Whitepaper

November 2022

Your Zero Trust journey begins with a strong Identity and Access Management platform

Just because it's complex, doesn't mean you shouldn't be doing it.

ICY
Security

Content

Publisher
ICY Security

Editor
Gitte Gormsen
ICY Security

Authors
Marcus Tanghøj
Michael Bennike
ICY Security

Executive Summary

Zero Trust is a very popular term in many organizations. It is regarded as the front of Cyber Security and is highly desirable. While implementing Zero Trust is a highly complex task, the core principles of the Zero Trust security model are relatively simple.

In this whitepaper, we explain the conceptual aspects of Zero Trust, and provide guidance on how classic Identity and Access Management (IAM) disciplines such as Privileged Access Management and Identity Governance and Administration can be leveraged as part of a Zero Trust journey.

Zero Trust is highly dependent on a strong foundation of identity and asset management capabilities. Many organizations already have an IAM program in place with accompanying processes and technologies, and a good way to make strides towards Zero Trust is therefore to integrate the right IAM capabilities with your Zero Trust strategy to achieve a unified and centralized strategy. You will therefore be able to start your Zero Trust journey by utilizing the IAM cornerstones you already have – and get a head-start.

Introduction to Zero Trust

Historically, network security revolved around perimeter-based security. A paradigm in which security is based on pre-defined permitters and security controls being applied accordingly: Those inside usually benefit from a significant portion of inherited trust simply from already being inside the perimeter. For example, a VPN connection: Once you are inside, you are treated as if you are on the corporate local network.

With the increase in remote working where employees work outside the company perimeter, and the increase in Bringing Your Own Device (BYOD) where potentially insecure devices are brought inside the company perimeter, the lines between company network and the outside world have become increasingly blurred, rendering perimeter-based security ineffective.

Zero Trust is a security model intended to combat the challenges modern enterprises are facing. It removes the well-defined and well-secured perimeter, and replaces it with a much more dynamic approach to security: Users are no longer given inherent trust based on the network they are on. Instead, users are continuously evaluated against a trust-engine and access policies to compute to which degree the systems trust the user and subsequently match that trust against the actions that the user is performing, ie. a highly privileged action will require more trust than trivial activities. This means that users are evaluated much more holistically based on numerous dynamic factors instead of just being evaluated on pre-defined roles and perimeters.

In this whitepaper, we present the benefits and relevancy of the Zero Trust model compared to the perimeter-based security model. We compare Zero Trust to existing IAM methodology and explain how IAM techniques, tools and principles already used by many organizations can be leveraged to support implementation of Zero Trust. By combining IAM and Zero Trust efforts, it is possible to succeed both within your IAM and your Zero Trust security program at the same time.

The core of Zero Trust

Zero Trust is based on the mantra:

