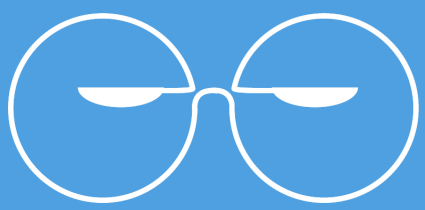
APPSEC engineer by Wiz

The Zero Trust Security Handbook

The complete guide to transforming your approach to AppSec, from the inside out

CONTENTS

What is Zero trust?



Before the concept of a 'Zero Trust Network' was introduced in 2010 by Forrester Research analyst John Kindervag, networks were protected using the perimeter model of security. Think of it like a castle surrounded by a large moat: all your trusted users and precious resources were within the castle walls, safeguarded from the outside world by the moat. Only those who were given access to cross the moat were allowed inside the castle, but once they were inside, they had free access to most parts of the castle. It's pretty simple, and it makes sense, right?

Just one problem: what if someone managed to get inside without authorisation? Maybe they disguised themselves as a trusted user, or found a way to cross the moat without raising the alarm? Now the castle has a dangerous outsider roaming its innermost sanctums, and no protocols have been established to even look for—let alone identify—the intruder.

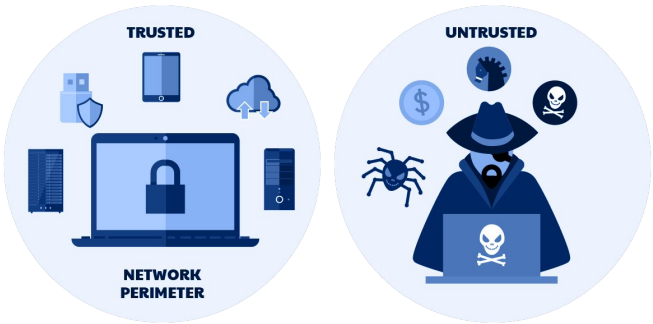
This issue is exacerbated by the fact that companies no longer have all their data in one place. Almost all organisations rely on multiple cloud vendors, services, and third party software to store and transfer data, and run their day-to-day operations. Companies are seeing their attack surfaces grow constantly, with a larger number of endpoint devices outside corporate walls. According to a 2022 Verizon report, 80% of web application attacks use stolen credentials to impersonate trusted users.

So this is the predicament hundreds of organisations find themselves in: with little to no security controls within their internal networks, an attacker who manages to penetrate the outer defence systems would enjoy unimpeded access to unprotected resources and privileges. In other words, companies are having an identity crisis.

How does Zero Trust address this issue?

Zero trust is the direct answer to the issues with the perimeter model, both on a conceptual and technological level.

As a concept, zero trust says that your network can't implicitly trust users to be who they purport to be. Any device or user trying to access resources on the private network needs to verify their identity first, regardless of whether they're within the network perimeter or not. The system assumes that there are always attackers present within the network, so no user can be trusted by default.



The biggest benefit of applying zero trust is that it reduces the attack surface of your orgnaisation's network. It minimises the damage an attacker can do by restricting the breach to one small area. It reduces the impact of user credential theft and phishing attacks by requiring multiple authentication factors. It also helps eliminate threats that bypass traditional perimeter-oriented protections.

In other words, zero trust is taking no chances. This is important, because as companies grow more dependent on cloud and remote work, they need a system to robustly manage identity and access management for users, services, and devices all around the world. he perimeter model is thoroughly decimated in such a scenario, and zero trust is the only way to truly ensure security at every level.

Organisations today recognise this: according to a 2022 report on zero trust, 97% of survey respondents have either implemented a zero trust initiative at their company, or have plans to do so within 18 months.engineering team would be exponentially harder

Challenges to implementing zero trust

While the concept of zero trust appeals to almost everyone, the actual process of implementing it is met with far less enthusiasm. There are several reasons why:

- **Large number of policies, procedures and technologies**

  Zero trust is a complex and multilayered framework, requiring organisations to rethink the way they configure access control policies and services across their entire network. This can be incredibly expensive and time-consuming.

