Orange
Cyberdefense

A guide to implementing Zero Trust

Helping organizations improve security in a decentralized world

Table of Contents

Introduction 3
Decentralized world, decentralized risks 4
What Zero Trust is and isn't 5
The five pillars of a Zero Trust approach 8
A framework for Zero Trust 10
Putting Zero Trust architecture into practice 12
A checklist to take you from theory to Zero Trust reality 16
The future 18

Introduction

Protecting corporate assets from cyber-attacks has long been a priority for organizations. Regulatory, reputational, and geopolitical considerations pressure enterprises to safeguard their brands.

In today's decentralized reality, this has become more complex. The pandemic showed businesses and employees, that hybrid cloud deployments and remote access could keep them operational and even help them grow. As the world gradually reopens, many of these innovations will remain in some form or other. And with that increasingly disparate, connect-from-anywhere model, and ongoing digital transformation, comes the need for new approaches to security.

Workers require secure access, to anywhere, from anywhere. With many systems moving to the cloud, where security needs to be is rapidly changing, the attack surface is expanding, and traditional solutions are becoming less appropriate. Security is more than protecting a fixed perimeter; it is also shifting to focus on identity.

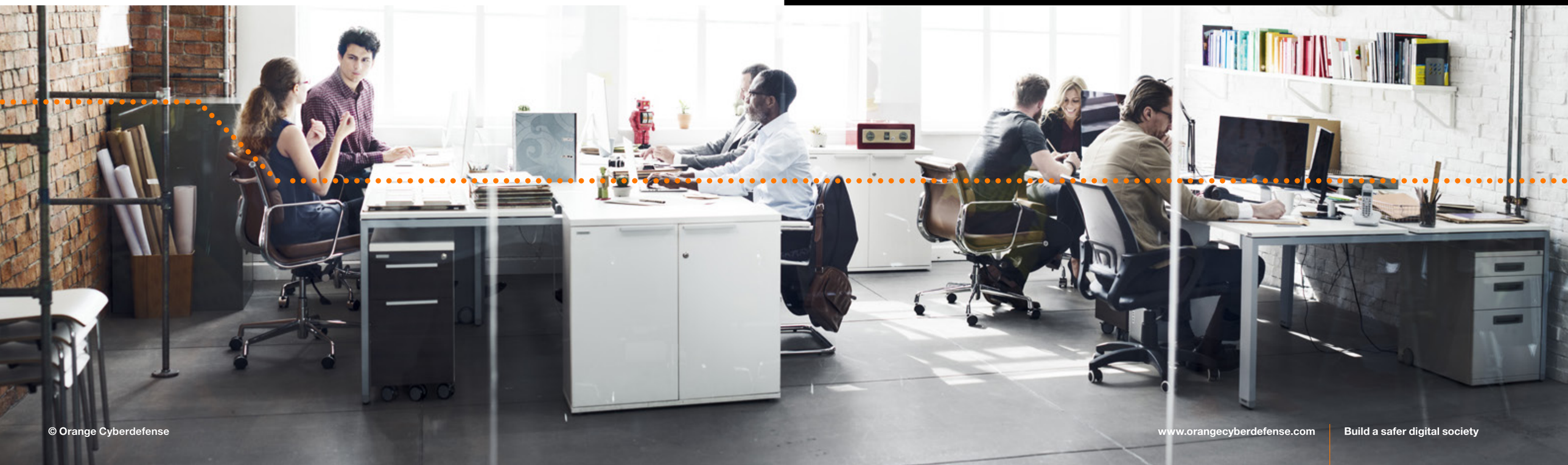
It is a change in approach that mirrors the agile, disparate and decentralized nature of business today, one that supports, rather than restricts, organizational flexibility and speed.

That approach is Zero Trust.

Zero Trust is not a new concept; indeed, it has been through an evolution as the way enterprises operate has changed. But it is gaining prominence as companies recognize that it may answer their security dilemmas.

But how many businesses genuinely understand what Zero Trust is? Understanding what it can do and how enterprises can take the right approach is a significant challenge.

This paper demystifies the hype around Zero Trust, unpicks the challenges, and provides a framework for how enterprises can switch traditional castle-style security to one more suited for how they work today.



Decentralized world, decentralized risks: the security challenges enterprises face today

A decentralized world may offer businesses more opportunities, but it also increases risks.

