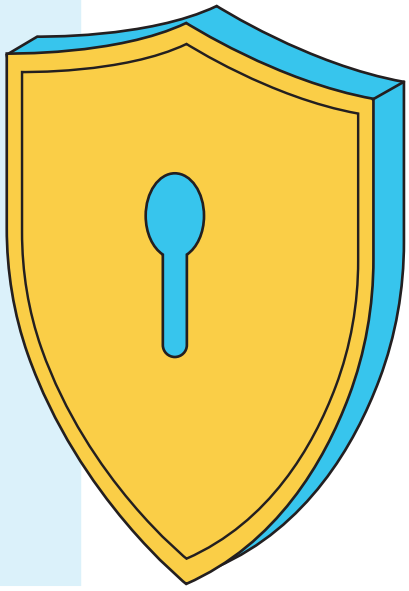
Achieving Zero Trust

ManageEngine's Path to Upgrading Cybersecurity

WHAT'S INSIDE?



Glossary

Abbreviation	Stands for
DLP	Data loss prevention
MFA	Multi-factor authentication
MDM	Mobile device manager
2FA	Two-factor authentication
UEBA	User and entity behavior analytics
ZTA	Zero Trust architecture
ZTNA	Zero Trust network access
ZTAA	Zero Trust application access
ZTDA	Zero Trust data access

Introduction

“Knock knock.”

“Who’s there?”

Even knock-knock jokes have verification! How about you? Would you welcome a stranger into your home without verification? You would probably look through the peephole. You would open the door and ask them who they are, based on which you would decide how much access they can have. A delivery agent stops at your porch. A plumber can enter your kitchen to fix the sink. A house sitter can enter all the rooms, but you would keep the closet with your valuables locked. Similarly, organizations have multiple layers of security covering everything from entering the network to accessing files. All of this is facilitated by the guiding principles we refer to as Zero Trust.

Who is this e-book for?

Zero Trust may seem intimidating without the right guidance. If your organization is stepping into this ocean now, this e-book is for you. We will start with ManageEngine's ongoing experiences and work our way to mapping out what you can do as an IT leader for your organization.

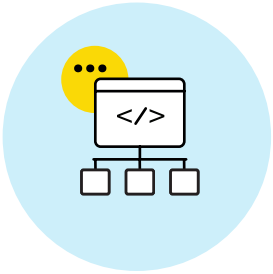
> (Zero Trust) addresses the agile needs of modern organizations and eventually it will become the way any security framework is (built).
>
> **From a business option to a business imperative, every one of us is on a Zero Trust journey-whether we know it or not.**

Rajesh Ganesan, President

ManageEngine

In this e-book, we will elaborate on:

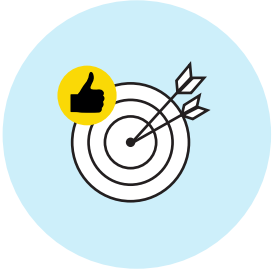
Zero Trust:
what it is and what it is not.



A framework you can implement without tearing your existing system apart.

ManageEngine's
Zero Trust plan.

Real-life use cases.



Challenges and
best practices.

Chapter 1

Self-Assessment to Get Started

1.1 What is Zero Trust?

Zero Trust is more than just a buzzword. It is the next step in cybersecurity. In the last decade, there has been an uptick in the number of security incidents organizations face due to internal and external threats. In ManageEngine's 2021 Digital Readiness Survey, we deduced that phishing, network endpoint attacks, and malware were the most prominent security threats, yet only 26% of organizations have opted for Zero Trust network implementation. Zero Trust is no longer an option. It is an imperative. At ManageEngine, we have started implementing Zero Trust in our network to give ourselves an extra shield against these preventable attacks.

Zero Trust stands on three principles

01. The principle of least privilege:

Also referred to as the principle of least authority, this is the practice of limiting user access to resources by providing just enough authorization for a member to carry out their tasks. It is also applicable to systems, processes, devices, and applications that request authorization.

02. Never trust, always verify:

Implicit trust has always been a point of vulnerability in security. We know that we cannot blindly trust everyone within a network. With Zero Trust, we reduce the implicit trust zone and enforce continuous explicit verification.

03. Assume breach:

This is one of the few areas where being a pessimist helps: assume a breach has occurred or is occurring at all times. Microsegmentation allows you to control the affected radius and prevent the breach from spreading.

1.2 Debunking the myths

Myth 01
Zero Trust is a product

Fact:

Zero Trust is not a single solution that you can purchase. On the contrary, it is a framework or set of principles to guide organizations to make better security choices and protect themselves from breaches. However, vendors can offer multiple tools, like user authentication, that can be integrated to support Zero Trust in a network.

Myth 02
A good strategy needs to start from scratch

Fact:

Google's BeyondCorp had to take apart and rebuild its entire network architecture to incorporate Zero Trust, but you do not have to do this. Enhance your existing network with a step-by-step approach. You can use a password manager tool, real-time auditing and monitoring, and multi-factor authentication (MFA) as a first step.

Myth 03

It really means "never trust (your employees), always verify"

Fact:

Security is not personal. Trusting that everyone inside your organization has good intentions is a vulnerability. Attackers can be within or without an organization, and your job as an IT leader is to always keep information secure. However, this does not mean employees must always be treated like threats. User and entity behavior analytics (UEBA) can be used to assign trust scores based on several parameters and to grant users personalized access.

Myth 04

Zero Trust is for large enterprises

Fact:

You do not need to burn a hole in your pocket or run a multinational corporation to introduce Zero Trust. BeyondCorp created a misconception that Zero Trust is expensive and time-consuming. That is only because it had to create something that did not exist before. SMBs, on the other hand, can now get started on their Zero Trust journeys with the simple tools that are available. In fact, you will save money on operational costs in the long run. Let us not forget that cyberattacks are not selective—they can happen to anyone. It makes more sense to spend a bit to protect your data than to pay hefty fines for non-compliance and damage control.

Myth 05
It only works on-premises

Fact:

Over the last few years, we have seen tremendous growth in organizations adopting cloud-based solutions and moving to cloud or hybrid environments. Likewise, Zero Trust implemented on-site can be extended to cloud solutions with cloud-based security approaches.

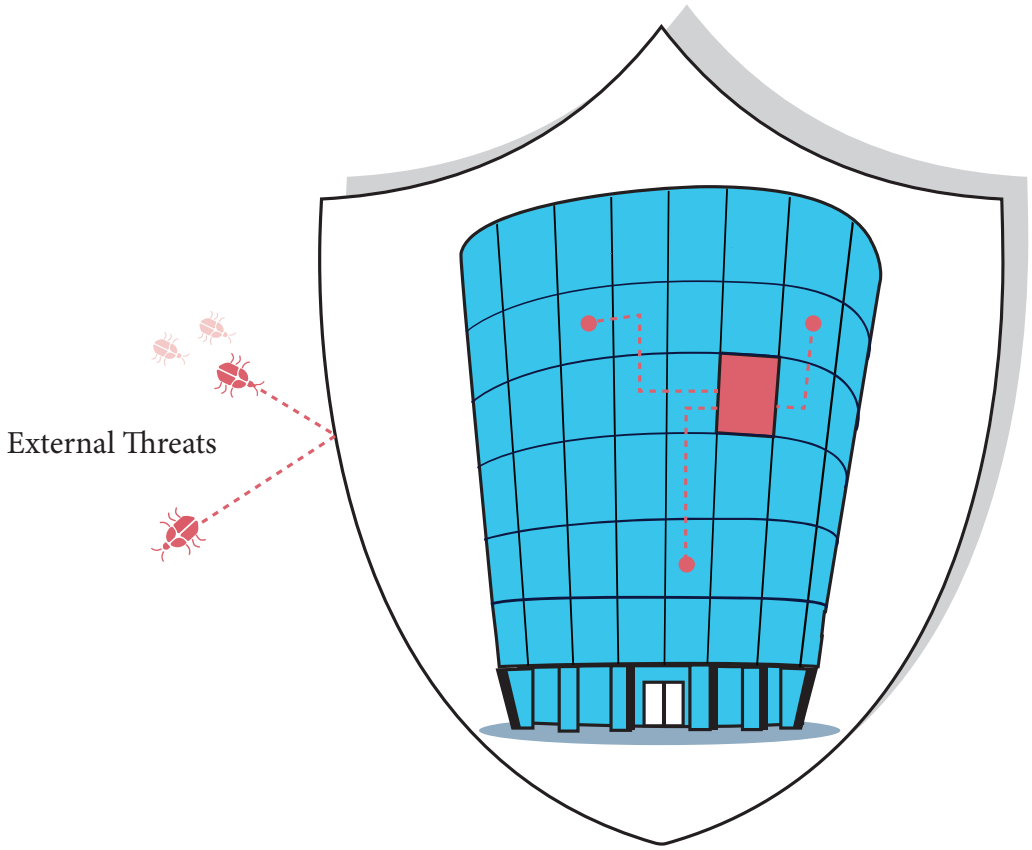
Myth 06
The user experience and productivity will suffer

Fact:

It might seem like a hassle to limit access and verify identities with each session, but with the right tools, workflows, and policies, it is possible to provide a user-friendly experience. Studying user behavior allows us to eliminate authentication requests for low-risk profiles and lessen wait times consistently. Additionally, Zero Trust increases productivity on the admin side. Once an employee leaves the organization, it automatically ensures they do not have access to any resources. There is no room for manual error. The admin team can focus on other critical tasks instead.

1.3 Assessing ManageEngine's security model

The traditional castle-and-moat model works under the assumption that everyone within a network is trusted. It weeds out external threats and vulnerabilities but does not account for the internal users or devices. That was the standard strategy for almost 20 years. Now, this is outdated.



The traditional perimeter-based security model

The perimeter-based security model worked when ManageEngine had employees working in the office every day. Access to information was granted through the corporate Wi-Fi only. Pre-pandemic, working from home was not mainstream yet. Apart from development teams and some remote employees, ManageEngine did not have a heavy requirement for the VPN. When the pandemic hit, everyone shifted to remote work. Simultaneously, we were hiring new employees for multiple teams.

At this point, ManageEngine faced five main challenges:

1.Capacity

There was an unprecedented surge in VPN users. We faced issues like slow performance and connectivity issues when using mobile data. Within a week, we had to block some non-work-related sites to optimize bandwidth.

2.Limited verification

VPN access was granted with just a username and password. Was this a safe way to verify user identity? Absolutely not. Even if one careless employee used a notes app to store their passwords or had a generic password like "ManageEngine123," we were vulnerable to attacks.

3.Visibility

VPN logs are not comprehensive, so we could not figure out who was accessing what, an essential capability on which we could not compromise.

4.Access control

We could not take privileges away from compromised devices or accounts. The burden then fell on the application itself.

5.Cost

During the pandemic, Zoho inaugurated over 30 spoke offices in India as a part of our rural revival initiative. Scaling up the VPN for all the spoke offices was expensive because we used a third-party service.