- **Legacy technology**

  Older systems often don't work with or support elements of a zero trust security model, leaving certain companies unable to adapt.

> **The biggest benefit of applying zero trust is that it reduces the attack surface of your organisation's network.**

- **Financial constraints and resistance to change**

  Zero trust often requires a major overhaul of security systems, requiring new technologies to be implemented and IAM policies to be modernised. Many companies can't afford to throw away years' worth of security practices, and employees may not want the hassle of relearning the way they do everyday things.

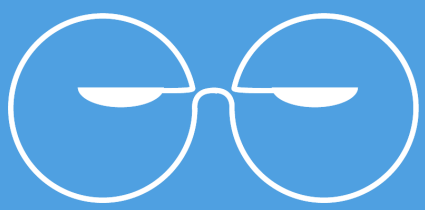
- **User pushback**

  Zero trust requires users to constantly authenticate their identity in order to access resources in the network. This can quickly become a pain point for users. "Zero trust raises friction," says Steve Wilson, principal analyst at Constellation Research, "and friction is the enemy of the user experience."

- **High level of complexity**

  Most organisations are still in the early stages of implementing the various security controls required for the zero trust model, and very have reached full maturity. In fact, only 2% of all companies worldwide have implemented passwordless access indicating that their zero-trust maturity is 'evolved'.

Principles of Zero Trust



While the technical implementation of the zero trust model can vary wildly from one organisation to the next, there are several core principles or practices you need to follow in order for it to be effective.

Here are the 6 main principles of zero trust:

1. **Least privilege**

   Zero trust focuses heavily on the goal of reducing the attack surface of your company's network, and the principle of least privilege is simply an extension of that. Giving users more permissions than the bare minimum they require can open up your system to unnecessary risk.

   The fewer privileges a user has, the less damage an attacker will be able to do if they somehow manage to steal the user's credentials and impersonate them. The attack can be contained and dealt with swiftly, reducing its impact.

2. **Continuous monitoring and validation**

   A zero trust network assumes that there are always attackers present both inside and outside the network, so it requires strict identity verification before giving access to any resource.

   The system should constantly validate user identity and privileges as well as device identity and security. In addition, logins and connections must time out after a fixed time period, requiring users to re-verify themselves each time.

3. **Device access control**

   The network should not only enforce strict controls on user access, but should keep an eye on device access controls as well.

   It needs to monitor how many unique devices are trying to access their network, ensure every device is authorised, and assess all devices to make sure they've not been compromised.

A zero trust network assumes that there are always attackers present both inside and outside the network.

4. **Microsegmentation**

Microsegmentation is the practice of dividing the network into smaller, isolated zones that all separately require authorisation, so that traffic to each of them can be closely controlled and monitored. A user with access to one zone of the network can't access any of the other zones without being authenticated first.

In the event of a breach, only a small, isolated segment of the network will be affected, limiting the impact of a security compromise.

5. **Preventing lateral movement**

An extension of the previous point, lateral movement refers to when an attacker moves to different parts of the network that are at the same level of privilege. Even if the entry point is discovered, finding them subsequently becomes a major challenge.

Access is segmented in a zero trust model, so once the attacker's presence is detected, the compromised user account or device can be quarantined and cut off from further access.

6. **Multi-factor authentication**

User accounts can't rely only on passwords to keep them safe, since credentials can be stolen through phishing attacks or other means.

Multi-factor authentication solves this by adding an additional layer of security (such as using an authentication code on a second device). Now, even if an attacker has your user credentials, they can't gain access to the network.

Prerequisites for achieving zero trust

Zero trust isn't something you can just wake up and decide to implement out of the blue. It has to be a carefully thought-out decision that takes months, if not years, to properly execute. Your team also needs to be prepared with a few prerequisites to make the transition to zero trust as smooth as possible.

1. **Inventory of assets and data**

   Zero trust is a collection of policies, procedures, and technologies. To build an effective zero trust strategy, organisations need to have an accurate inventory of assets, users, and devices, as well as a robust data classification program with privileged access management.

