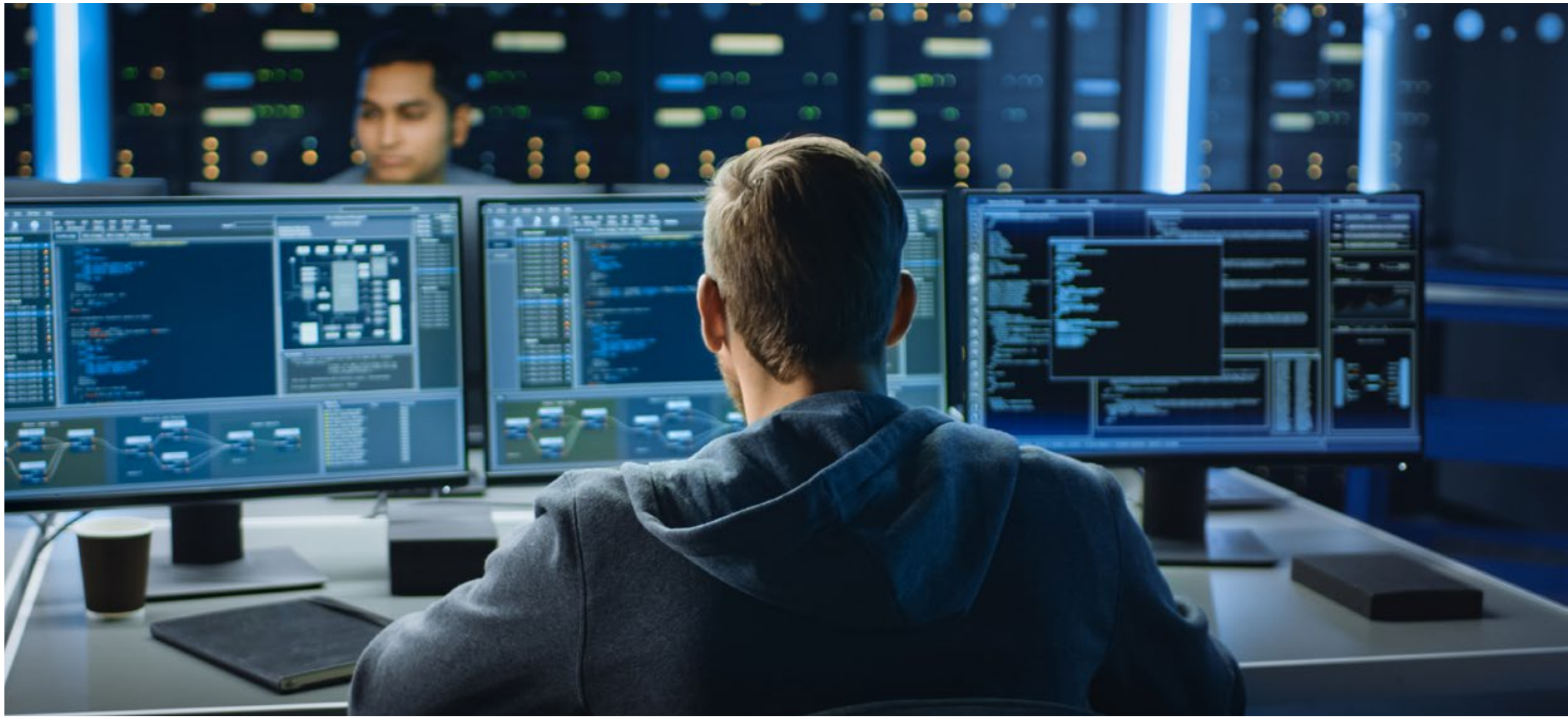
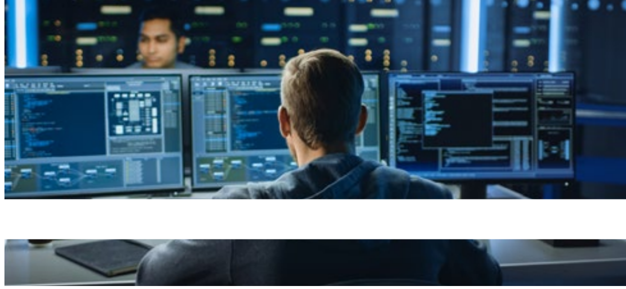
Decoding Zero Trust