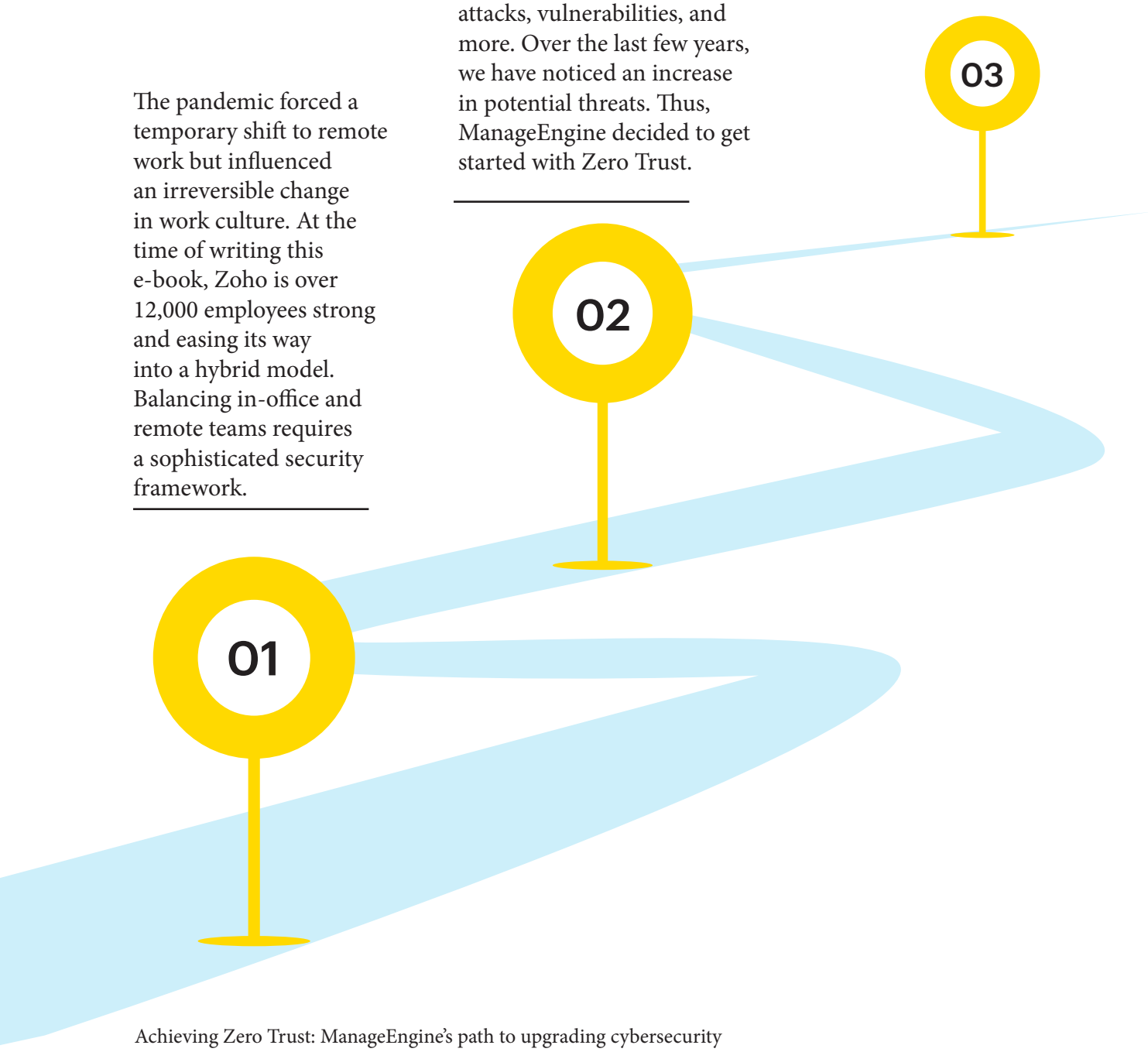
It became evident to the Admin team that it would have to step up its security to keep business moving as usual. Our Security team got to work—it was time to find a stronger alternative to the VPN.

1.4 Why did we decide to begin our Zero Trust journey now?

The pandemic forced a temporary shift to remote work but influenced an irreversible change in work culture. At the time of writing this e-book, Zoho is over 12,000 employees strong and easing its way into a hybrid model. Balancing in-office and remote teams requires a sophisticated security framework.

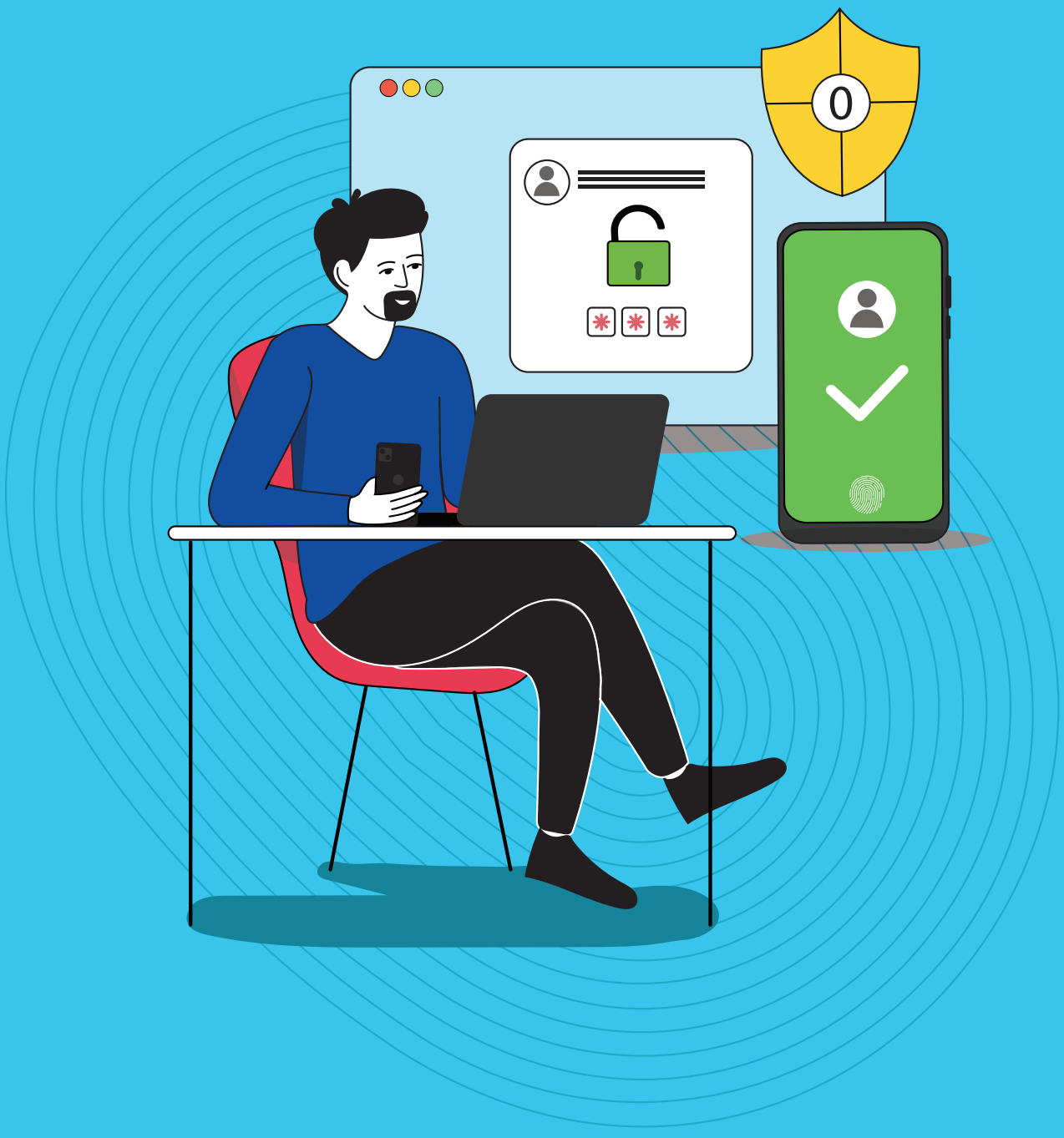
A successful enterprise is always the biggest target for cyberattacks. It is inevitable. It is at risk for ever-evolving external threats, insider attacks, vulnerabilities, and more. Over the last few years, we have noticed an increase in potential threats. Thus, ManageEngine decided to get started with Zero Trust.

Zero Trust is not infallible. There is still room for attacks, but Zero Trust is an additional form of protection in which every organization must invest.