Attackers are becoming more sophisticated and prolific. In 2021, ransomware alone affected 37% of global organizations,[1] and was the most prevailing cyber threat according to Orange Cyberdefense's Security Navigator 2022.[2] In addition, Gartner estimates that by 2025, threat actors will have weaponized operational technology (OT) environments successfully enough to cause human casualties.[3]

Defending against this is becoming harder:

- The boom in remote working means people, data and devices are outside the traditional corporate network but still want access. Nearly half (48%) of employees work remotely at least some of the time in the post-pandemic world, compared with 30% before.[4]
- The use of Internet of Things (IoT) and OT devices continues to expand, all of which are connecting and sharing data. IDC estimates that there will be 41.6 billion connected IoT devices, or "things", generating 79.4 zettabytes (ZB) of data in 2025.[5]
- Traditional on-premises environments are moving to a hybrid footing, with enterprises expecting workloads and data to pass from legacy to cloud and back again without hindrance.
- Strategic business decisions, such as opening new channels (like direct to consumer), mergers and acquisitions, or using new suppliers to circumvent supply chain issues, are adding complexity, with new systems that need to be integrated and new users wanting access to data.
- The interconnected nature of business means collaboration with external partners has become vital. This demands the sharing of access to company applications and data with third parties.
- The proliferation of connected devices and the sprawling nature of corporate networks means many enterprises don't really know just what assets they have on their networks.
- Finally, there is the skills issue: enterprises do not have the resources and skills internally to keep up with ever-changing environments and protect them. One study estimates that the global cybersecurity workforce needs to grow 65% to defend organizations' critical assets effectively.[6]

How do you adapt to all of this? How do you check who has access to your data and where that data is being stored at any given moment? How, ultimately, can you prevent compromises of critical business information?

Many turn to a Virtual Private Network (VPN). A typical enterprise VPN solution integrates tightly with perimeter security and is effectively an extension of the core corporate network. Connecting via a web browser, and coupled with software-as-a-service solutions like Microsoft Office 365 or Google Workspace, an employee can use many, if not all, of the services they can access when on-premises.

The issue is that while VPNs enable remote working, the core challenge of perimeter defenses has not been addressed. Traditional secure remote access services like VPNs have always been a bolt-on, providing a degree of communications security when employees step outside the confines of the physical workplace. Fundamentally, they are not fit for a decentralized world.

> **"Zero Trust is an approach where implicit trust is removed from all computing infrastructure."**
>
> Gartner

What Zero Trust is and isn't

As a concept, Zero Trust has been around for more than a decade. Over that time, it has gone through its transformation. Initiatives such as Google's "BeyondCorp" helped propel the idea forward, emphasizing the required technology and understanding how it could be implemented. Now, the rest of the world is following suit, and Zero Trust is becoming increasingly crucial for enterprises.

Gartner defines it as "an approach where implicit trust is removed from all computing infrastructure".[7] Underpinning this are three basic concepts:

1. **Diligently implement "Least Privilege" throughout the organization**
2. **Assume a breach has happened or will happen**
3. **Authenticate and authorize every transaction**

In short, it is an approach to security that mirrors the decentralized, flexible, and agile operations businesses are adopting post-pandemic.

Unsurprisingly, a third (32%) of respondents to one survey named Zero Trust as an area that their organizations need to address to improve security in the wake of COVID-19.[8]

But as with any exciting concept, there is some confusion over what Zero Trust is. Certain myths have started to take hold, feeding a lack of understanding that prevents enterprises from implementing the right approach. These myths include:

- That Zero Trust is a solution to a technology problem
- That Zero Trust is a product or set of products
- Zero Trust means you don't trust your employees
- Zero Trust is expensive to implement
- There is only one way to begin the Zero Trust journey
- Deploying Secure Access Service Edge (SASE) means you have Zero Trust
- Only large multinational companies need Zero Trust
- That Zero Trust impedes business flexibility

If those are the myths, what is the reality? Zero Trust is an approach that requires a mindset shift away from thinking of the security of fixed lines of defense towards a state of continual verification, but that doesn't hamper the user experience. One that is not solely about fixing a technology problem but ensuring that the right processes are being followed and that people are aware of their cybersecurity responsibilities.

The goal is for enterprises to move from traditional deployments that rely on collating multiple point products into a working solution to an architecture that incorporates a Zero Trust approach.