March 2023



www.pwc.nl



Zero Trust (ZT) is one of the most repeated words in the cyber business today, especially after COVID-19 and its effect on how and where we work. Vendors all around the world are adding this terminology to their marketing campaigns, often to increase revenue. ZT has become a buzzword, as it promises to:

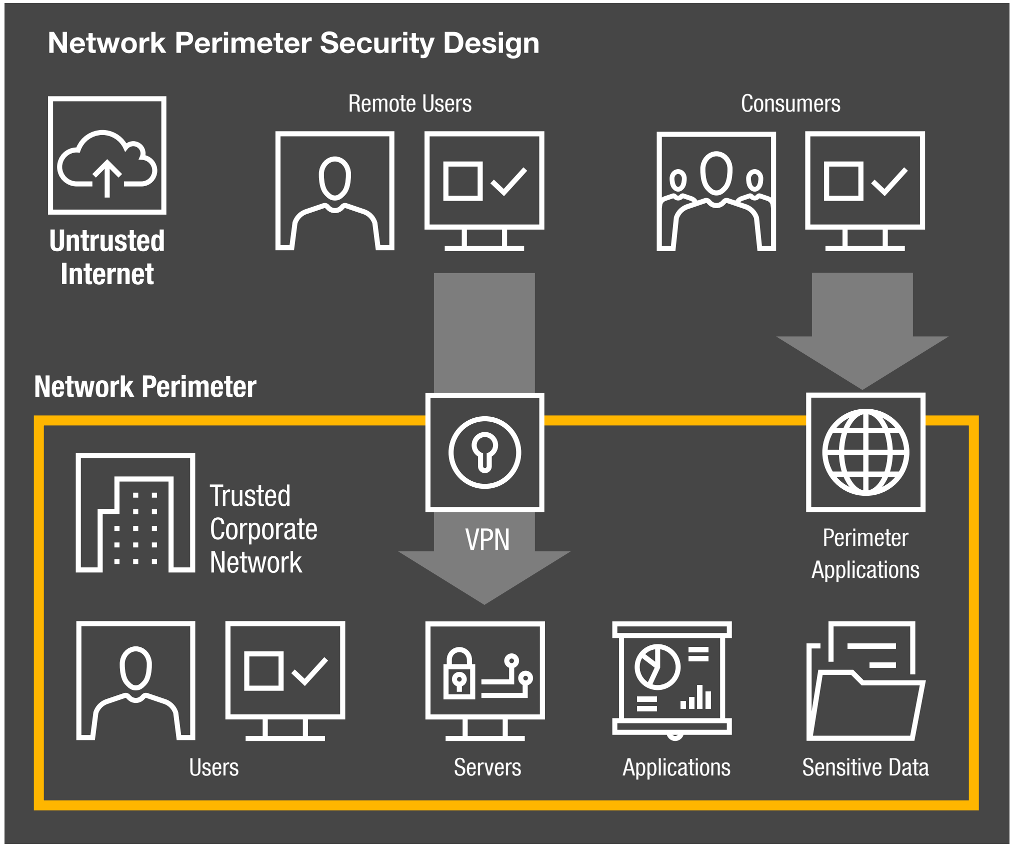
1. Improving your security posture
2. Saving you from all kinds of threats
3. Increasing your Cyber Resilience

This sounds very appealing, and many organizations are eager to implement ZT around the world. In fact, the White House issued a memorandum in January 2022 requesting the U.S. government to move toward ZT cybersecurity principles. But what does this actually mean? Are the mentioned promises all true? Where do we start? How can we do it? Has anybody ever done it? And done it successfully?

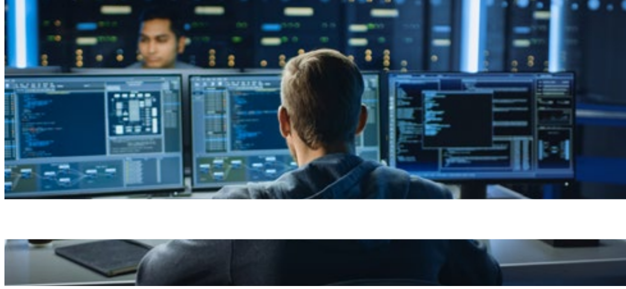
In this paper we aim to answer the above questions, by defining in simple terms what ZT is, how we can embark on this journey and realize the goals we set for ourselves when implementing ZT.

NIST defines ZT as a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.

A few years ago, protecting resources meant: (1) putting the resources in a building; (2) protect the resources by constructing big strong walls around it; and (3) give access to whoever is in the building. These big strong walls represent the network. This paradigm is called network security perimeter.