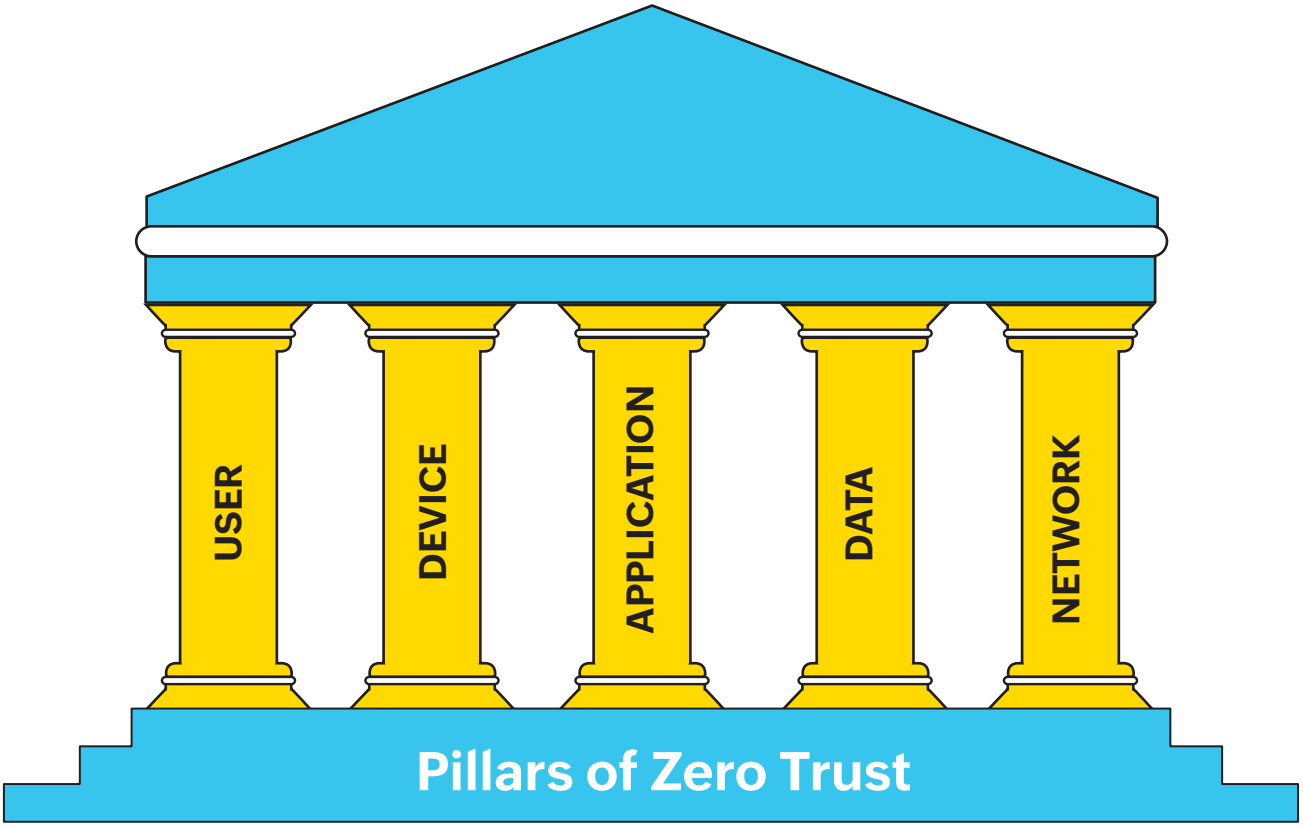


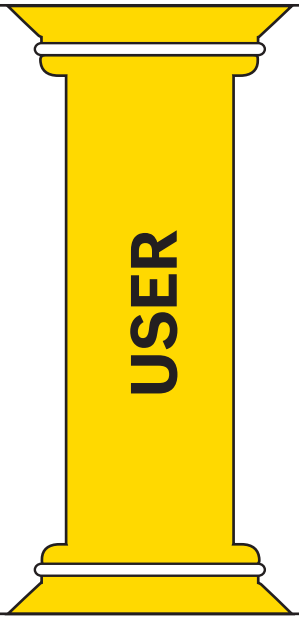
Chapter 2

ManageEngine's Zero Trust framework

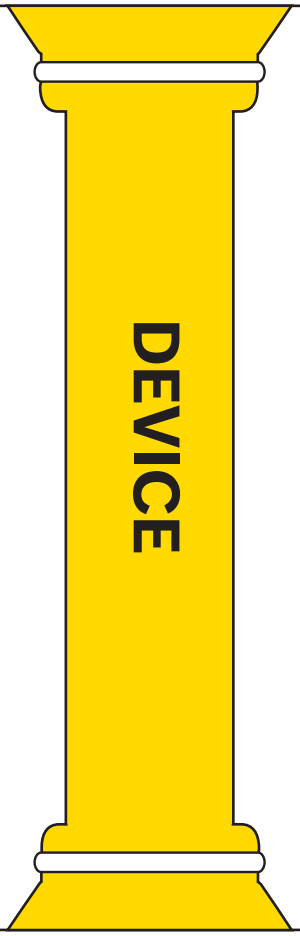


2.1 Pillars of Zero Trust





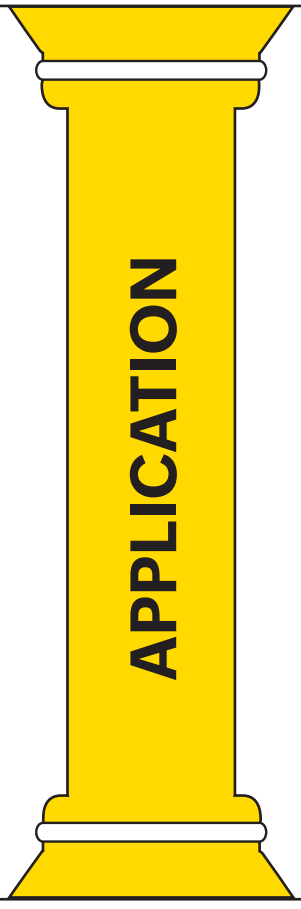
Authentication, authorization, and constant monitoring are our focus with user identity. We validate user trustworthiness to make decisions about privileges. Our Zero Trust system, known as 0Trust, maintains a list of employees and their departments by syncing with our HR tool. As employees join the company, change roles, or leave, these changes are reflected in the 0Trust system via webhooks. Employees are granted access to resources based on their roles. Identity providers help in the verification process by providing a list of users for the system to validate against.



As with user identity, devices must be verified each time there is an access request. At Zoho, we have over 12,000 employees, and each user has at least two devices. Zoho's 0Trust system maintains an inventory of these devices. Each device is uniquely identified by a certificate installed at the root level. Employees do not have root access. To identify connection requests from managed devices, we enforce a two-way SSL authentication, where the client and server validate each other's identities.

Devices are monitored via our unified endpoint management solution. Device verification relies on two things: risk assessments and data loss prevention (DLP). DLP solutions aim to secure data in all forms. This is achieved through these methods:

- File auditing and analysis: monitoring user activity in files and assessing vulnerability
- Data discovery and classification: locating and tagging sensitive data
- Endpoint DLP: monitoring data transfers



- **2FA**

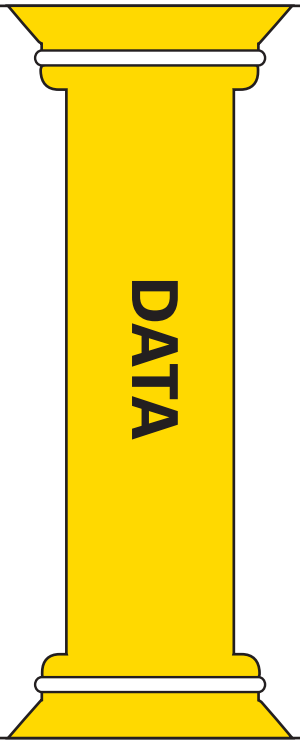
Using MFA tools like 2FA is one way to ensure employees have appropriate permissions and to prevent unauthorized access. The application layer depends on the user, device, and network data. To further secure identities, we are moving towards passwordless sign-in coupled with biometric verification for employees on our in-house MFA app.

- **SSO**

Employees have to authenticate themselves with both primary and secondary factors and will be assigned temporary tokens after authorization for access to specific resources.

- **CASB**

We monitor uploads and downloads on web apps and restrict the use of unauthorized shadow apps by validating them against allowlists, blocklists, and reputation scores.



Resources are identified, categorized, and encrypted from end to end. We then enable least privilege access for all organization data. Data can be classified based on purpose, confidentiality, and other factors..

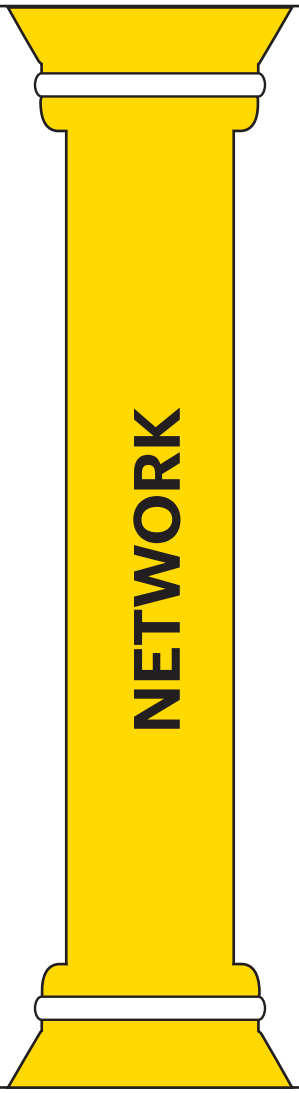
For example:

- **Purpose:**

Email should be accessible for all employees, whereas organizational policies and SOPs should be read-only with edit access restricted.

- **Confidentiality:**

Employee salaries, customer data, and product source codes are examples of data that should be restricted.



- **Microsegmentation:**

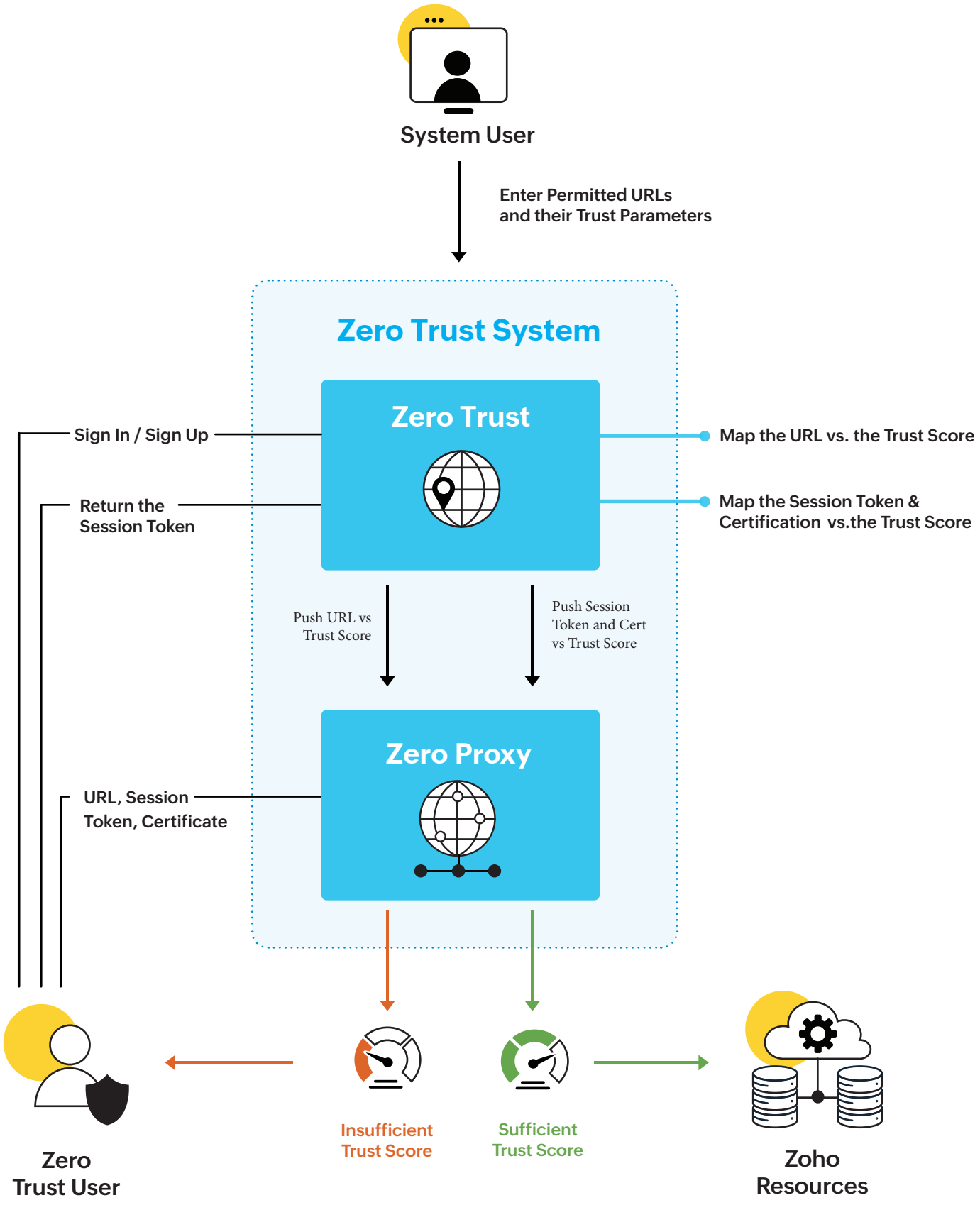
One of the advantages of Zero Trust is the ability to segment and monitor your network perimeter. Microsegmentation is the practice of breaking a large network down into smaller, isolated segments so businesses can monitor and control traffic easily.

- **0Proxy:**

0Proxy is an internet-facing reverse proxy. Traffic is always assumed to be from an untrusted network and is routed through the 0Proxy, which filters requests based on their associated trust scores.

- **Trust scores:**

A trust score system is used to evaluate if an individual should be granted access to the organization's network and data, and if so, how much. Admins can use a 0-1 or a 0-100 scale to rate the activities of each user, device, and network access request based on any number of parameters. At ManageEngine, we use a 0-100 scale to score each login.


