

Why is Zero Trust Important?

As much as we have been seeing an increase in security breaches and attacks, 2020 has made it apparent that organisations everywhere are under attack more than ever before. Traditional perimeter security is no longer enough to defend against this rising tide of threats. Trends like an exploding number of connected devices, work from anywhere, and supply chain vulnerabilities are the presiding factors that push business leaders and cybersecurity practitioners towards Zero Trust journey.

- Volume and Diversity of Devices - Networks today are being overwhelmed by the sheer volume and diversity of devices: mobile/ IoT devices, laptops, operational technology, and systems, with billions of devices connecting every year to enterprise networks around the world. Cumulatively, Gartner predicts there will be 25 billion devices connected around the world by the end of 2021, many of which will be reconnecting to the office after an extended absence during work from home.

  With the right Zero Trust tools, business and security leaders will be able to have full visibility into the landscape of the devices, as well as the users behind each of these devices, to implement proper authentication and access control.

- Digital Transformation & Cloud initiatives - Organisations are embracing digital transformation to manage continuous business environment changes, and shifting their business models based on the supply chain demands and technology trends. Jumping onto the cloud bandwagon is becoming a natural progression in today's digital transformation strategy, but the old way of security does not provide business agility, user experiences, and protections needed for a rapidly evolving cloud platform.

  As part of digital transformation and cloud initiatives, cybersecurity is now becoming the strategic driver for growth, along with regulatory requirements and compliance mandates. Zero Trust is among one of the top concepts being looked at to address all these challenges, but many enterprises still have a long way to go.

- Work from Anywhere - The rapid shift to working remotely due to the covid-19 pandemic has forced companies around the world to improve their security tools and processes. On top of that, devices that were once kept inside of the corporate office are now connecting from the home. However, this is more than just a short-term shift as an increasing number of companies are considering making the transition to remote work permanent.

  While many devices may never even touch a corporate resource, even as they gain necessary access to critical assets and networks, perimeter security defences that default to high trust levels on the internal network are ill-suited for this remote enterprise world.

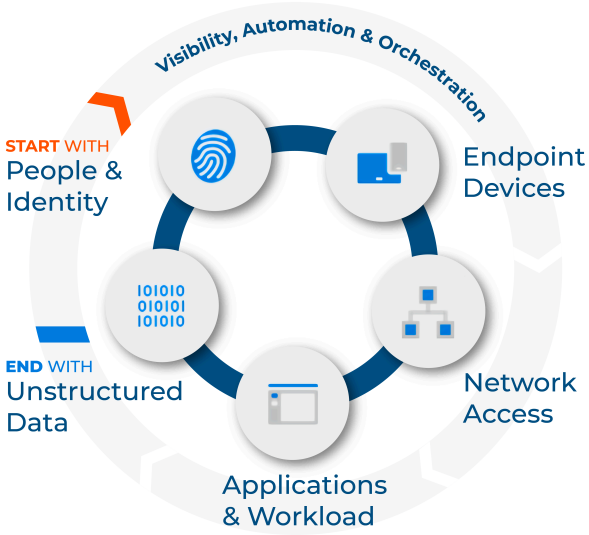
  Zero Trust allows organisations to implement continuous assessment and enforcement against 100% of these remote devices connecting to their corporate networks and automate control implementation across heterogeneous networks.

Fálaina Zero Trust Technology Pillars and Guiding Principles

Enterprises need a new security model that effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects:

- Identity
- Endpoint Devices
- Network Access
- Infrastructure
- Applications
- Data

This is the core of Zero Trust. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model verifies every request from any device or network. Regardless of who the request originates from or what resource they access, the Zero Trust model tells us to "Never Trust, Always Verify". This journey starts with identity and end with data.



Identity

Identities, representing people such as workforce (employees and remote employees), vendors, and contractors, using unique identities with differing access privileges is one of the least mature domains. In the Zero Trust security model, they function as most powerful, flexible, and granular way to control access to data. Identity and password is also one of the top vectors for attacks or breaches.

Before you attempt to administer identity and their accesses (from devices) to network, applications, infrastructure, and data, you need to first have complete visibility around who has access to what.

Zero Trust Identity key use cases include:

- Identity and Entitlement Catalogue - Complete visibility on identities and their entitlements is important before embarking on a Zero Trust journey. This information also provides insights into the risk element of an identity across the enterprise

- User Access Rights Review - Also called access certification or attestation, this process allows identities and their access to be reviewed regularly automatically via a campaign. The reviews include regular access to critical applications, access to roles with conflicting access or with sensitive access and also privileged access.