Network Perimeter Security Design



Today, organizations are increasingly migrating their data and resources to the cloud. Everyone and all things are connected; employees, third parties and customers working from anywhere, and with time more Operational Technology (OT) are getting connected to Information Technology (IT). At the same time, cybersecurity incidents continue to soar, attacks are getting smarter and more complex for security teams to protect their organization’s assets.

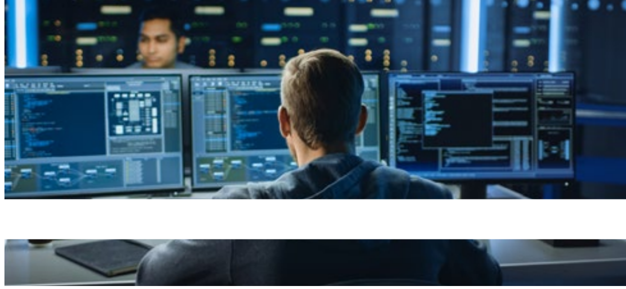
These security incidents are clear evidence that the traditional network perimeter focused security strategy is no longer sufficient to stop today’s cyber threats. Organizations need to explore a modern, comprehensive strategy for their information security architecture. This new paradigm is called Zero Trust, and instead of the network perimeter focused security, the new solution is based on identity, where identity is the new perimeter.

At PwC we like to define ZT as an architecture paradigm with clear principles to design an effective information security architecture.
Let’s decode these principles:

- **Principle (1) - Verify explicitly (Never trust, always verify):** it’s important to note that explicitly is the opposite of implicitly. In another word, we should think of designing our security by letting in only who we know and trust (instead of letting everyone in) and keeping who we do not trust outside. We do that, by verifying the identity against policies, where identity is not only about humans, but also applications, devices, things, SaaS, PaaS, IaaS and anything else that needs to have a connection to the organization.

- **Principle (2) - Use least privilege access:** following principle 1, once a resource is identified and verified, then access will be granted to specific assets with the least privilege (Just Enough Access) required for the resource to perform work. This does not apply to users/humans only, rather to all resources including applications, servers and all other services.

- **Principle (3) - Assume breach:** when designing the architecture, we need to assume that the organization is breached, and therefore we try to contain each area separately by:
  - Minimizing the extent of the access via microsegmentation, to simplify it further, imagine a ship with many compartments, and then one compartment had a hole in it. A good design in this case will prevent the ship from sinking as the water will be contained in that specific compartment, preventing the whole ship from sinking.
  - Assuming that users access all applications and services from untrusted networks, such as the Internet. Emphasis is therefore placed on keeping applications up to date and behind defensive mechanisms such as web application firewalls and application proxies.
  - Increasing threat visibility by collecting telemetry on at least the following contexts
    - **Identity context:** Who is the user? How is the user authenticated? In which department does the user work... etc
    - **Application context:** Which application is being requested, how critical it is to the business? and what kind of data is stored in the application?



- **Device context:** What device does the user use to connect? Is it managed by the organization? Is it secure?
- **Location context:** Where does the user connect from? Home? Office? Hotel?
- **Network context:** How secure is the network the user is connected to? Is it malicious? Are there any network anonymizers?

Only when we are aware of these contexts, will we be able to verify the identity, define our policies and make decisions about who and what can access our assets.

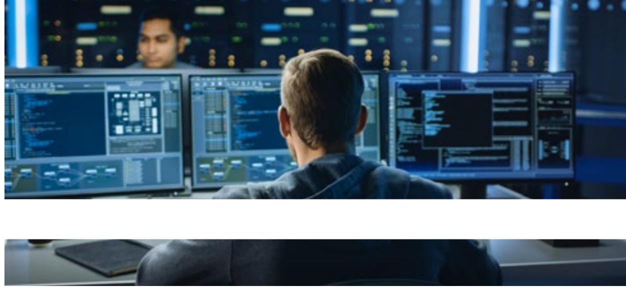
To implement ZT, different building blocks will interact with each other continuously to either:

- Provide valuable telemetry and information, to be used for decision making;
- Make decisions on allowing, blocking or requesting more info on each access request received; or
- Enforce the decisions made on the access management platforms of the organization.

By doing so, only authorized resources will be able to access the organization's assets with the least privilege required. This establishes ZT where Identity is the new perimeter.