2. **Identity governance**

   Identity governance is a centralised system used to manage and orchestrate activities related to users and non-person entities (NPEs) like service accounts. Everything from when an individual joins, moves, or leaves an organisation or team, etc. need to be managed by the system.

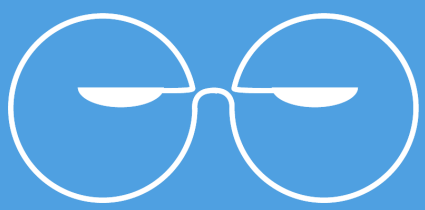
   This ensures access control policies are kept in check, permission creep doesn't occur, and risks associated with compromised or abused credentials are mitigated.

3. **Network detection and response (NDR)**

   While prevention is always the first choice in security, your organisation also needs to invest in tools to help you quickly detect when malicious activity is taking place in your network, and shut it down before it can do serious damage.

   NDR and endpoint detection and response (EDR) tools allow you to closely monitor network traffic and watch for signs of suspicious behaviour. In many cases, incident response can even be automated to rapidly shut down attacks as they're happening.

7 Pillars of Zero Trust



There's no silver bullet for implementing zero trust — it all depends on your organisation's needs and how you execute on the zero trust framework. Part of this framework are the 7 pillars, which can help standardise the execution of zero trust across your company networks.

Let's take a closer look at each one:

1. **User security**

   User or workforce security looks at the authentication and access control policies that dictate how users can obtain access to resources. This pillar also includes continuous monitoring of user activity to identify suspicious activity before it can become a problem.

2. **Device security**

   Just like with users, every device that connects to the networks needs to be identified, authorised, and assessed for signs of compromise, regardless of whether they're controlled by human users or completely autonomous.

3. **Applications and workload**

   Your organisation relies on numerous applications, containers, public and private IT resources for its daily operations. These would need to be wrapped in a layer of security to prevent attackers from stealing data, gaining unauthorised access, or tampering with apps and services.

Just like with users, every device that connects to the networks needs to be identified, authorised, and assessed for signs of compromise,

4. **Network and environment**

   The organisation's private network needs to be microsegmented, isolated, and controlled using granular policy and access controls. This will help reduce the attack surface and make incident response much faster and more effective.

5. **Data security**

   Sensitive data is usually the target of any cyberattack. You need to first categorise and organise the data, after which it can be isolated from everyone except those who are authorised to have access. This pillar also determines how the data is stored and transferred, including encryption of data at rest and in transit.

5. **Visibility and analytics**

   All activity across your organisation's network should be closely monitored, all the way from events, to user activity, to behaviour patterns. To further personalise and automate security responses, you could even apply AI/ML to rapidly detect and react to malicious user activity.

6. **Automation and orchestration**

   Automation can go even beyond incident response and security monitoring. For example, old or unused user accounts can automatically be removed after a certain period to prevent attackers from stealing the credentials and impersonating them. Or if a particular user or device is making too many requests to the server in a short span of time, the network can block them to prevent a DDoS attack.

> **Your zero trust program should be able to support users accessing your network from any location or device.**

Strategic outcomes of Zero Trust

Before any major undertaking or project, it's important to establish a concrete set of goals or a 'game plan' to help guide your team's efforts. But no strategy is complete without a set of outcomes that clearly communicate what your ideal 'end state' should look like. What should happen once you achieve your goals? What will fundamentally change in your organisation at the end of this undertaking?

Borrowing from the US Department of Defense's (DoD) zero trust strategy, here are 5 strategic outcomes for your organisation's zero trust program you need to aim for:

1. **Users able to access resources from anywhere**

   As networks grow more decentralised and remote work becomes the norm, it's vital to ensure employees and authorised third parties can securely access the resources they need without having to be in a specific location and time, or using a specific device.

   Your zero trust program should be able to support users accessing your network from any location or device, provided that both the user and device are sufficiently authenticated and secured.

2. **Agile, mobile, cloud-supported workforce**

   An extension of the last point, a zero trust program should allow you to secure and protect your information to the extent of facilitating a workforce that can easily and efficiently collaborate over the cloud.