System User
Enter Permitted URLs
and their Trust Parameters
Zero Trust System
Zero Trust
Sign In / Sign Up
Return the
Session Token
Map the URL vs. the Trust Score
Map the Session Token &
Certification vs.the Trust Score
Push URL vs
Trust Score
Push Session
Token and Cert
vs Trust Score
Zero Proxy
URL, Session
Token, Certificate
Insufficient
Trust Score
Sufficient
Trust Score
Zero
Trust User
Zoho
Resources

Network scoring system

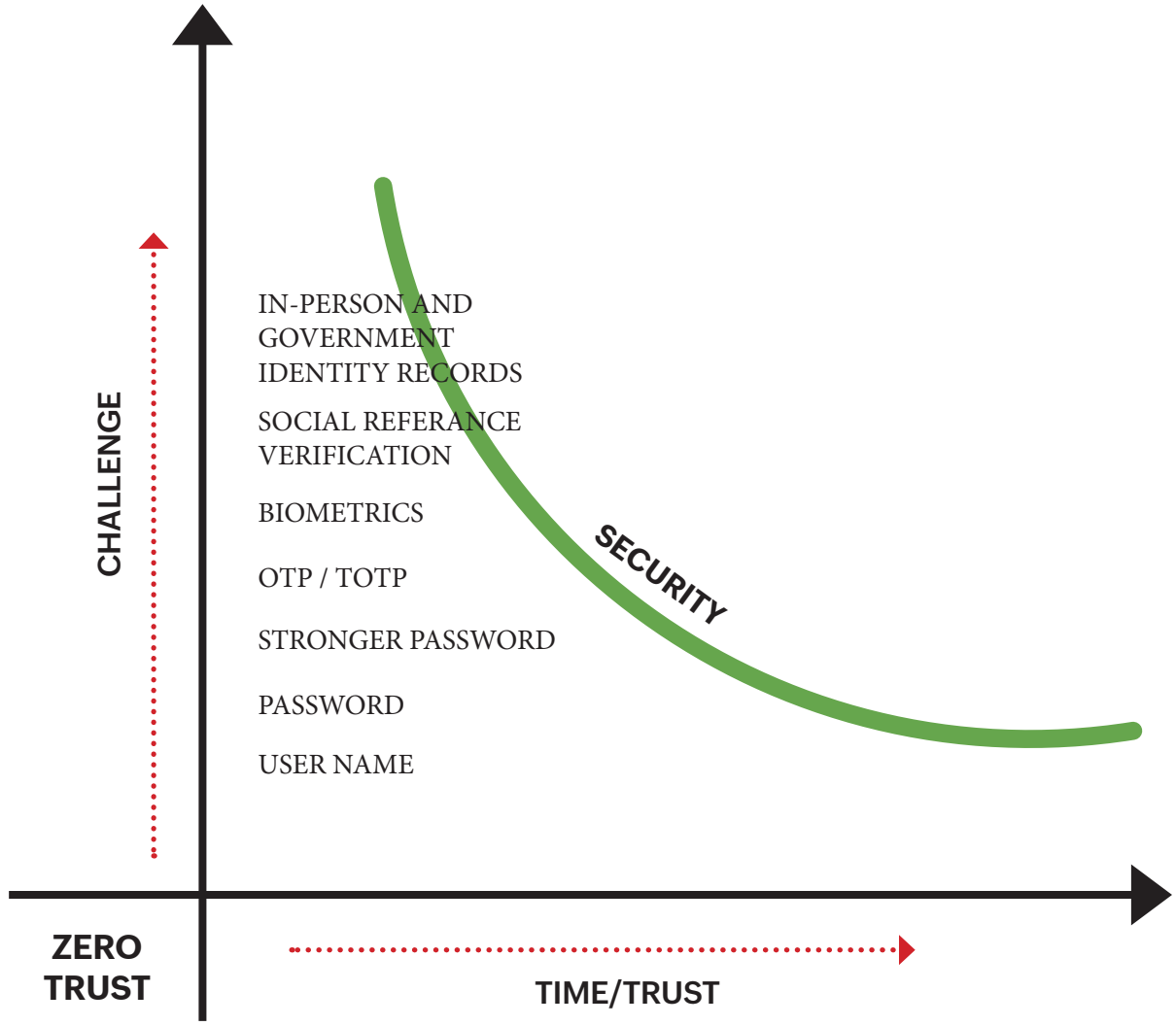
Parameter	Sample score
Trusted IP	40
Anonymous IP	30
Suspicious IP	30

User scoring system

Parameter	Sample score
Has no invalid sign-in attempts	30
Has non-breached credentials	30
Has no anomalous sign-in time	15
Has no anomalous sign-in location	11
Has no anomalous sign-in device	4
Has a good password strength	10

Device scoring system

Parameter	Sample score
Requires a password to unlock	10
Has a non-vulnerable OS version	10
Has no suspicious plug-ins, add-ons, or extensions	10
Has no suspicious applications or packages	10
Has no vulnerable application or package versions	10
Has no suspicious running processes or services	10
Has not visited any known vulnerable or suspicious sites	8
Jailbroken or rooted access is not available	8
Antivirus software is installed and running	6
Firewall is enabled	6
No listen ports are open	4
Secure boot is enabled	3
Driver integrity verification is enabled	3
Data storage is encrypted at rest	2



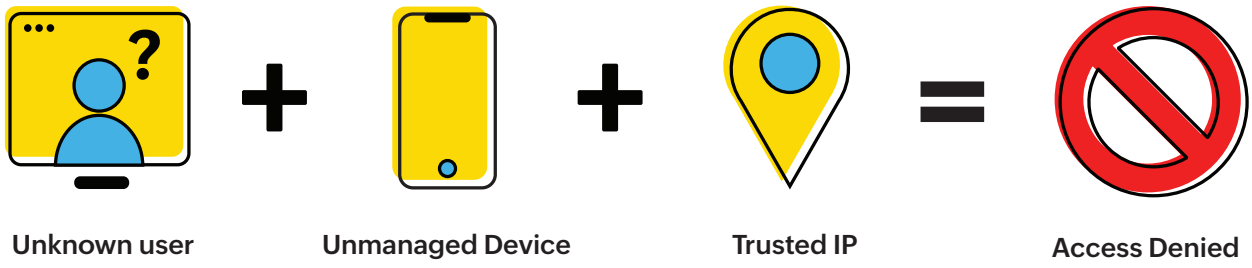
The level of access an employee is granted depends on the trust score allotted to each session, which is calculated based on factors like device, user, and time.

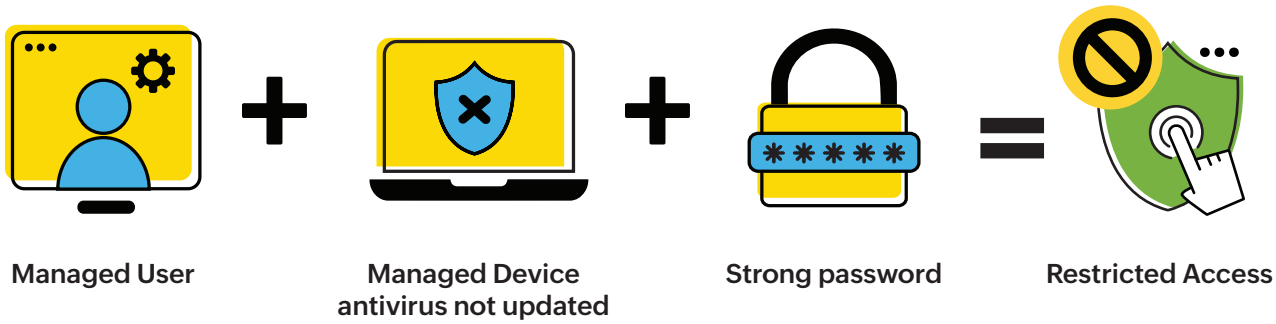
Device:
A managed device will have a higher trust score than an unmanaged device. This is influenced by parameters like its antivirus status, its location of access, and whether its OS has the latest patch.

User:
Role-based access is influenced by parameters like resources and the severity of authentication (such as biometrics or 2FA).

Time:
Trust scores are modified periodically based on the session time.

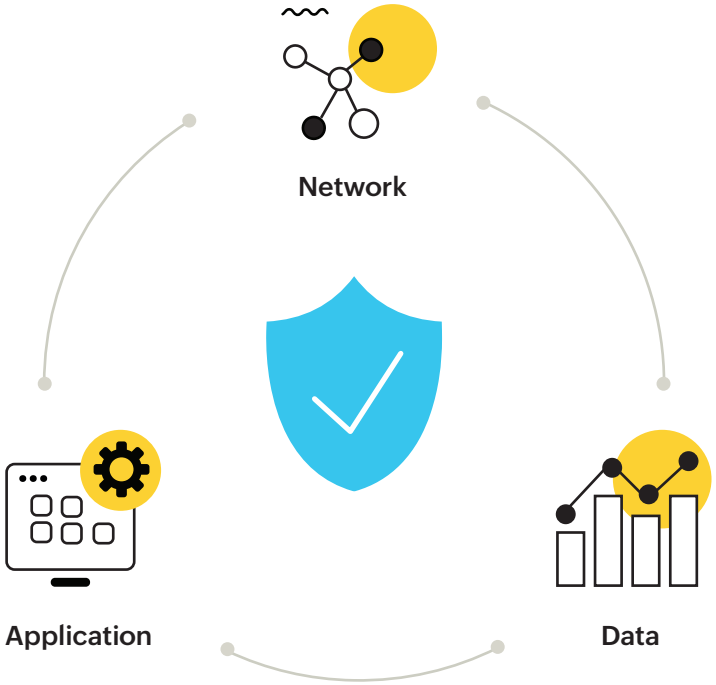
Even if the CEO uses a device that is not enrolled in the endpoint management tool, the access will be restricted to public data (i.e., the data that requires the minimal trust score of 10/100). In order to access sensitive financial information, the CEO has to use a company-owned device.





Access control based on trust score

2.2 Zero Trust vs. Zero Trust architecture: What is the difference?



Zero Trust and Zero Trust architecture are often used interchangeably. What do they mean, exactly? Zero Trust is an approach to security based on guiding principles. Zero Trust architecture is a broader concept that applies these principles to tackle three different security models:

- Zero Trust network access **(ZTNA)**
- Zero Trust data access **(ZTDA)**
- Zero Trust application access **(ZTAA)**

ZTNA	ZTAA	ZTDA
User-to-network connection	User-to-application connection	User-to-data connection
Can be considered an evolved replacement for a VPN that protects the network	Protects applications by enabling access only after user and device authentication	Restricts access to data until the user is provided authorization and their identity is verified

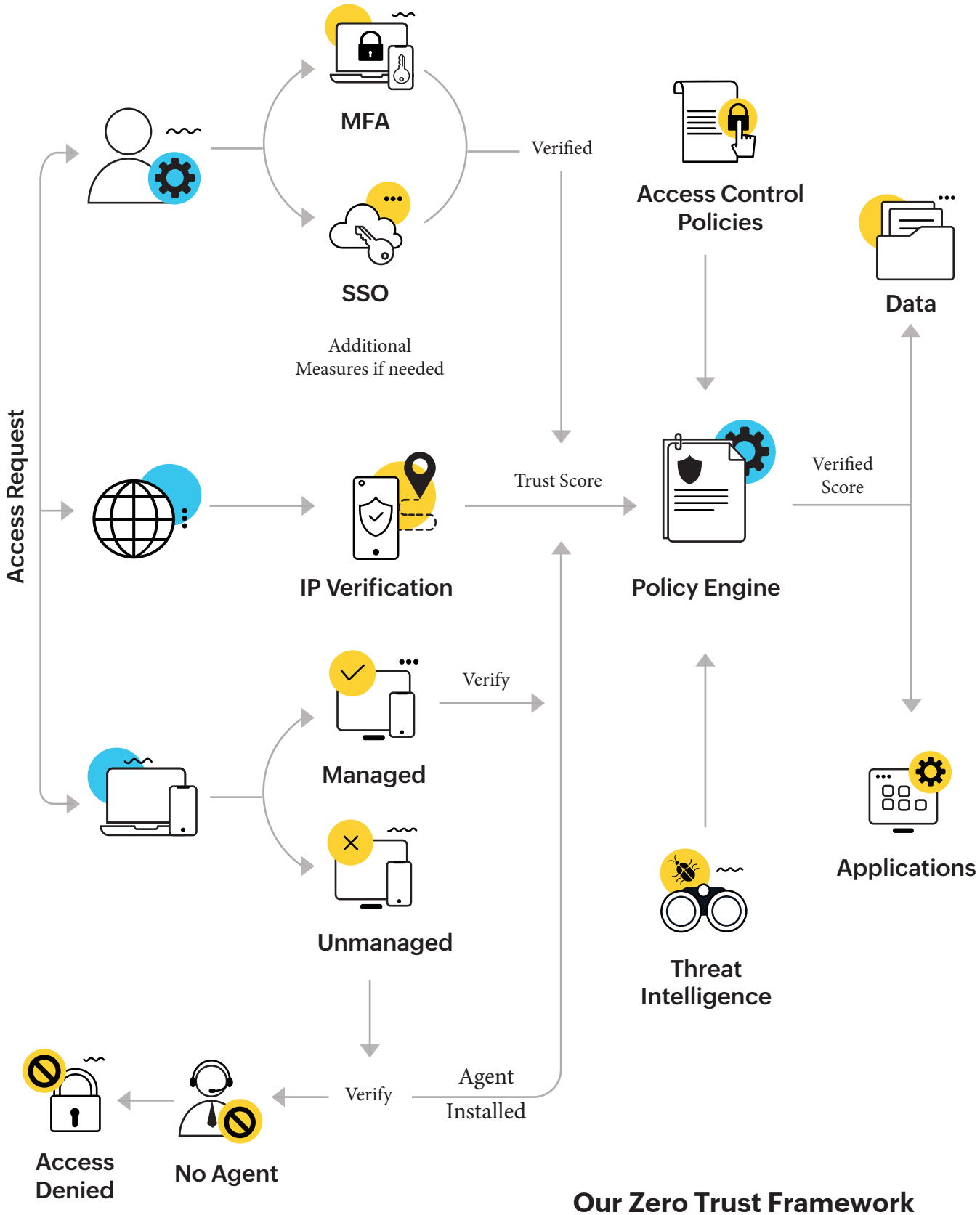
2.3 Migrating to Zero Trust

Speaking to our Zero Trust team gave us a better idea of our goals and roadmap. In the team's words, "Zero Trust is a front-end service, like a door that leads to a room. You can't rely on the door alone and not have walls. It's meaningless. Zero Trust is an additional security measure that should be combined with back-end securing services."