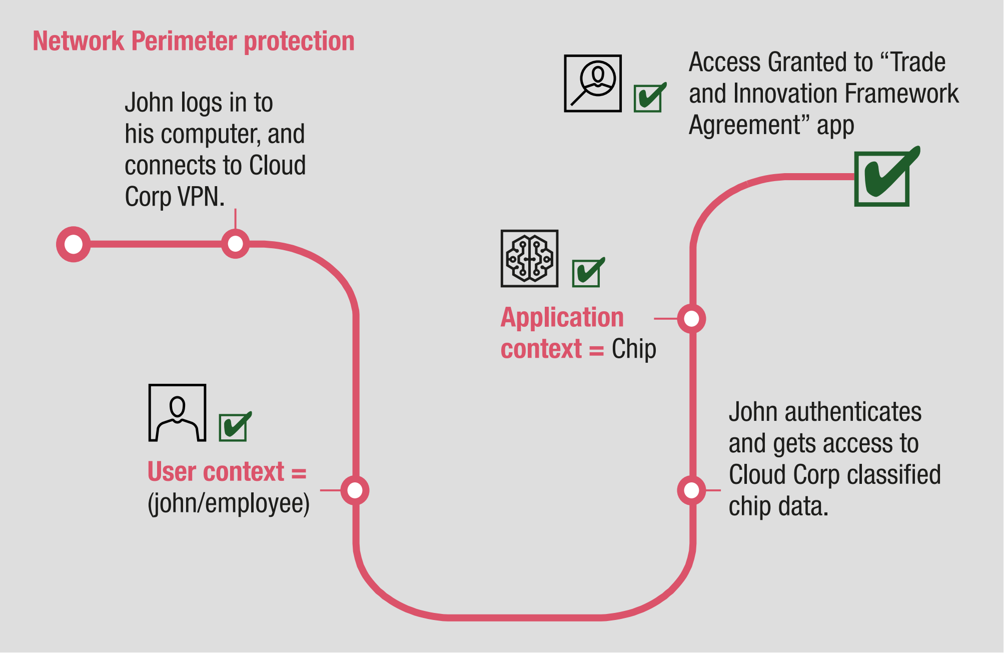
The building blocks of ZT, can be categorized into the following:

1. **Identity & Access Management:** Identity is at the heart of ZT, exists to only allow entitled resources access to appropriate assets and services with proper authorization.
2. **Application Workload:** Application workload aims to ensure threat protection, accessibility (the right people having access to the right resources), application security, visibility and analytics, automation orchestration, governance capability, virtual machine management and security and information event management.
3. **Network Segmentation:** Applications & servers segmented through their identities by importance with least-privileged communication between each other. Unauthorized traffic to/from the data center will be blocked.
4. **Secure Endpoints:** Endpoint security controls applied to users and devices (including mobile) before remotely accessing data center or cloud resources.
5. **Data:** Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the device, apps, infrastructure, and networks the organization controls. Data should be classified, labeled, and encrypted and access restricted based on those attributes.
6. **Governance & Management:** Strategy, policy management, and continuous real-time monitoring are critical to program success.



To understand ZT better, let's look at an example:
John is head engineer at Cloud Corp. He's spending his holiday abroad in Midgar and needs to check on the progress and latest developments on Cloud Corp's latest innovation: the Aeris chip. He opens his corporate laptop, connects to his cafe public WiFi and logs into the "Trade and Innovation Framework Agreement" app for classified documentation.

Let's compare the **Network Perimeter Protection** way vs **Zero Trust (Identity Perimeter protection)**.