Adopting a Zero Trust approach to increase business agility

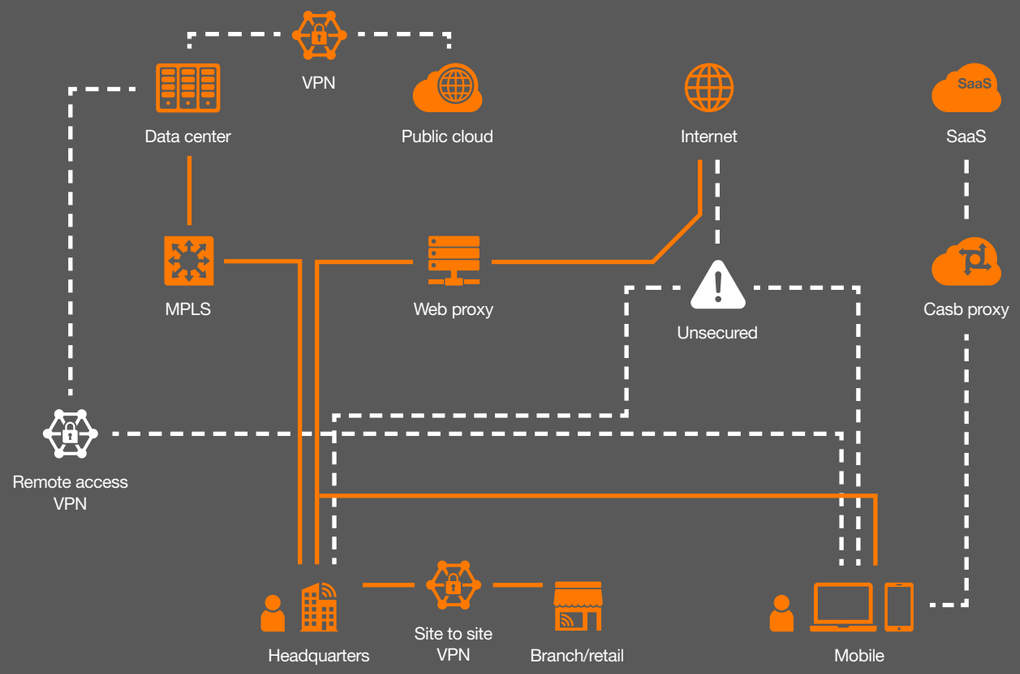
Companies need to move quickly to keep up with the competition, but that need for agility can often conflict with security. For example, a business department might choose shadow IT to quickly address a market need and circumvent onerous security procedures.

A well-engineered Zero Trust implementation can help resolve this. Policies and procedures are embedded into every access point so that every connection is rapidly assessed and either accepted or rejected based on defined processes that are continually under review.

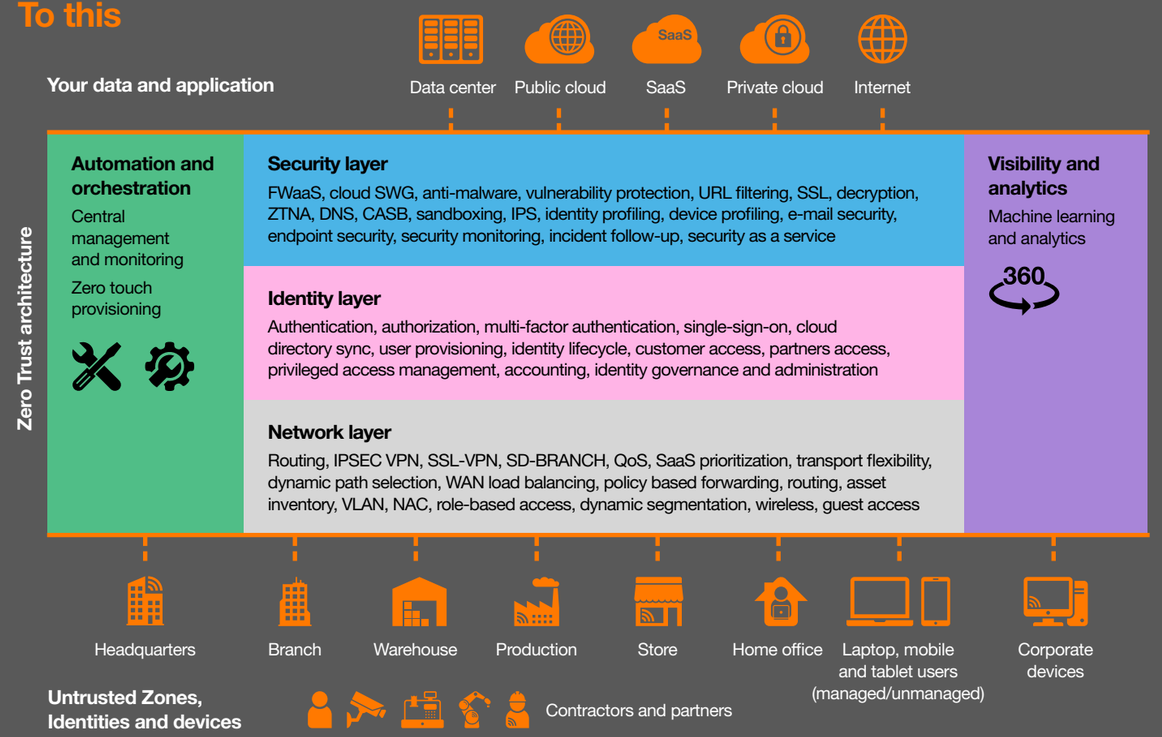
This can help enable:

- Cloud-based data analytics that provide rapid insights, accessing data without compromising critical information
- Employees connecting to some of the apps and services they need without exposing the network
- Devices being enrolled or restricted rapidly and consistently
- Identification of and responding to breaches quickly, mitigating their impact
- Robust backup and disaster recovery systems so that when there is a breach, contingencies are in place to ensure business continuity

From this



To this



The five pillars of a Zero Trust approach

What makes up a Zero Trust approach? According to the Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model,[9] there are five pillars that underpin a robust Zero Trust implementation:

Identity

The authentication and authorizing of users, applications and services, while continuously monitoring their interaction with the organization's digital landscape.

Devices

Identifying and managing all devices (including mobile, IoT and OT) connected to a company's resources.

Applications and APIs

Limiting access to applications and workloads to those that require it, covering both users and other apps and services.

Data

Encrypting data and giving it the right attributes to keep it secure both in transit and at rest, while still allowing the organization to access it and use it in business operations.

Network/Environment

Being able to control, segment, and analyze traffic across corporate networks, isolate problem areas and respond effectively, while protecting the environment that supports workloads and applications whether they reside on-premises or in the cloud.

Running through each pillar is automation, orchestration, integration, monitoring and governance. This allows you to manage everything, without significant investment in hard-to-find human resources and cyber talent. In fact, even if you could acquire the individuals needed, the almost instant nature of Zero Trust security means that adding humans to the verification process would only create a bottleneck and damage the end-user experience. Through careful and skillful automation, access can be verified and validated rapidly, threats identified, and access revoked in moments.

> **"The Zero Trust Maturity Model represents a gradient of implementation across five distinct pillars, where minor advancements can be made over time toward optimization."**
>
> **Zero Trust Maturity Model**
> CISA

A framework for Zero Trust

Zero Trust is a journey, not a destination. The nature of threats today is that they are constantly evolving and seeking out new opportunities. As such, an effective defense needs to have the same capabilities – constantly evolving, constantly monitoring and adapting.

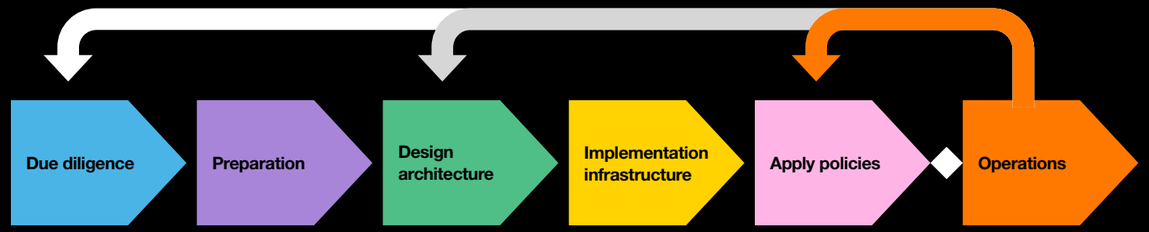
To get to that point requires a phased approach:

1 Start by defining what you need to protect, based on how your organization would be affected by a successful attack. This needs to be focused, allowing you to define clear use cases which will inform your Zero Trust roadmap.

2 From here, design a strategy that will meet your needs and identify the solutions and technologies to support it.

3 Next, you need to implement and test, creating a feedback loop which will allow you to adjust your approach in a cycle of continuous improvement. As well as ensuring that you are constantly checking on the coverage of your existing security, this process also means that new threats can be identified, and countermeasures incorporated seamlessly.