   This means they won't be restricted by location or timezone, and their cloud-first approach can enable them to maintain high productivity levels.

3. **Reduced attack surface risk profile**

Microsegmentation and access management can help not only reduce the chances of an attacker entering your organisation's network, but limit the amount of damage they can do in the event of a breach.

Zero trust can help your team reduce the blast radius of a compromise, thereby reducing the cost of a potential cyberattack.

4. **Threats to cloud infrastructure remediated**

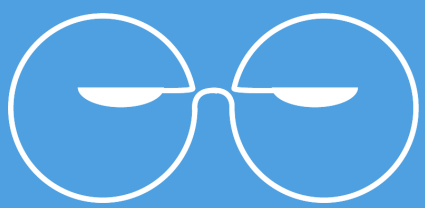
Zero trust practices help your organisation effect risk-based cybersecurity protocols and policies that remediate or outright eliminate threats to your cloud infrastructure and network.

5. **Effective damage containment**

Even if an attacker manages to steal a user's credentials or compromise a device, they need to be found and contained before they can do more damage.

Segmented networks, monitoring systems, and incident response protocols are essential to reduce the impact of an attack. The faster you can identify, locate, and quarantine/block an attacker from further compromising your network, the quicker your organisation can recover from a security incident.

How to Adopt Zero Trust at Your Organisation?



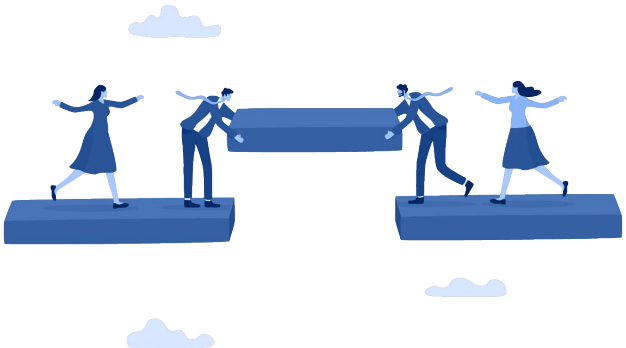
Zero trust isn't a singular milestone or 'event' that you can reach simply by implementing the right security controls. It's a complex, multi-stage process that involves making incremental changes to your system, assessing the needs of the tech stack, and gradually adopting more secure practices and technologies at every level of your organisation. This, as you might imagine, takes time and consistent effort.

It helps to break down the process of zero trust adoption into various stages or levels of maturity, letting you answer questions like:

- How many potential threat scenarios have we covered so far?
- What are the most critical security concerns we must address?
- What is the next step to take?

At each stage, you need to evaluate the successes (and failures) your team encountered during each project, and strategically decide what the next stage of implementing zero trust measures will look like. Naturally, this would vary significantly depending on the organisation, and there's fixed blueprint one can follow.

Broadly speaking, however, we can break down the adoption of zero trust into a 5-stage plan:



Stage 1: Building the foundation

This is the starting point, where you're laying the foundation for your entire zero trust program. The goal of this stage should be: 'Don't allow anonymous access to anything.' That means implementing access management controls that necessitate users to verify their identity before they get access to resources.

Key tasks/projects to undertake at this stage:

- Inventory all applications in your company
- Identify all your data assets
- Implement multi-factor authentication (MFA) for employees
- Remove unused IAM roles, users, identities

Stage 2: Add preliminary access controls

Having laid the groundwork in the previous phase, you'll have a better understanding of your applications and identity infrastructure. Now you can move into access management that is adaptive and context-based, giving you more fine-grained control over your network.