Network Perimeter protection

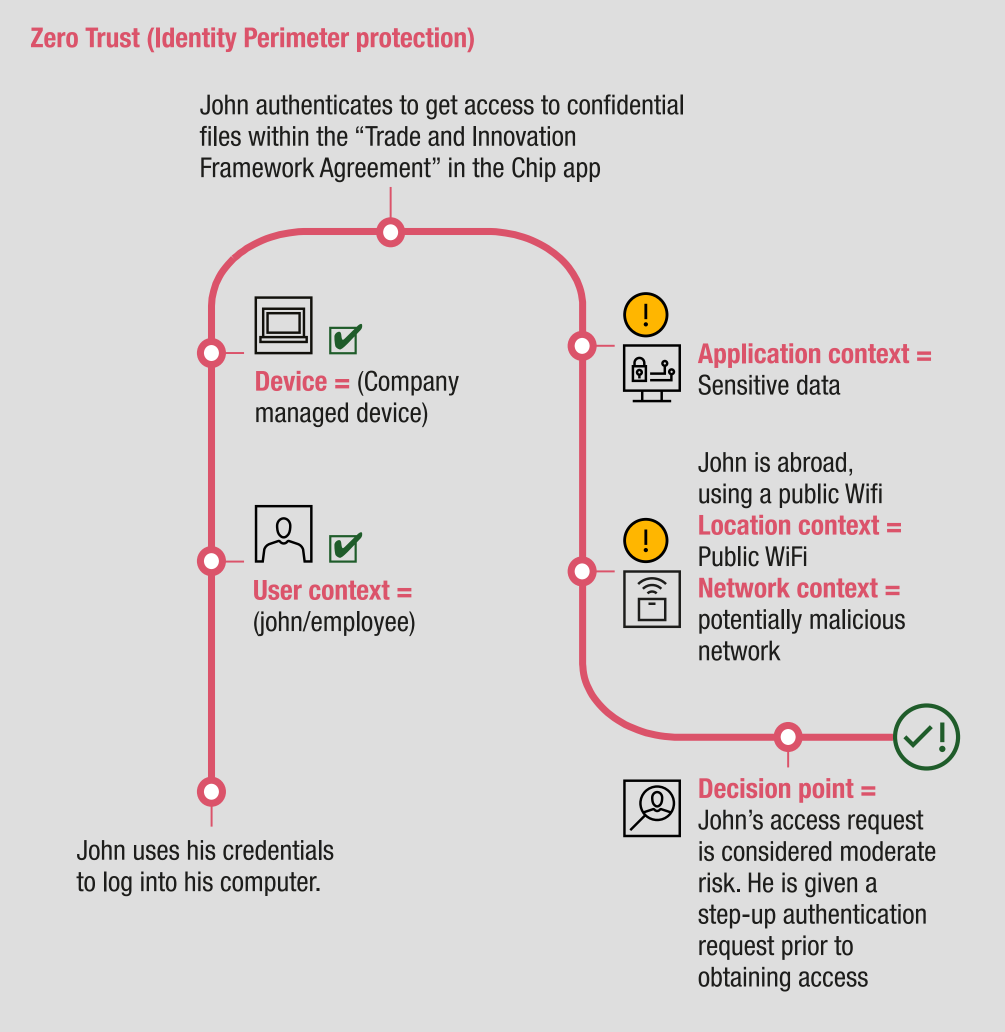
John logs in to his computer, and connects to Cloud Corp VPN.

User context = (john/employee)

Application context = Chip

Access Granted to "Trade and Innovation Framework Agreement" app

John authenticates and gets access to Cloud Corp classified chip data.



Zero Trust (Identity Perimeter protection)

John authenticates to get access to confidential files within the "Trade and Innovation Framework Agreement" in the Chip app

Device = (Company managed device)

User context = (john/employee)

John uses his credentials to log into his computer.