Feedback loop



To support this, there needs to be a framework against which enterprises can benchmark themselves and see what they need to do in order to progress on their journey. One that identifies how to obtain specific maturity levels in line with the ambition of the enterprise and its obligations towards its own customers.

There are five stages, with progression determined based on an organization's maturity levels in three areas: people, processes, and technology. This is a blended approach which uses leading frameworks, standards, and models that are delivered with expert consultancy.

More specifically, it uses SANS-recommended security principles, along with ISO27001 to frame a model Information Security Management System (ISMS) and position the Capability Maturity Model Integration (CMMI) to measure enterprise maturity.

During the process, maturity indicators are identified within a given cybersecurity capability. Resource adequacy is measured across each capability to determine if a company and its employees have appropriate abilities and knowledge to deliver the cybersecurity program.

The results gives enterprises a visual representation of its current Zero Trust cybersecurity footing, coupled with a prioritized and actionable list of recommendations to improve its maturity and reduce risk.

Framework

	Level 1: 0-20% Basic	Level 2: 20-40% Standard	Level 3: 40-60% Essential	Level 4: 60-80% Advanced	Level 5: 80-100% Expert
People	**Basic** Small all-round IT team, blissful security ignorance of users	**Developing** IT members with Security specialization, Initial user security awareness, information security officer	**Defined** Dedicated IT security team, user and management security awareness, developers code secure,data protection officer	**Managed** Computer security incident response team (CSIRT) user data security awareness	**Optimal** Threat intelligence research, forensics team, supply chain cyber security awareness
Process	**Ad-hoc** No security program, incidents with business impact and IT fixes them	**Partial** Continuous monitoring of availability, periodic security incident monitoring on standard use cases, security policy and process, basic governance and risk management	**Documented** Regular penetration testing, regular Incident response, continuous security incident monitoring of data, systems and network, organization wide security policy and process, governance and risk management	**Software supported** Threat intelligence sharing, real-life security exercises, automated incident response, continuous security incident monitoring on insider threats, follow-up and verification of policies and process	**Regularly reviewed** Security orchestration process, brand monitoring process, incident response exercises, continuous security incident monitoring on business risks, comprehensive security process with business process integration
Technology	**Basic** Firewall, anti-Spam, wireless, networking, anti-malware, ad hoc back-up	**Partial** Next-gen firewall, e-mail security, (reverse) proxy, 0-day malware protection, guest wireless, network segmentation, core routing, integrated IPAM, high availability, disaster recovery, automated back-up, SSL VPN, 2FA, advanced endpoint protection, server based computing, VDI	**Available** Web application firewall, cloud security, vulnerability management, network access control, network segmentation firewall, mobile device management, identity and access management, data discovery, data classification	**Enabled** Data loss prevention, data exfiltration, privileged account security, user and entity behavior analytics, firewall analyzer and optimizer, firewall and e-mail DDoS, NG intrusion detection system, micro segmentation, incident response	**Integrated** Real-time threat intelligence platform, adaptive security architecture

Putting Zero Trust architecture into practice

That's the theory, but how do enterprises put Zero Trust into practice? As it is very much a journey, this means gradually increasing the cybersecurity posture and maturity within the organization. Central to this is to take an intelligence-led approach in applying the National Institute of Standards and Technology (NIST) Zero Trust tenets across five phases of the threat lifecycle:[10]

Anticipate **Identify** **Protect** **Detect** **Respond**

Anticipate

Enterprises need to anticipate the latest cyber threats and digital risk to avoid breaches. This is a continuous process as threat constantly evolve. So, to stay ahead of attacks, complex dark web investigations, following threat intelligence feeds, investigating malware, and researching threat actors are necessary. Services exist which allow companies to subscribe to threat intelligence updates and recommendations. For example, at Orange Cyberdefense, worldwide threat intelligence information is collected into a data lake and fed back into the following identify, protect, detect & respond phases, to inform future actions can be taken.

Identify

The same vulnerability threat intelligence services used to Anticipate can, in combination with scanning, identification and notification of critical assets and data, be directly contextualized and applied to specific infrastructure to prepare a security strategy. Through the continuous monitoring of both internal and external sources and the collection of device characteristics and applications states, enterprises can manage their vulnerabilities effectively. This enables them to establish a Continuous Diagnostics and Mitigation (CDM) system to monitor the health of devices and applications and anticipate where to apply patches/fixes as needed. Assets that are discovered to have known vulnerabilities can be denied access to certain enterprise resources, based on score, criteria or context.