Our goals were to:

- Implement organization-wide Zero Trust.
- Rely on user and device identification.
- Make our verification parameters stricter.

Achieving these goals would take time, so we carried out our Zero Trust plan in phases.


MFA
SSO
Verified
Additional
Measures if needed
Access Control
Policies
Data
Access Request
IP Verification
Trust Score
Policy Engine
Verified
Score
Verify
Managed
Unmanaged
Applications
Threat
Intelligence
Verify
Agent
Installed
Access
Denied
No Agent
Our Zero Trust Framework

Phase 1

Objectives:

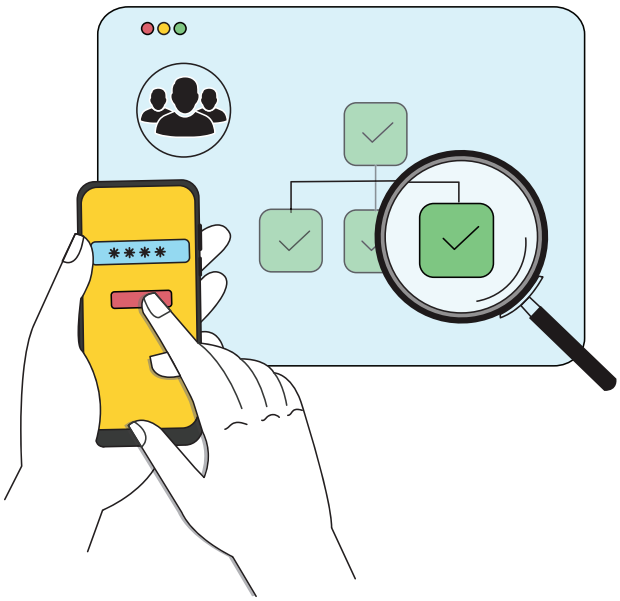
- Identify user groups based on their roles and required access.
- Identify network flows and try to capture all of them in 0Trust.

First, we established a device enrollment policy for employees:

1. Only company-owned devices should be used to access Zoho resources.
2. All devices should be enrolled first in our mobile device manager (MDM) solution (in the case of phones) and our unified endpoint management solution (in the case of laptops and desktops). This is to ensure that the devices are secured by default and monitored for vulnerabilities and potential hacking attempts.
3. Access to Zoho resources using devices that are not owned by Zoho should be avoided. Such access is restricted to resources that are public and definitely do not deal with customers and source repositories.
4. Employees who need root access for their devices will have access restricted to a non-production setup.
5. If a developer wants to access a production setup, they should use a different device for which they do not have root access. This is to ensure all controls are intact on the device that is used to access production setup.

In the early stages, resources were available via both the 0Proxy and the VPN externally and via both the 0Proxy and the corporate network internally. It was too early to abandon the VPN, but it was time for an upgrade. Instead of relying on the old username-password verification, we added 2FA and UEBA.

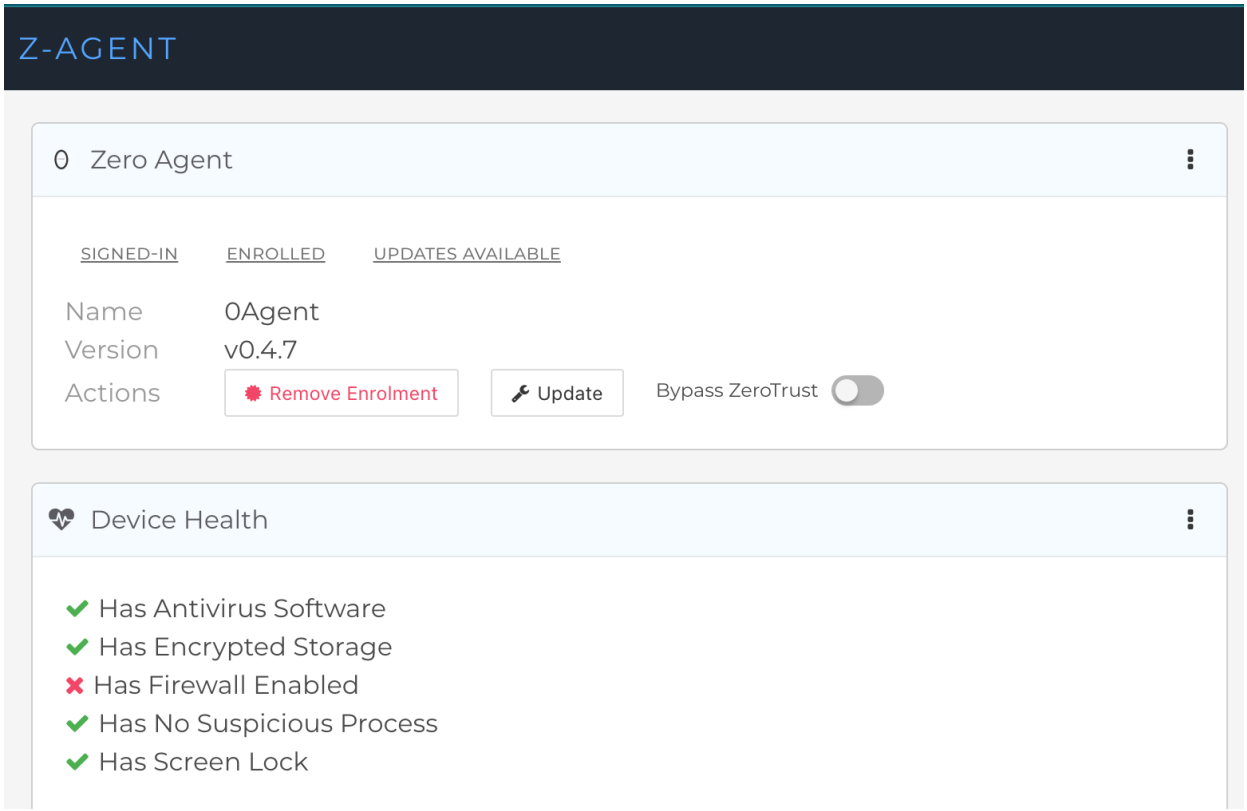
Our UEBA system builds behavioral profiles of users and entities in the organization and assigns a risk score when the behavior deviates from the previously established normal baseline. It helps us identify compromised accounts, data exfiltration, and insider threats, serving both as a diagnostic tool and an early warning system.



The UEBA system is highly customizable, thus giving us complete control over the types of anomalies to be detected. It adapts to changing data patterns automatically without any intervention and can be deployed in any domain, as long as the configuration of the types of anomalies to be detected is done correctly. ZLabs, the R&D team at Zoho, has filed a provisional patent on the design of our UEBA engine.

Phase 1 was all about experimenting. To start with, we had 250 users from both the business and IT sides of Zoho volunteer to test out the 0Trust system. For example, a leader who does not require access to development tools signed up for the 0Trust test run in the early stages. He chose to participate because he felt using the VPN to access internal resources led to sub-optimal performance of applications. Everything from build deployments and performance statistics to meetings went through the VPN, often causing issues like poor audio and video quality.

Upon creating a user account, a user could view their device health and trust score. This helped them figure out what they could do to improve their trust score and comply with policies.



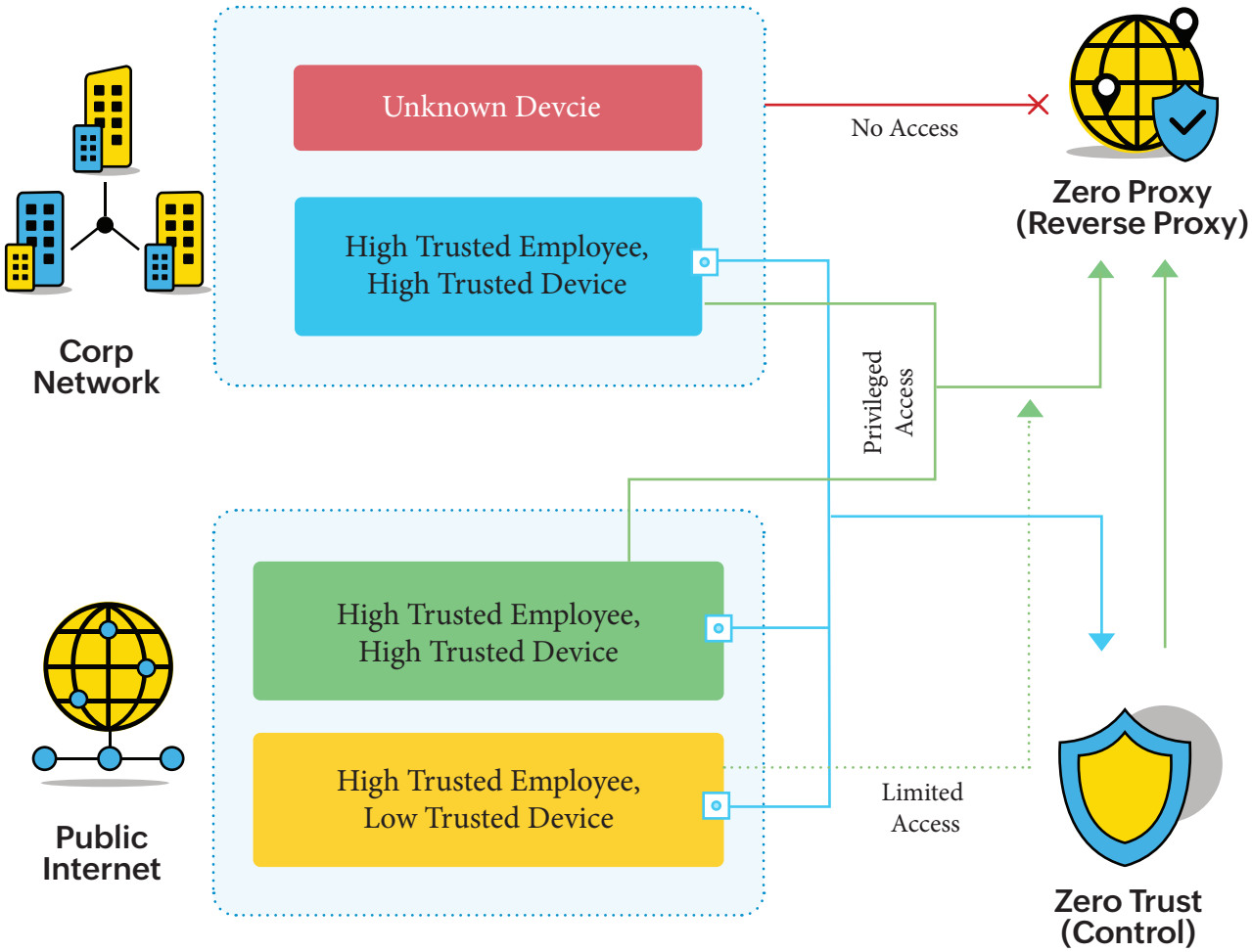
When the user started their system, 0Trust was activated automatically. If they wanted to add a specific domain to the 0Trust system, they could raise a request to the Zero Trust team. If the Security team could validate it, the domain was mapped to the local system.