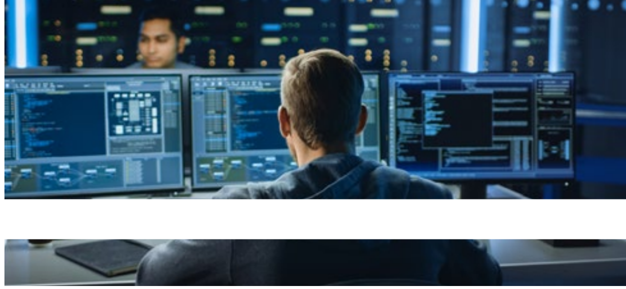
Application context = Sensitive data

John is abroad, using a public Wifi

Location context = Public WiFi

Network context = potentially malicious network

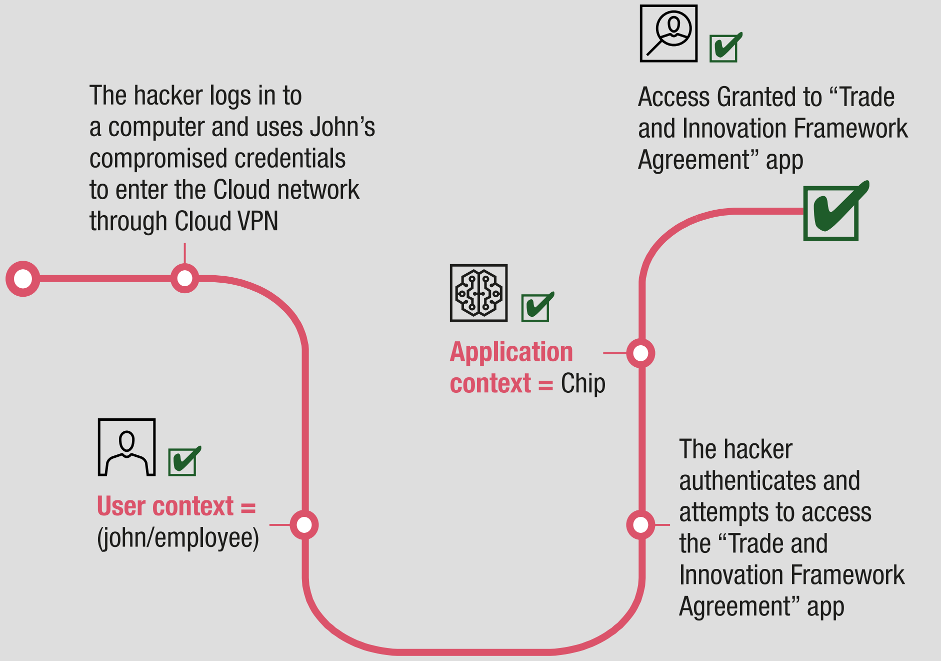
Decision point = John's access request is considered moderate risk. He is given a step-up authentication request prior to obtaining access



John’s journey goes wrong

Let’s see what happens when a Shinra, a malicious hacking group, compromises John’s credentials in order to access Cloud Corp data and leak critical design documents on the Aeris chip.

Network Perimeter protection



The hacker logs in to a computer and uses John’s compromised credentials to enter the Cloud network through Cloud VPN

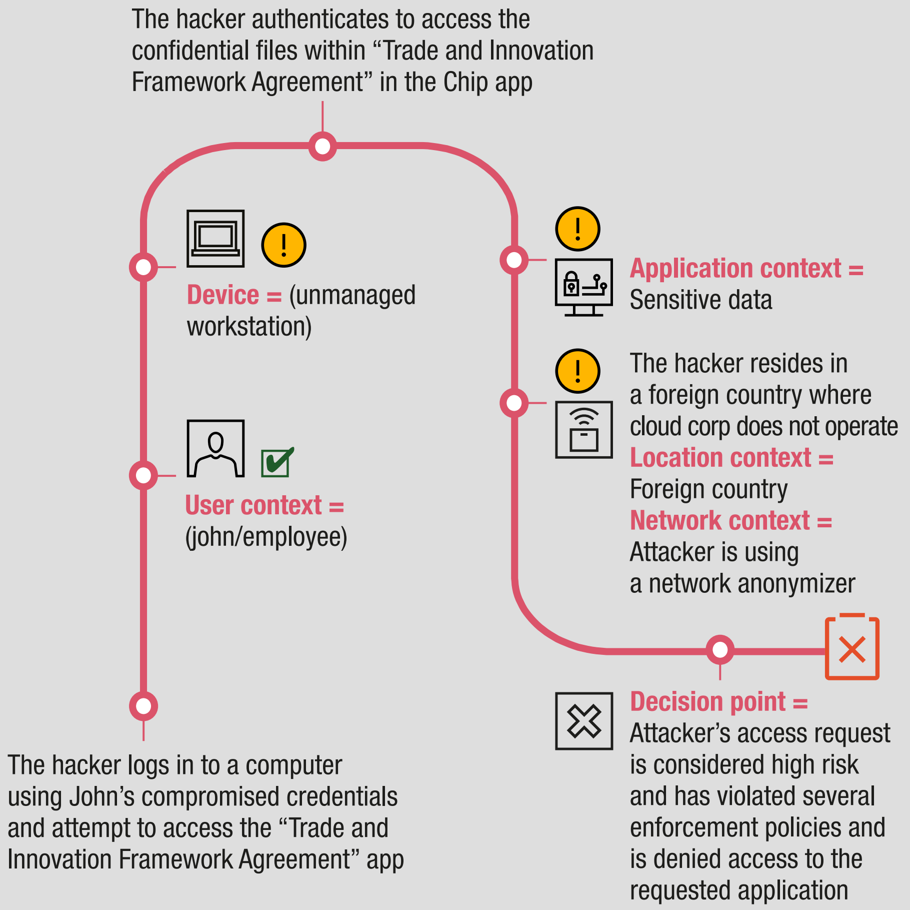
User context = (john/employee)