Protect

While Zero Trust operates on the principle that it is a case of when, not if, a breach occurs, protecting critical assets is still a core part of the approach. In particular, it ensures that:

- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy-including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed. A Zero Trust Architecture would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place).

Each of these points serves either as a source, as an element of the control plane for enforcement, or as a critical part of the data plane to defend. At the center of this resides a secure network infrastructure that has security build into its DNA. This requires a platform that protects the enterprise by performing enhanced identity management of anyone accessing data and applications based on contextual parameters, while conducting a full inspection of the traffic from each session, filtering on content, and ensuring the right policies are enforced. In addition, this platform prevents lateral movement while enabling micro segmentation.

It's also a platform that provides one central management tool, providing complete visibility of the network. In an ideal world, all this functionality would be embedded into one single tool to ease of use, efficiency and manageability.

However, that's not yet achievable. This is down to the natural focus of vendors to specific areas of the cybersecurity ecosystem, whether that's network access control or deep packet inspection. As such, to achieve this single version of the truth requires the deployment of managed services, which can simplify the multiple offerings of vendors by consolidating where necessary.

Detect

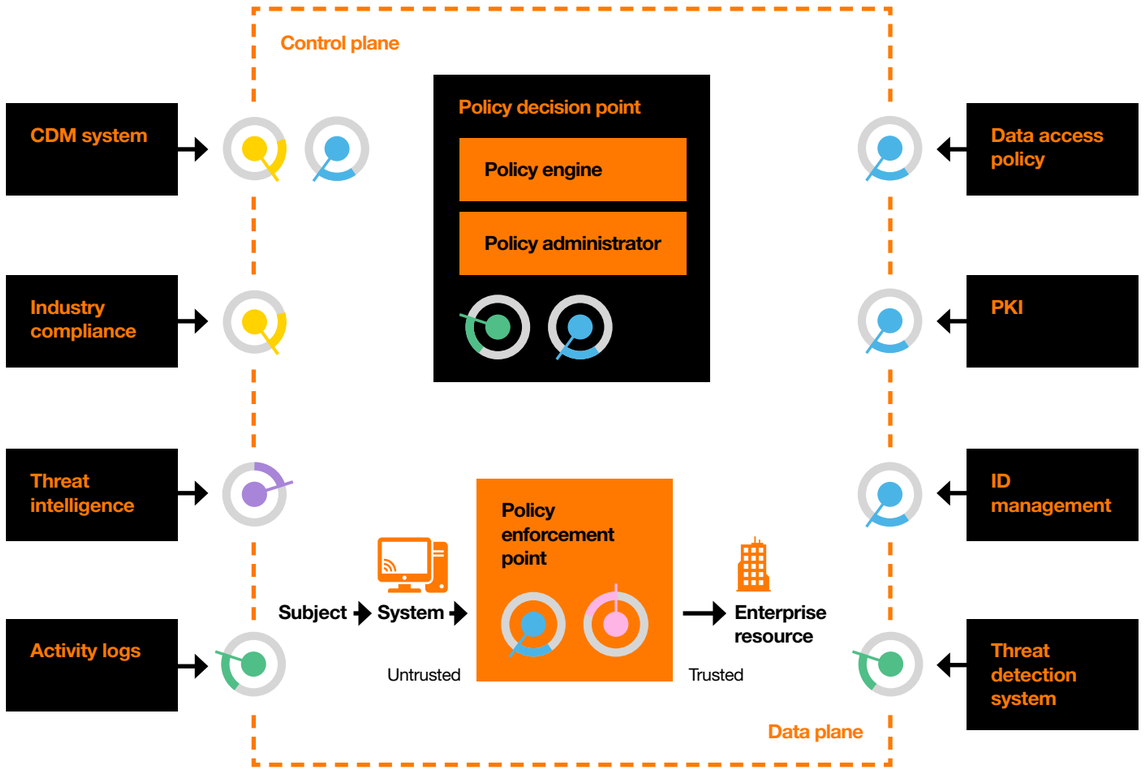
Of course, as Zero Trust operates on that when, not if, principle, it is also critical to be able to detect a breach as quickly as possible. That means being able to analyze behaviors. Through the aggregation of endpoint logs, network traffic and access actions and requests, enterprises can gather real-time feedback on its security status.