After signing up for 0Trust, the aforementioned leader inferred that application performance had improved considerably. It also reduced the load on Zoho's proxy servers, so it was a win-win situation.

Phase 2

Objectives:

- Route all employee traffic via the 0Proxy.
- Monitor the traffic and log the invalid traffic, but grant access if a user is accessing via the VPN or corporate network. Analyze the failed traffic and try to address that case.
- Monitor employee VPN usage. If all their flow can be achieved via 0Trust, we will encourage them to use 0Trust completely.
- Monitor employee VPN usage. If it is not accessed for a certain period, revoke their access.
- Restrict VPN access to employees with proven needs only.



Access through Zero Trust

Our spoke office in Madurai was one of the first offices to sign up for the 0Trust trial. Home to about one hundred employees from multiple teams, it was the perfect location to start with due to its small size.

Before the pandemic, these team members were working at our Chennai headquarters, so they used the local network. Most people did not even know how the VPN worked. After relocating to the Madurai office, they had to use the VPN for daily operations. In this scenario, security became a bit of an inconvenience.

There were two problems with using our VPN. One, there were connectivity issues when accessing the VPN through mobile data. Two, users had to log in each time they unlocked their devices. So, multiple times a day, after stepping out for fresh air, grabbing a bite, or engaging in a quick chat with a colleague, they had to log in each time. To avoid this, some employees would leave their devices unlocked, which goes against our security policies.

At the same time, our development leads started to wonder, "Is VPN access required for the new employees?" New members joining the development teams did not require access to all the internal resources that the VPN granted.

Enter 0Trust. Now, the system can maintain sign-in sessions and reconnect automatically. However, this transition did not happen overnight. Installing 0Trust in each system was tedious. This was when our sysadmin introduced the 0Agent. Installing the 0Agent (via our MDM app) made the switch to 0Trust effortless, almost like working from the Chennai office. Likewise, new employees were given access to resources based on their requirements, like Git operations. Access was granted after a preliminary security evaluation, for which employees had to review the security policies thoroughly and take a security awareness test.

Today, the Madurai spoke office operates almost entirely on 0Trust. About 5% of services still need the VPN, which will be phased out once the team works out the kinks. The success of this trial run was an indicator that we were on the right path and ready to move to the next stage.

Phase 3

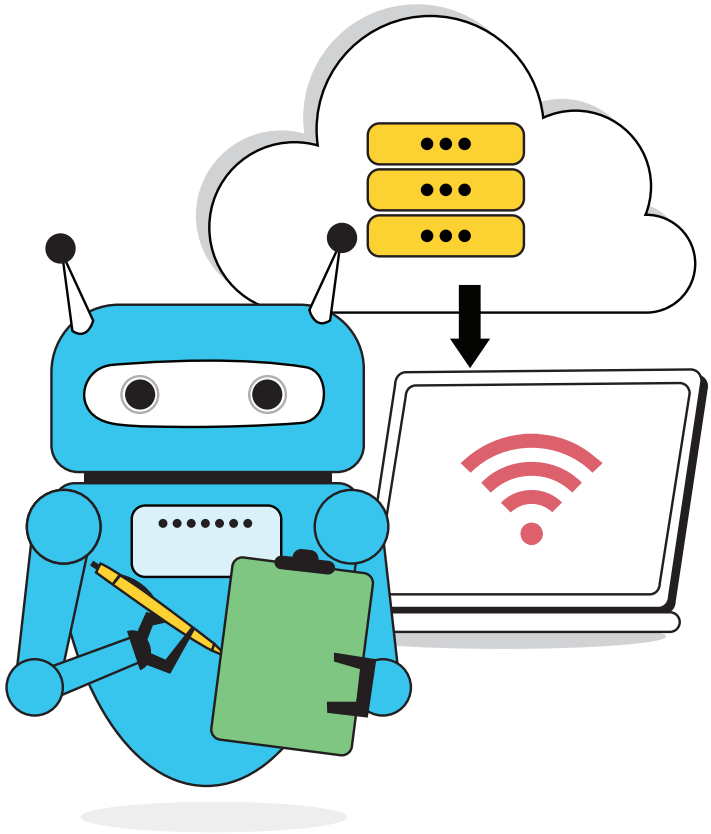
Objectives:

- Route all traffic via the 0Proxy in block mode. Block the flow if the trust criteria are not met.
- Restrict the Zoho accounts of our cloud services to accept requests only from 0Trust IPs using our IAM solution's IP restriction.

Before, if you were using the corporate Wi-Fi, you would have access to internal sites, regardless of your role. Now that we are in Phase 3, as we continue work on Zero Trust, we intend to change that. Eventually, even if an employee logs in through the corporate Wi-Fi, they will need 0Trust to access confidential information.

During the development phase, the team is working on fixing roadblocks, like scalability for all applications and device confidentiality. Once those issues are sorted out, we will make 0Trust mandatory for all employees. The 0Agent will be installed on all systems by the admin.

The Zero Trust team has partnered with a third party to monitor credential leaks. Our admins also rely on threat intelligence, an independent service developed by the Security team that provides information on vulnerabilities to help mitigate potential attacks. The purpose of threat intelligence is to enable quick resolution for security issues. Our teams connect with third-party analysts on threat intelligence platforms to combine local organization data with global data and to align their security strategies accordingly.



2.4 Factors that influence Zero Trust

1. Access control policies

For a Zero Trust system to handle authentication and authorization, it needs instructions, such as session and password policies. These policies are usually set by the security team based on input from the sysadmin.

Session policies

Parameter	Sample limit
Session lifetime	Expire session after one day
Idle session timeout	Remove idle sessions after one day
Concurrent sessions	Allow five concurrent sessions

Password policies

A. Complexity

Parameter	Sample instruction
Minimum password length	Eight characters
Minimum number of numeric characters	One
Minimum number of uppercase characters	One
Minimum number of lowercase characters	One
Minimum number of special characters	One

B. Management

Parameter	Sample instruction
Password reuse	Do not allow passwords to be reused
Password expiration	Expire after six months
Invalid login attempt	Never lock any accounts

2. Integrations

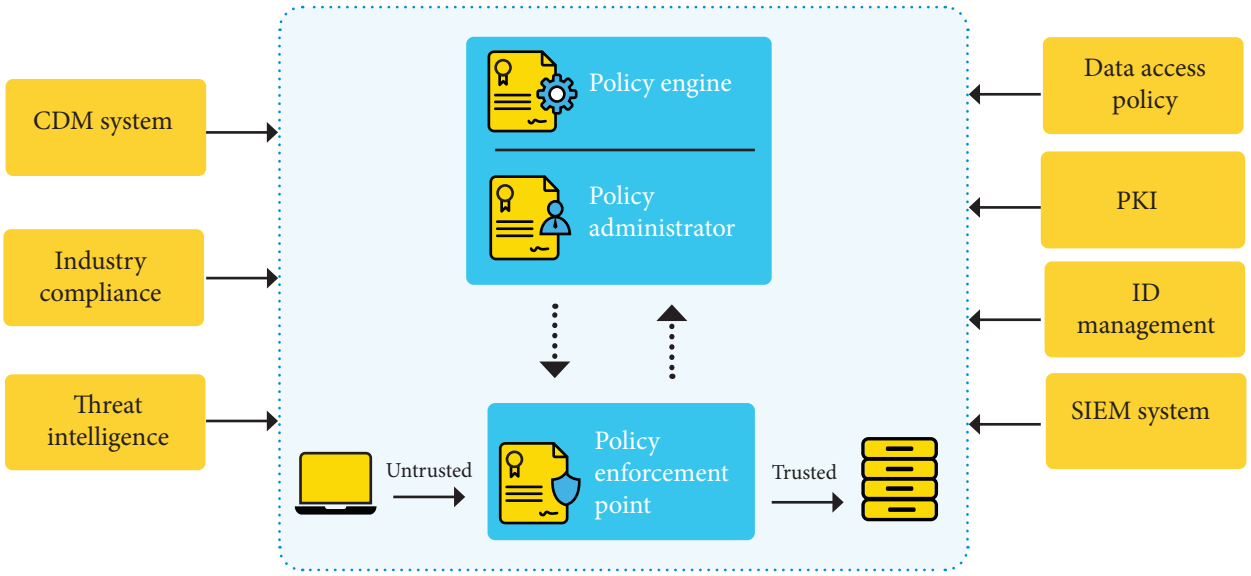
HR:

When a new user is added to, updated on, or removed from our HR portal, it is reflected in the 0Trust system as well. The employee's details, such as first name, last name, and mobile number, are collected, and the employee's email address is used as the unique identifier.

Analytics:

0Trust maintains logs. It contains details about each user, the resources they have accessed, and the access location. This is usually monitored for incident analysis, so we plan to integrate 0Trust with our analytics tool in the future.

3. Automation and orchestration



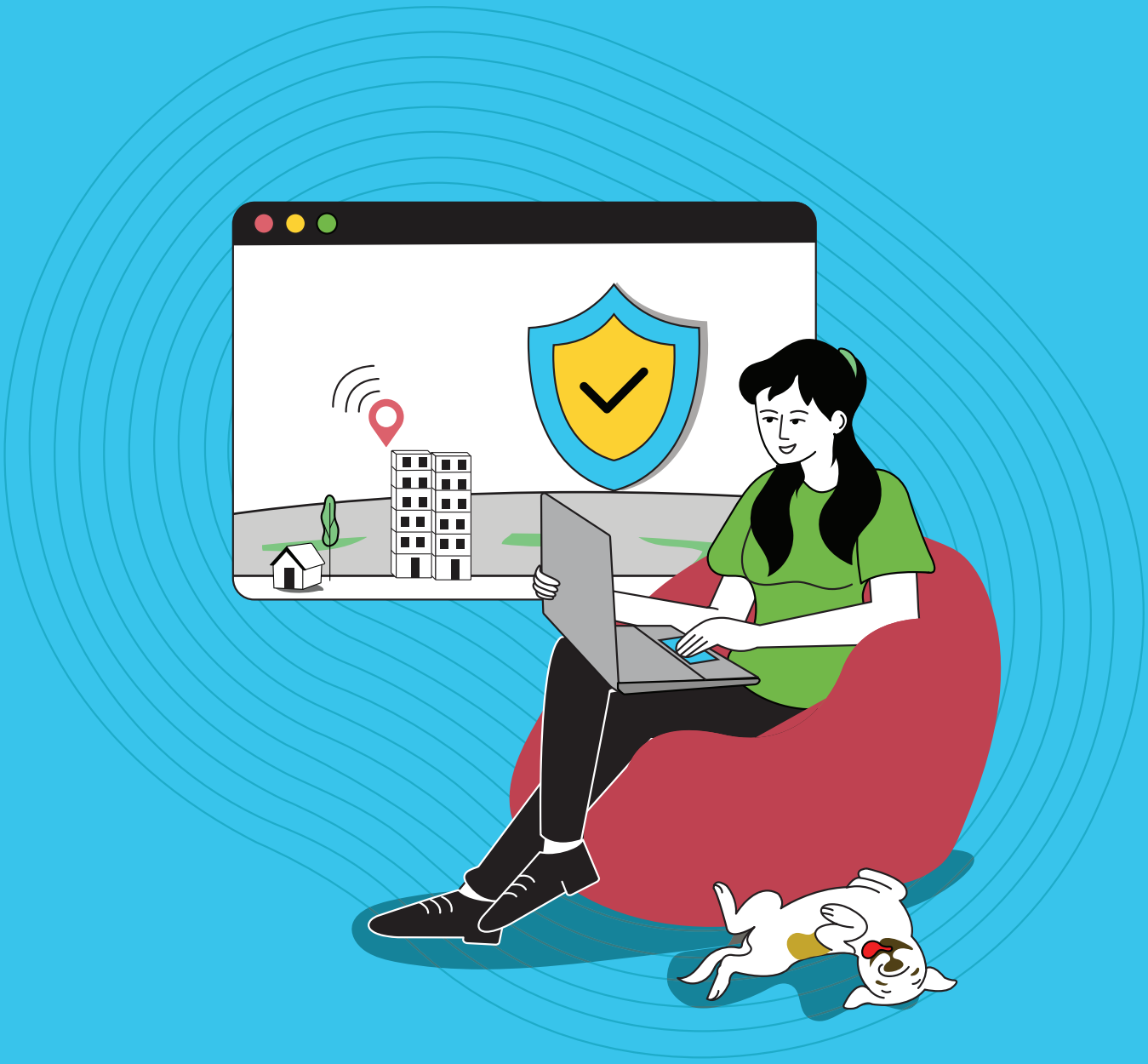
Logical Components of Zero Trust Architecture