The hacker authenticates and attempts to access the “Trade and Innovation Framework Agreement” app

Application context = Chip

Access Granted to “Trade and Innovation Framework Agreement” app

Zero Trust (Identity Perimeter protection)



The hacker logs in to a computer using John’s compromised credentials and attempt to access the “Trade and Innovation Framework Agreement” app

User context = (john/employee)

Device = (unmanaged workstation)

The hacker authenticates to access the confidential files within “Trade and Innovation Framework Agreement” in the Chip app

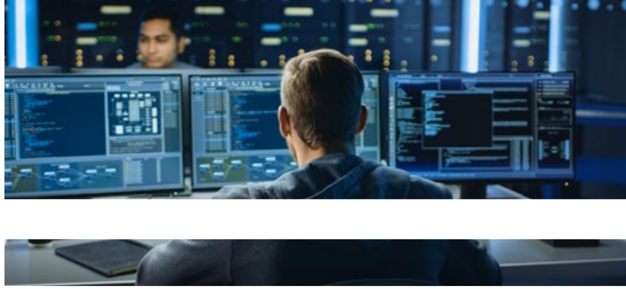
Application context = Sensitive data

The hacker resides in a foreign country where cloud corp does not operate

Location context = Foreign country

Network context = Attacker is using a network anonymizer

Decision point = Attacker’s access request is considered high risk and has violated several enforcement policies and is denied access to the requested application



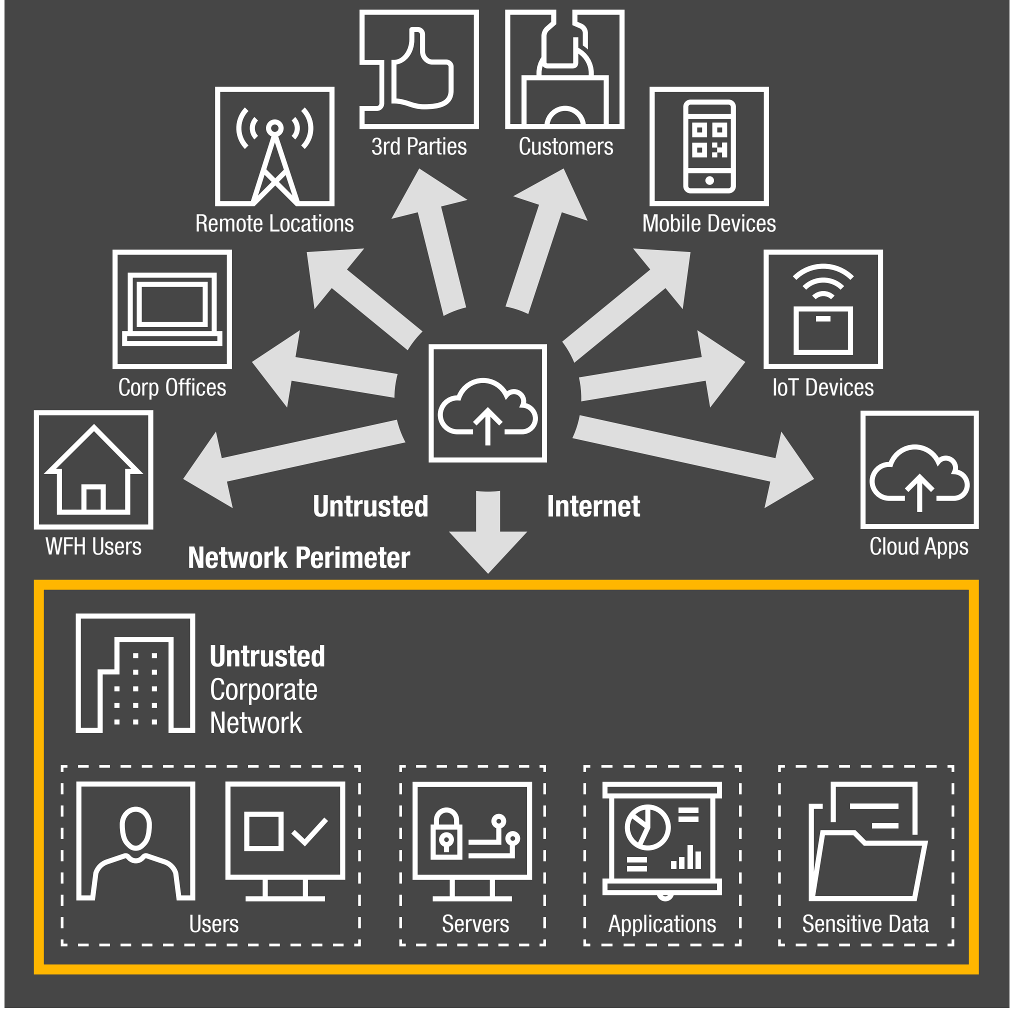
This sounds interesting, but how do we do that in practice? How can we embark on this journey?