Key tasks/projects to undertake at this stage:

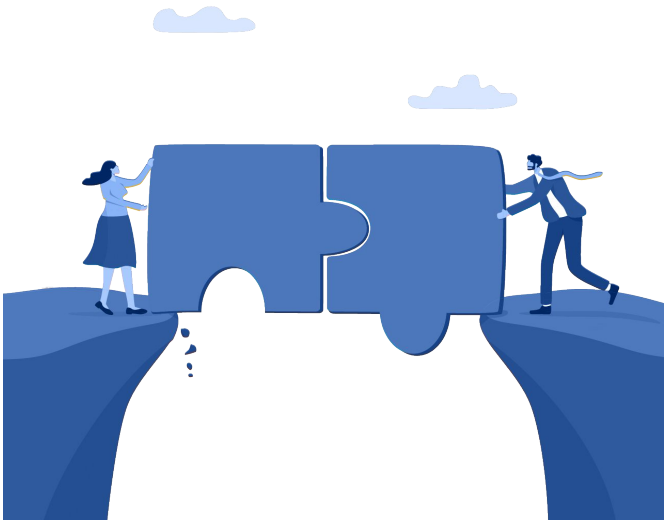
- Construct and maintain a database that maps users (employees and third parties) to applications
- Add context to access control policies (block, read-only, or allow specific activities depending on various conditions)
- Implement MFA for external users, like business partners and contractors
- Implement single sign-on (SSO) for employees in supported apps

Stage 3: Building mature access controls

At this stage, your organisation should be sufficiently advanced in your security program to implement effective processes and tools that enable remote work and 24/7 access to enterprise resources. You'll also need to add measures to enforce isolation in high-risk conditions to reduce the blast radius of a cyberattack.

Key tasks/projects to undertake at this stage:

- Extend SSO to all authorized external users
- Build policy requirements around SSO support for applications
- Automatically insert remote browser isolation for access to risky websites or from unmanaged devices
- Set up and integrate security information and event management (SIEM) tools with endpoints and cloud apps



Stage 4: Closing all the gaps

With the most critical access management issues taken care of, your organisation can now shift its focus to closing less obvious gaps, such as deprecating outdated legacy tech where necessary, and implementing data access and protections measures. You should also be looking at continuously identifying and removing instances of excess trust, working to strictly adhere to the principle of least privilege.

Key tasks/projects to undertake at this stage:

- Add secure access to APIs
- Deploy tools which act as proxies to modernise legacy technologies
- Closely monitor and control movement of sensitive data, whether at rest or in transit
- Remove excessive permissions wherever possible, enforcing principle of least privilege

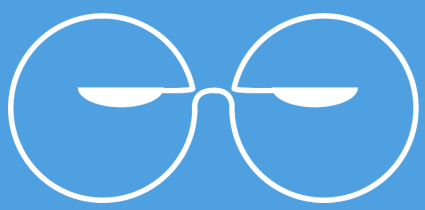
Stage 5: Real-time monitoring

At this stage, your organisation has implemented the basics of zero trust security, and can begin refining your access control strategies based on real-time information on user trends and anomalies. This involves setting up a robust monitoring and logging practice that gives you visibility across every layer of your network, alerting you to suspicious behaviour, and helping you quickly react to security threats.

Key tasks/projects to undertake at this stage:

- Implement real-time logging and monitoring systems/tools
- Set up alerts and event triggers to get instant warnings of malicious activity
- Deploy secure passwordless login across the board
- Continuously refine granular access control policies in response to network activity

Prepare Your Team for Zero Trust



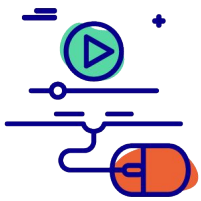
The path to Zero Trust begins with skills. At every step in the journey, your team will face unique challenges and setbacks that they've never had to deal with. But in order to formulate a vision that elevates your organisation's entire network to a higher level of security, your team needs to have the requisite skills.

Hands-on training—where they get to try out what they learn in real-world environments and solve problems by hand—is the only way to properly upskill your organisation in a short time frame without losing their interest.

AppSecEngineer has a vast library of courses designed to prepare your team in every aspect of zero trust: from network security for the cloud, to access management and cryptography, to monitoring and incident response.

With the added bonus of real-world Challenges in AWS, AppSec, DevSecOps, and Kubernetes, every member of your product team will be able to go from zero to zero trust in just months, not years.

Check out our full library of courses, or chat with us.



Courses

Playgrounds

Challenges

Community

60+ Courses, 800+ Labs, 100+ Challenges and counting...

View Course Catalog