Source: NIST's guidance for a Zero Trust architecture (a ManageEngine e-book)

This diagram represents NIST's Zero Trust architecture. Without going into the technical details, it is important to note the role of a policy engine. It evaluates the trust score for each access request and automatically accepts or rejects it. The purpose of automation and orchestration is to bring the pillars of Zero Trust together, allowing IT teams to make fast, reliable decisions. Applying automation and orchestration to the policy engine makes the IT team's work easier by eliminating the need to manually assess each potential threat before taking action.

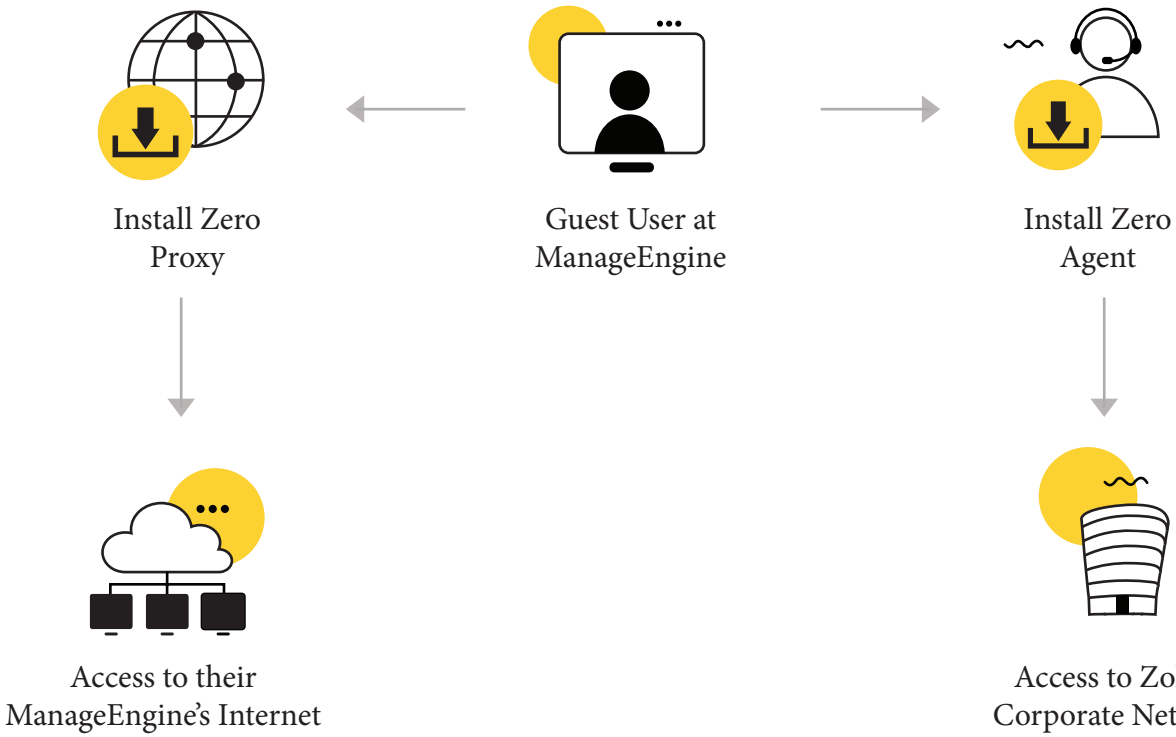
Chapter 3

Securing remote access with Zero Trust principles



Use case 1:
Guest users visiting ManageEngine

In a scenario where we have visitors on-premises who are accessing our resources, they must install the 0Agent. This can be done by the sysadmin, who also terminates sessions and blocks users and devices that do not comply with our policies. However, if a guest needs to access their own organization's intranet, they have to install the 0Proxy server.



Use case 2:
Restricting access to high-value enterprise applications

Zorro is our Data Center Operations team. It handles all the procedures involved in maintaining our data centers, improving their performance, and mitigating potential threats. One of its key responsibilities is to perform maintenance activities on app servers, such as updating firewall configurations and patching.

For a systems analyst from Zorro to access the server, these are the steps they usually follow:

Step 1: Connect to the VPN.

Step 2: Log in via our privileged access management tool.

Step 3: Connect to the application server.

Step 4: Carry out upgrades.

Ever since we implemented 0Trust, our systems analysts have found it easier to access the app server. They can connect directly to our privileged access management tool and carry out the upgrades.

Use case 3: Accessing development tools

Development tools have far more requirements than other tools. A development lead has to review and test different features built by their team. These features are hosted in the local distributed server, so they cannot access it via Wi-Fi alone.

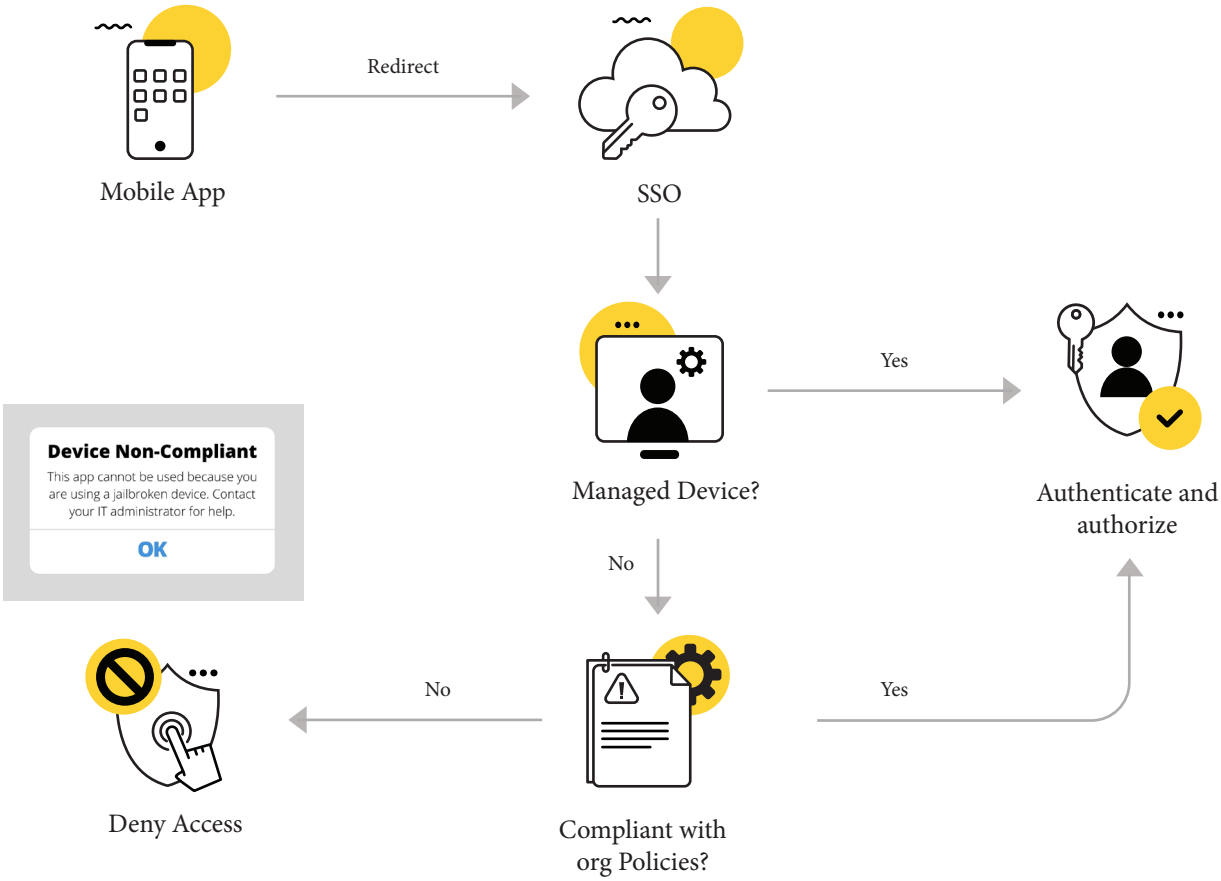
Right now, team leads have to connect to the VPN to access the local builds. This often impacts connectivity speed because all of the access is tunneled through the VPN. Sometimes, it requires multiple logins after the VPN session times out. After implementing Zero Trust, they will be able to directly connect to the tools without needing to log in to the VPN every time.

Use case 4: Access from a non-compliant device

Imagine that a member of the administrative staff is trying to log in to a corporate application from their personal mobile device, which is jailbroken. By integrating a Zero Trust system with an IAM tool, you can verify user identity and detect anomalies, if any. An endpoint management tool verifies device identity.

	Attributes		User Info	Risk Posture	Actions to Improve Security
Evaluate Dynamic User Attributes	User	User ID	Managed	Low	N/A
		Behavior	No Anama-lies		
		-Time	Usual		
		-Locations	Usual		
		-Frequency	Usual		
	Device	Device ID	Unmanaged	High	The Device is Non-compliant, So Deny Access
		Device Status	High Risk		
	Network	Network ID	Unmanaged	Medium	
		Status	Secured		
Evaluate Enterprise Resource Attributes	Application	App ID	Managed	Low	
		Status	Secured		
		App Access	Authorized (temp)		
	Data	Data Type	Secured	Medium	N/A
		Data Access	Authorized		
			Overall	High	Deny Access

In this case, the device is not managed and violates the organization's policies, so access is denied.