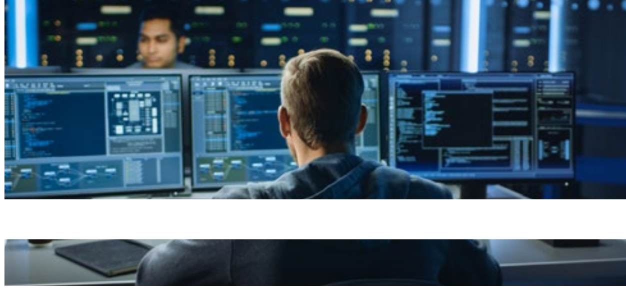
Step (1) – Start with a vision: “A thousand-mile journey starts with a single step (and a clear vision).” Organizations will not have an infinite budget to transform their security infrastructure. Therefore it’s crucial to determine your risk appetite, specifically which risks an organization is willing to accept, and which ones need to be mitigated. Depending on your risk appetite, a vision can be drawn which will determine the objective of our journey.

Step (2) - Establish Identity as the base: Identity is the new perimeter, it is the base where you will build on the other elements. Without a solid, modern, well-managed identity, the base will not hold the pressure! Well-managed identity does not only include human identities, but also Applications, Devices and Things. To understand this step better, let’s look at the layout of a typical organization today:

In this organization, many identities need to be managed, including: employees, third parties, customers, mobile devices, IoT devices, cloud apps, servers and applications. By managing identities, we mean how their life-cycle is managed, how they authenticate and access resources, the authorization and permissions per identity (least privilege), through where and how frequently these permissions are certified per certain amount of time.

Identity Perimeter Security Design



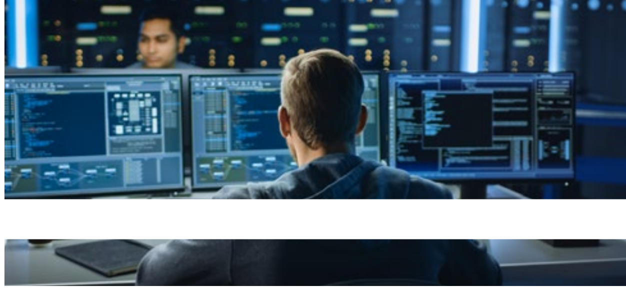


Step (3) - See the contexts: Security events must be tracked as access decisions depend on them. Organizations can also subscribe to collect threat intelligence signals and feed this info to the access management platform.

Step (4) - Start the journey: with a clear vision, risk appetite, a solid identity management and security events. We can start our Zero Trust Journey by assessing the building blocks available in the organization. Organizations might already have what is required to achieve ZT, but some tweaking might be required to be fit for purpose. Organizations might also opt to procure new technologies if needed.

It's also worthwhile to note that not all organizations will require the most advanced technology per building block; organizations might decide to have a very mature Identity & Access management system but focus less on the network segmentation, or decide to work on implementing or increasing the maturity of one building block at the time. It is however very important to consider the interoperability between these blocks at any point in time.

In conclusion, we hope that this article clears any confusion about what Zero Trust is and isn't, and eventually provides you with some knowledge to tackle this paradigm in your organization.



How can we help?

Building around Zero Trust is now a critical part of a successful information security strategy. However, executing that strategy can seem overwhelming. PwC takes a holistic approach in tailoring Zero Trust transformation programs that fit the organization's needs. Our methodology is based on an assessment of business processes, people, and technologies. Our goal is to design the program objectives and the target state architecture that is right for your organization.

If you'd like to start with Zero Trust, or you need help building it, please reach out to us:

Gerald Horst
Partner
gerald.horst@pwc.com

Fadi Daood
Manager
fadi.daood@pwc.com

About the Author:

Fadi Daood is an experienced Information Security architect leading PwC's Zero Trust Practice in The Netherlands. Fadi is also an active member within PwC's European Zero Trust community.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. At PwC in the Netherlands over 5,300 people work together. Find out more and tell us what matters to you by visiting us at www.pwc.nl.