- Automated User Lifecycle Management - Automated user lifecycle management enables organisations to have a structured process with policies to ensure that least privilege access is provisioned to employees and non-employees. Timely de-provisioning not only removes unwanted access, but also reduces attack surfaces with stolen credentials.

- Least Privilege Access - Least privilege access is achievable through regular access rights reviews and granting least access as part of birth right access for regular users. As for privileged users, this is done by vaulting privileged credentials and allowing usage based on access request and approval only.

- Password Management - As part of Zero Trust, the best recommendation is to retire the use of password and enforce 2FA/ MFA across all access for all users. As for privileged users, regular password rotation or password rotation at the end of every privileged session is recommended.

Endpoint Devices

Every enterprise today has heterogeneous endpoints accessing applications and data. Enterprises today are either not managing or not owning these endpoint devices – they are mostly on different platforms, operating systems, and patch levels. This creates a massive attack surface and, if left unresolved, accessing work data from untrusted endpoints can easily become the weakest link in your Zero Trust security strategy.

Zero Trust adheres to the principle, "Never Trust, Always Verify". In terms of endpoints, that means always verifying all endpoints. This includes not only contractors, partners, and guest devices, but also apps and devices used by employees to access work data, regardless of device ownership.

Zero Trust Endpoint Device key use cases include:

- Endpoint Device Visibility - Complete visibility on endpoint devices is crucial before embarking on a Zero Trust Device journey. This is made possible by integration with Microsoft Active Directory Server and with endpoint devices joining Active Directory Domain. Mobile device registration for MFA authentication is mandatory as part of this Zero Trust policy. List of devices with their operating systems patch level are among information managed.

- Automated Device Lifecycle Management - Automated device lifecycle management enables organizations to have a structured process with policies to ensure that only authorised endpoint devices can access applications and data. As for MFA, self-service facility is provided for employees to register their devices. Timely de-provisioning and removal of these devices reduces attack surfaces.

- Enforce Zero Trust Network Access via VPN/NAC - Fálaina MFA and Radius Server helps to secure employee and non-employee access with MFA authentication from VPN/ NAC from self-service registration, workflow approval, authentication against Ms. Active Directory or Fálaina IDP, then accessing the corporate network or applications.

Network Access

The network perimeter has not disappeared, but instead has evolved over time, especially with on-premise applications moving to SaaS platforms and hybrid environments. Thus, it is important to Administer, Authenticate, Authorize and Audit access at segmentation boundaries within each network segmentation, and secure access to your network from network login (VPN/NAC) all the way to your applications.

Access management (AM) tools integrate to provide authentication and identity context to Zero Trust network access (ZTNA) tools and are best positioned today to provide contextual based access to web applications and SaaS applications for all user types. ZTNA is best positioned today as a VPN replacement to enable granular access policies for internal and B2B users to non-web and web applications hosted in any environment.

Zero Trust Network Access (ZTNA) key use cases include:

- Endpoint Device Visibility - Complete visibility on endpoint devices is crucial before embarking on a Zero Trust Device journey. This is made possible by integration with Microsoft Active Directory Server and with endpoint devices joining Act

- Web Application Access via Web Single Sign-On (WSSO) - WSSO tools provide real-time access through robust adaptive access controls, centralized authentication, authorization enforcement and single sign-on to on-premise and cloud applications/ services for both employees and non-employees

- VPN/Network Access - ZTNA technologies typically start with remote access, such as VPN or NAC. ZTNA requires an identity and access management system that integrates with identity providers to establish user and device authentication and attributes that are used as part of the ZTNA access security policy. This is also supported for non-employee self-service registration, workflow approval, authentication against Ms. Active Directory or Fálaina IDP, then accessing the corporate network or applications.

Applications & Workloads

Rapid adoption of cloud platforms and the new models of computing that support rapid application development have made workload security an urgent area to mature. Enterprises need to ensure both on-premise application and cloud workload security are implemented with the right balance of access while maintaining control to protect critical data. Also, there is a need to control access via APIs.

Zero Trust for applications and workloads enables you to define the way you want users to behave in these environments. This can be done by creating policies, which allow you to implement appropriate in-app permissions, detect risky behaviour, violations, and suspicious data points and activities in these environments.

Zero Trust for Workloads key use cases include:

- Applications and Workload Access Rights Management - User and access rights management can be implemented to ensure end-to-end security management from administration, authentication, and monitoring. Visibility across who has access to what is equally important for applications and workload security.