Respond (and Recover)

Being able to respond (and recover) from an attack with the right containment and remediation plans is a must. With network segmentation and clear policies, anomalies can be isolated, with affected parts of the business informed without disrupting the entire organization. Depending on the regulatory requirements, the enterprise may need to alert external stakeholders; while this is a task no one looks forward to, by having a clear detection process and response that has mitigated the impact, this notification becomes a piece of administration, rather than an admission of guilt.

The combination of being able to anticipate, identify, protect, detect and respond, driven by security intelligence, ensures the Zero Trust architecture is managed and remains adaptive to the latest threats.

Zero Trust Architecture - logical components



“Due to the nature of procurement, many of our new devices, while innovative in what they do, are behind when it comes to cybersecurity.”

Jürgen Taverniers
IT System Engineer at Jan Yperman

Zero Trust in action: Jan Yperman Ziekenhuis

While much of the discussion around cybersecurity is currently on the impact of newly remote workers trying to connect to corporate networks designed with office-based access in mind, the proliferation of connected devices has, arguably, had a much more dramatic impact on protecting mission-critical services.

This is an area that the hospital Jan Yperman Ziekenhuis knows well. Formed from the merger of three smaller hospitals in 1998, the hospital now employs more than 1,300 employees and 130 doctors with an emphasis on technology. Its use of connected devices has increased significantly, and it was this growth that prompted the hospital to start to implement a Zero Trust approach.

Securing both device and network

“Due to the nature of procurement, many of our new devices, while innovative in what they do, are behind when it comes to cybersecurity,” said Jürgen Taverniers, IT System Engineer at Jan Yperman. “Adding them to the network, while critical to their functionality, presents a security risk. By taking a Zero Trust approach and implementing segmentation, we can separate them from our mission critical services and apps, without impacting their usability. That way, we can fully secure both the device and the wider network.”

This applies to medical devices, but also the personal technology clinicians use as part of their work. “We might have nurses taking patient’s vitals, capturing it with a wireless parameter device and uploading that data directly to the patient’s e-record. Then we have a mix of hospital-issued devices, which we can control and centrally manage, and bring-your-own, which we have little to no oversight on. These are all endpoints wanting access to the system, all posing their own threats. Being able to track behavior and manage access through context allows our clients to do their work, without increasing the risk to the hospital’s digital footprint.”

Delivering security users don’t notice

The hospital also benefits from Orange Cyberdefense’s Managed Detection and Response service, which provides ongoing feedback and updates on any potential threats or anomalies on the Jan Yperman network. “The nature of our organization is such that we need an ongoing monitoring system,” said Taverniers. “Through Orange Cyberdefense, any anomalies are picked up, the team there alerts us, and we can then isolate, investigate and take any necessary action. It’s an extra layer which means that nothing is going to get overlooked and turn into a problem.”

And what do those users think of the Zero Trust approach? “At a senior level, we’ve had significant buy-in,” Taverniers explained. “There’s been a greater need to combat misconceptions of Zero Trust, such as it’s not a product but an approach, with the technical teams implementing it, but at an individual, non-technical level, users aren’t really aware. We run education and awareness classes each year to remind clinicians and administrative staff of being cyber secure, improving password security and all that, but if we do our jobs properly, most people shouldn’t even notice that we’ve implemented a Zero Trust approach. They should just be able to go about their day.”

A checklist to take you from theory to Zero Trust reality

Ultimately, every enterprise's Zero Trust journey will be different. But as we have highlighted, there are core principles that run through every Zero Trust strategy. What matters is taking the step from theory to reality.

Make no mistake, this is a transformation, of a legacy setting to one fit for the decentralized, digital era. That encompasses technology, of course, but people and processes too. But in many ways this makes Zero Trust more achievable – it is not simply a case of adding a new solution, but of true transformation that fundamentally alters how every part of the organization approaches security.

As with any change, it is challenging and complex. Working with experienced partners can help. That doesn't mean necessarily adding more vendors to an already overloaded security stack, but engaging advisors who can assess your current situation, identify where you are in the Zero Trust framework and suggest next steps.

To make things easier, it can help to interrogate your existing approach. There are several questions every organization can ask itself to build understanding as part of that initial due diligence process.