Use case 5: Malware-infected employee devices

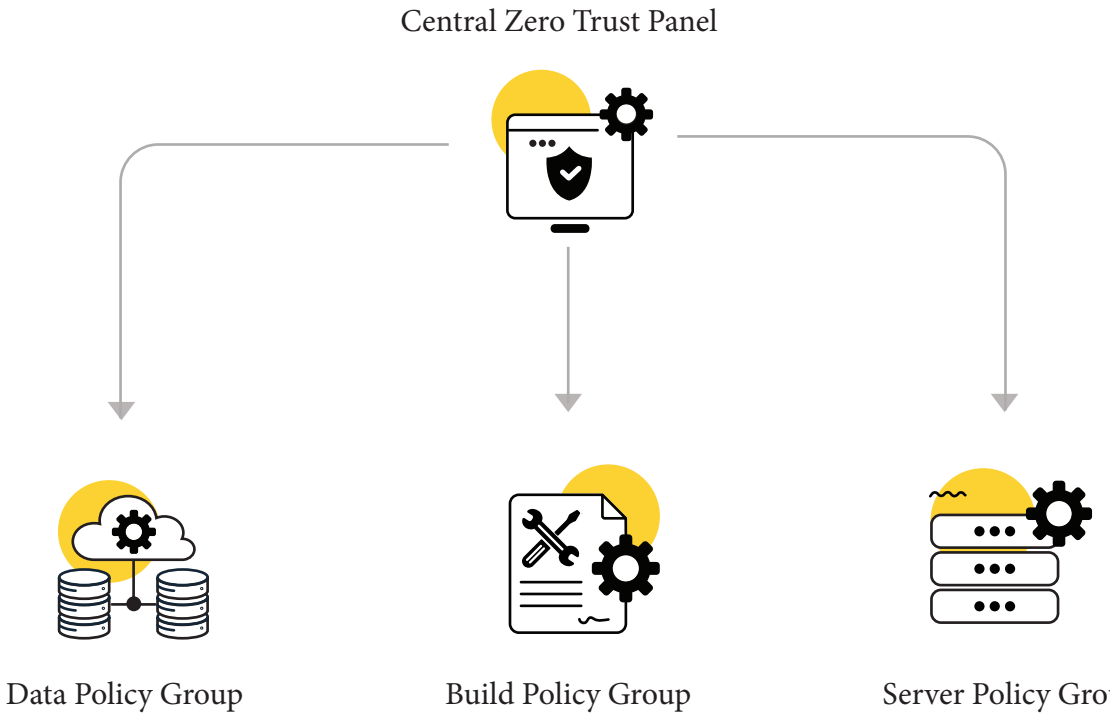
In the event of an employee's system being infected by malware, the objective is to isolate the system quickly and stop all the user's active sessions. Usually, a systems security engineer would have to use our MDM tool to initiate actions to cut off access to resources, which takes time.

With 0Trust, we can avoid that situation entirely. An agent is constantly monitoring the security posture of each device. When the session score falls below the required number, it is terminated immediately. If there are other ongoing sessions, they can also be terminated regardless of trust score. This action is carried out from the 0Trust management dashboard by a systems engineer.

Use case 6:
Customized policies for different teams

Product teams consist of members with different roles and varying requirements. Some members need access to servers or databases, while others need access to local or production builds. Resources are often hosted on different internal networks. Here, we need to enforce one of the cornerstones of Zero Trust: least privilege. Employees need minimal access to specific resources based on their roles.

Without 0Trust, product owners would have to configure access permissions individually. This might work for small teams but not for an enterprise with hundreds of members on a product team.



With 0Trust, product owners can create a policy group for each team in the central 0Trust panel and distribute each configuration. While this capability is not available in our system now, it is on our roadmap, and we hope to implement it soon.

Chapter 4

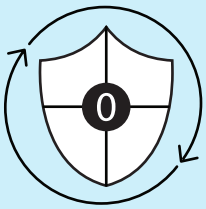
Challenges and best practices

4.1 Challenges & best practices

Challenge #1

Zero Trust is a continuous process

If only we could fix our problems with the push of a button. Zero Trust does not end with implementation, especially for growing organizations. Access controls need to be updated to align with role changes. For instance, someone who has left the organization should lose their privileges immediately. If their account is still active, you are at risk of exposing sensitive information. This continuous, complex requirement is the reason some organizations abandon their Zero Trust efforts midway.



Best practice:

Put together a dedicated team

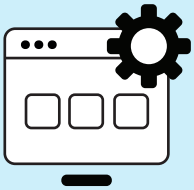
Perpetual maintenance can only be carried out with the help of a team. At Zoho, we have a small team whose purpose is to implement Zero Trust and monitor related activities. IoT devices and wearables are becoming popular in the workplace, so our access control policies have to reflect these changes.

Challenge #2

Finding a balance between security and productivity

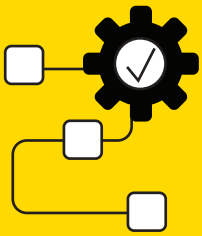
Enforcing stringent security policies might be viewed as a hindrance to productivity. Imagine having to sign in each time you open any app on your phone or verifying your identity each time you make a call. This might be secure, but it is unreasonable.

Challenge #3



Legacy applications

Transitioning to Zero Trust with legacy apps is trickier. These apps are not designed around current technology and security requirements. The foundational principles of Zero Trust are least privilege and access control, both of which cannot be performed with older systems. Some organizations go so far as to ignore legacy systems and build Zero Trust around modern applications, leaving gaps in security.



Best practice:

One step at a time

Do not jump into Zero Trust and make drastic changes right away. Ease into it with a hybrid system that balances both Zero Trust and legacy systems. Assess your existing system first. Then, create a roadmap like we did, charting out what your priorities are and what steps you need to take to achieve your security goals.

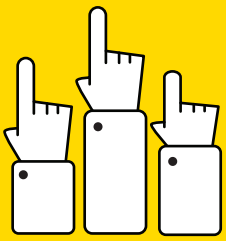
Challenge #4

Zero Trust =/= 100% security

Zero Trust helps you block potential threats based on where, when, and how a user is accessing confidential information. Even so, it does not account for social engineering attacks. There is no foolproof strategy to prevent phishing, insider attacks, ransomware, and other similar attacks

Best practice:

Zero Trust = 100% participation

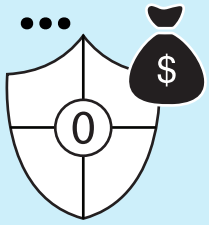


There can be no weak links! Zero Trust, once adopted, should be mandatory for everyone in the organization, regardless of their role or location. At ManageEngine, we have employees across the globe working both from the office and from home. They use a wide range of devices, applications, and services. Although it is a lot of work, our Security team is actively working with the Zero Trust team to implement it organization-wide as soon as possible.

Challenge #5

Zero Trust is expensive

Achieving Zero Trust requires compatible hardware and software. However, as we mentioned earlier, it is cheaper to invest in Zero Trust than to pay for damages. Consider it high-end insurance or an asset for the future. You will be thankful you did.



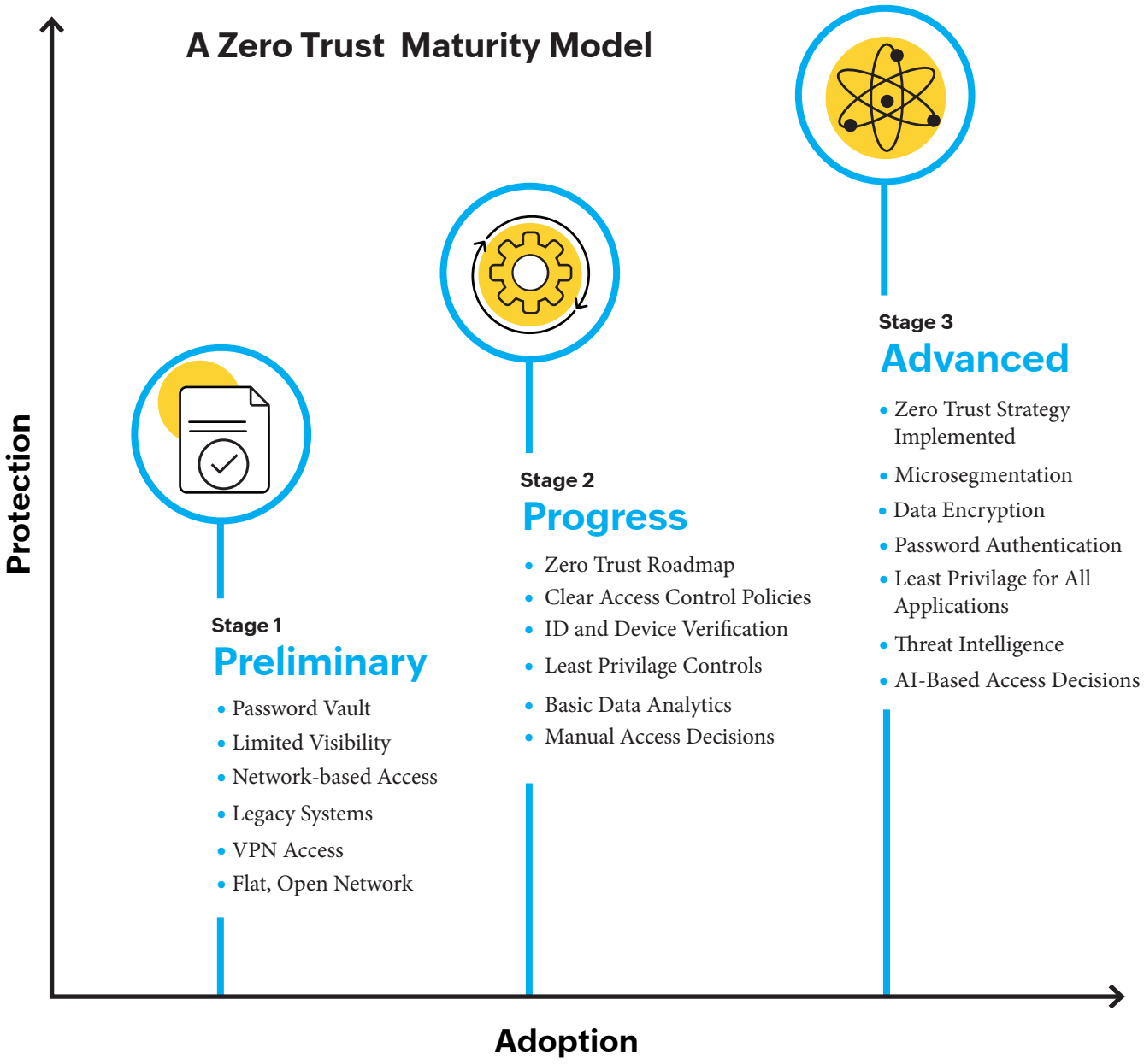
Best practice:

Invest in a strong IAM tool

IAM solutions can help users access resources by analyzing the posture of each request and determining the next step (i.e., grant access, deny access, or prompt further verification before access).

4.2 What is next?

Before you begin your Zero Trust journey, you should have a Zero Trust maturity model for your organization that charts out where you are and where you should be in terms of Zero Trust readiness. This model is usually influenced by security requirements, preexisting policies and technology, and limitations.



Right now, ManageEngine is still in the progress stage, working our way towards an optimal Zero Trust system. We plan on phasing out our VPN service soon after. Additionally, we are looking into providing 0Trust as a solution for customers.

Another exciting feature we are looking forward to is 5G. It has been a topic of discussion for years, and we are anticipating its rollout in our systems soon and a subsequent increase in IoT devices. What does it mean for Zero Trust? How will 5G services impact our operations? Presumably, 5G offers better, more granular control over network and device identity. As an enterprise, 5G could offer us an avenue to strengthen our security like never before—if we implement Zero Trust the right way.

Conclusion

Zero Trust is a developing concept and needs time to evolve into a fully fledged security system. We are still figuring out how to fine-tune our process and catch up to the likes of Google and Microsoft. Hopefully, a few years from now, we will have a second edition of this e-book with more insights into how we are taking ManageEngine to the next level of Zero Trust.

About ManageEngine

As the IT management division of Zoho Corporation, ManageEngine prioritizes flexible solutions that work for all businesses, regardless of size or budget. ManageEngine crafts comprehensive IT management software with a focus on making your job easier. Our 120+ award-winning products and free tools cover everything your IT needs. From network and device management to security and service desk software, we're bringing IT together for an integrated, overarching approach to optimize your IT.

About the author

Mahanya is a content specialist here at ManageEngine. She has been a part of ManageEngine Academy since 2020, sharing in-house stories and resources for IT leaders. When she isn't creating content, she spends time with rescue dogs.