- Secure Privileged Session - Applications and workload privileged users' access can be secured and controlled via Privileged Access Management (PAM), with secure session and remote monitoring. All access to applications and workloads will be granted based on access request and approval.

- Credential Vaulting - Zero Trust for applications and workload suggests that all privileged credentials are to be vaulted and used only when required. These credentials can be retrieved based on access requests and approvals as and when required via appropriate security policies implemented via credential vaults or PAM solutions.

- Step-up Authentication (MFA) for Privileged Access - Privileged access to all applications and workloads typically requires approvals from systems or business owners. Once approval is granted, step-up authentication (MFA) is typically required to ensure secure access. By using step-up authentication with MFA, attack surfaces can be greatly reduced.

Unstructured Data

Data should remain protected while at rest, in use, and when it leaves the endpoints, apps, infrastructures, and networks that are within the control of the organization.

To ensure protection and that data access is restricted to authorized users only, data should be inventoried, and access should be granted via access request and approval and periodically reviewed by the data/ business owner.

If there is insufficient knowledge about what sensitive data you have on-premises and in cloud services, you cannot adequately protect it. Thus, it is necessary to discover data across your entire organisation and classify all data by sensitivity level. It is also important to understand where it resides, whether on-premise or in the cloud, and available security options.

Zero Trust for Unstructured Data key use cases include:

- Unstructured Data Access Catalogue - Complete visibility on who has access to unstructured data is important before embarking on a Zero Trust journey. Discovery of all folders and files is done regularly to ensure complete understanding of data and its landscape. Other information includes duplicate files, dormant files, and ghost files.

- Data Access Rights Review - This process allows unstructured data access to be automatically reviewed regularly via a campaign. The review includes access to folder and files in Ms. Windows File Server and SharePoint Server.

- Data Access Request and Approval - With Zero Trust for unstructured data, all access to data can be governed and controlled with access request and approval mechanisms. This will not only provide records of who has access to what, but also the ability to remove access in a timely manner with a centralized record.

Fálaina Zero Trust Technology Pillars and Guiding Principles

The table below describes Fálaina's key technology capabilities that allow enterprises to start their Zero Trust initiatives starting with Identity and end with Unstructured Data.

Identity Governance & Administration		Privileged Access Management	Unstructured Data Access Governance	Access Management	
Identity Administration (Provisioning)	Access Governance (& Compliance)			Web Access Manager (WebSSO)	Multi-Factor Authentication (MFA)
1. Automated workforce identity lifecycle management 2. Access Request & Approval 3. Password Management	4. Entitlement Catalogue 5. User Access Rights Review 6. SoD & Sensitive Access Checks	7. Credential Vaulting 8. Secure Privileged Session 9. Step-up Authentication for Privileged Access	10. Inventory of data (documents) 11. Data Access Rights Review 12. Access Request & Approval for Data	13. Centralised & secure authentication 14. Step-up Authentication for Privileged Access 15. Support on-premise legacy web app, client/ server app and SaaS/ protocol based SSO	16. Integrated MFA and IGA mobile app 17. Variety of MFA authentication options 18. Support Radius server for secure ZTNA implementation

Benefits of Zero Trust with Fálaina Integrated Identity & Data Security

The Zero Trust model moves from perimeter security deployment to identity and data security, dynamically securing user experience end to end. This approach to security minimises exposure and increases compliance by securing identity and data for all users.

In addition, other benefits of Zero Trust include:

- No gaps left behind by covering the broadest range of attack surfaces, ranging from identity, endpoint devices, applications and workloads, network, and data.
- Organisations are able to increase agility through secure adoption of cloud and mobile solutions
- Framework provided to properly manage the risk of exposure for sensitive apps and infrastructures within and outside company network.
- Complete visibility of risk in users' access controls across all systems
- Less management, skills, and costs required compared to silos of patchwork security

About Fálaina

Fálaina is a technology provider of Identity and Access Management solutions. Fálaina enables enterprises to have visibility and secure their infrastructures, applications and data for private and public cloud. Fálaina comprehensive solution addresses today's requirements of an enterprise for:

- Identity Governance and Administration (IGA)
- Data Access Governance (DAG)
- Access Management (AM)

It provides businesses with the relevant reporting and analytics to improve IT security, maintain compliance and eventually minimise business risk.

To learn how Fálaina can help your business, visit www.Fálainacloud.com,
or email us at sales@Fálainacloud.com.

fálaina