Identity

- Do you use single sign on (SSO)?
- Have you enabled multi-factor authentication (MFA), and if so for which % of users and which group of users?
- What is your MFA based on?
  - Knowledge (password or PIN)
  - Possession (badge or smartphone)
  - Inherence (biometrics like fingerprints)
  - Behavior based (keystroke pattern)
- Is there an Identity and Access Management (IAM) solution in place (for IT and OT identities)?
- Is there a policy engine verifying identity in real-time and is it using context-based input (like location, network, type of application)?
- Do you have processes in place to handle temporary machine identities (as well as user ones), which may only be in use for specific periods of time?
- Do you have solutions to handle privileged access management?

Devices

- Have you rolled out mobile device management?
- Do you have an OT asset management solution in place?
- Do you differentiate between managed and unmanaged devices?
- Are you performing end-point threat detection and determining device health?

Applications and APIs

- Where are your critical business applications stored (on-premises, cloud)?
- Is there a policy engine determining real-time access to applications?
- Do you monitor application access for anomalies?
- Do you monitor for shadow IT?

Data

- Do you label your data according to sensitivity?
- Is classification manual or automated?
- Is data encrypted?
- Do you have a data loss prevention (DLP) solution (such as blocking uploads to public clouds, or copying data)?

Infrastructure

- Are your workloads linked to an application?
- Do you monitor and correlate access based on context to your workloads and network by means of logs, network and endpoint detection?
- Is there any automated response in place in case of security incident detection?

Network

- Are your networks segmented to prevent lateral movement?
- What protections do you have in place to protect your networks?
- Are you using secure access controls to protect your network?
- Do you encrypt all your network communication (including machine to machine) using certificates?
- Are you using ML-based threat protection and filtering with context-based signals?
- Do you manually configure and manage permissions to the network?
- Do you use logical labels to dynamically manage access instead of IP addresses?
- Is there a distinction between on-premises and cloud network protection?

The future

New challenges and obstacles are going to appear that we are not yet aware of. Threats will emerge that require new counter measures; new trends in working and business operations which will require new types of protection; emerging technologies will need integration so that they do not expose enterprises in unforeseen ways.

Attackers are developing ways to target companies with much greater speed and applying new technologies to the way they set up an attack.

And it is that constant evolution that makes Zero Trust the security approach businesses are increasingly adopting today. Although the concept itself is nothing new, companies need to have an effective response to the increased level of attacks, ensuring their Zero Trust approach is future-proofed by applying the same capabilities and technologies into their security. Already we are seeing new terminology, such as cybersecurity mesh, gain increasing traction. Cybersecurity mesh is, according to Gartner, a "modern conceptual approach to security architecture that enables the distributed enterprise to deploy and integrate security to assets, whether they're on premises, in data centers or in the cloud."[11]

Cybersecurity mesh is one example of what the future holds for Zero Trust: that it will, as a terminology, disappear. As the default setting for organizational cybersecurity, there will be no need to call it Zero Trust, but simply as the accepted approach to a security posture that is intelligent, proactive, and adapts to the changing environment its organizations operate in by moving away from point solutions that target a specific threat and towards a holistic and integrated approach which delivers a more effective response to cyber threat events.

Vendors and their solutions have naturally focused on specific parts of the Zero Trust architecture. What's needed is a way to go beyond these various point solutions and endeavor to incorporate them into one seamless overall managed service.

> **"Modern conceptual approach to security architecture that enables the distributed enterprise to deploy and integrate security to assets, whether they're on premises, in data centers or in the cloud."**
>
> Gartner

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats and helping our customers of all sizes progress their Zero Trust journey.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 10 CyberSOCs and 8 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Visit us at: www.orangecyberdefense.com

Twitter: @OrangeCyberDef
LinkedIn: Orange Cyberdefense

Sources:

1. https://www.idc.com/getdoc.jsp?containerId=US48093721
2. https://orangecyberdefense.com/global/wp-content/uploads/sites/12/2021/12/Security-Navigator-2022.pdf
3. https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. https://www.gartner.com/en/human-resources/trends/remote-work-revolution
5. https://www.businesswire.com/news/home/20190618005012/en/Growth-Connected-IoT-Devices-Expected-Generate-79.4ZB
6. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
7. https://www.gartner.com/smarterwithgartner/new-to-zero-trust-security-start-here
8. https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
9. https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf
10. https://csrc.nist.gov/publications/detail/sp/800-207/final
11. https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

Orange
Cyberdefense

orange™