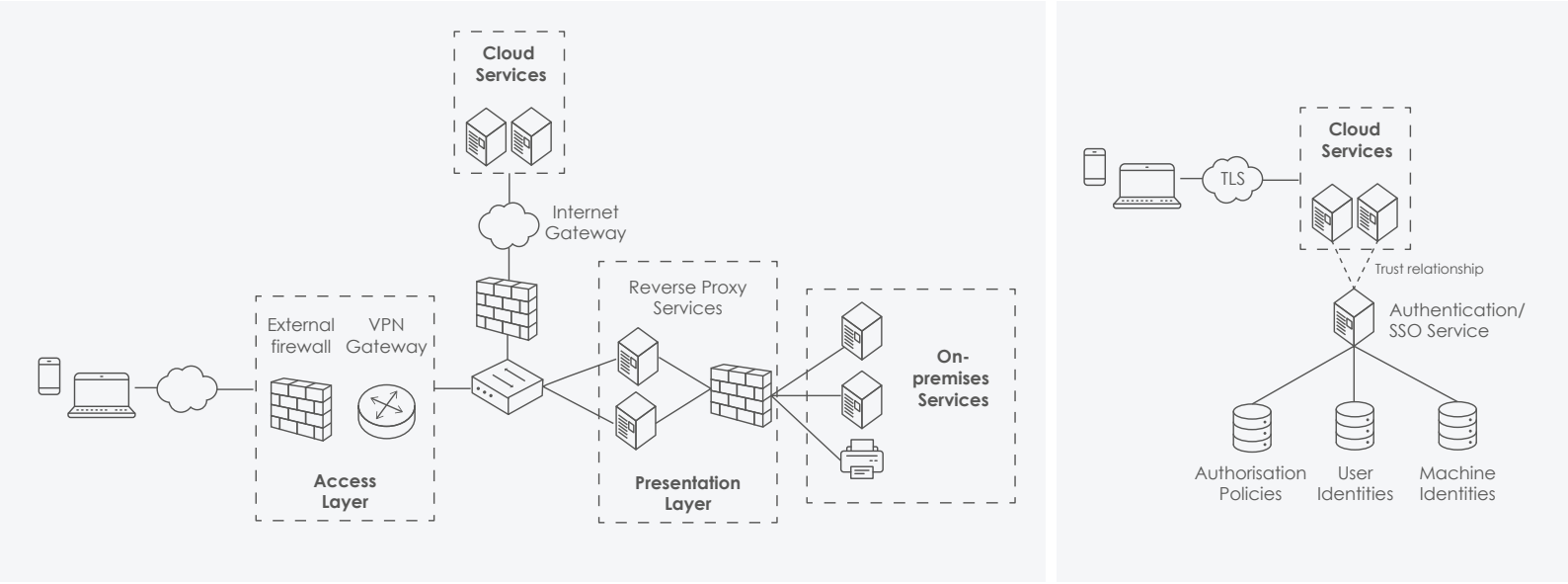
Never trust, always verify

This mantra stems from the core assumption of Zero Trust networks:

Every incoming request to servers, devices and applications are assumed to be potentially hostile

Let us assume that every device is isolated and exists in a hostile environment. An example of this could be the design of server security in the context of a server (or web application) which is exclusively internet-facing with no external firewalls to filter traffic. Very much like a Cloud service. Based on that assumption, there is no longer a trustworthy network-based perimeter since the device can no longer trust requests regardless of them originating inside or outside a given network perimeter. The requestee's origin and position within a given network should not imply any additional trust just because they are already within the corporate network. This is the "Never trust" part of the mantra.

Figure 1:
Example of perimeter-based network architecture (left) compared to a Zero Trust-based architecture (right)



Source NCSC

In the Zero Trust model, the 'perimeter' therefore becomes the device itself and must be responsible for its own internal security perimeter. To achieve this, the device should always verify the authenticity of incoming requests and validate whether the requestee has appropriate authorization to perform the request. This is the "always verify" part of the mantra. The main challenge of Zero Trust is how to manage trust between the device and the requestees when there is no implicit trust by default. Never trusting is easy, this can be achieved by the devices simply using a default-deny firewall no exceptions. However, it makes for poor service if no one can communicate with it. To balance this, in a Zero Trust ecosystem, it is a matter of establishing trust by aggregating data from multiple sources. Here, the verification is key: How can the device verify and trust every request? Zero Trust architecture aims to *enable* devices to achieve this by providing key input such as access policies, encryption, trust evaluation, context-based risk scores and many other security principles.

At a conceptual level, consider the above figure (1.0.) which shows an example of the traditional perimeter-based architecture to the left and a comparable setup with Zero Trust applied to the right. Note that in the Zero Trust model, the firewalls (perimeters) are no longer in place, and instead, a centralized security management plane (or security controller) is introduced to provide centralized control and Authentication/SSO services. The security controller facilitates access between the user and the Cloud services based on access decisions derived from repositories consisting of authorization policies and user- and machine-identities.

The technologies and principles to achieve verification and establish trust in a Zero Trust ecosystem are numerous. We will not delve into details in this whitepaper, but at a high level, Zero Trust architecture leverages a selection of tools and technologies to work in unison. There is no single tool or off-the-shelves solution that can deliver Zero Trust. Zero Trust is a strategy and is highly complex to implement, requiring involvement from both deeply technical stakeholders all the way to up the executive level. But just because it is complex doesn't mean it isn't worth striving towards.

The benefits of implementing Zero Trust

Perimeter-based security is growing obsolete due to its inability to properly mitigate several key trends that organizations face today. For example, the permitter model struggles at:

- Properly mitigating insider threats: They are authorized to act inside the perimeter.
- Securely accommodate Bring Your Own Device policies: BYOD introduces potentially insecure devices to the ecosystem that can be brought inside the perimeter.
- Isolating tenants in multi-tenant Cloud deployments: With the move toward Cloud-based deployments, the physically neighboring devices in the datacenter, or even virtual machines in the same hypervisor, can no longer assume trust between them due to the shared resources between tenants.
- Supporting remote workforces securely: With a single point of failure such as a VPN, the organization faces the risk of creating backdoors to its own internal network and the VPN therefore presents a high-value target for outside threats and can limit workforce remote productivity.
- Preventing lateral movement: Attacks from cyber threats such as ransomware aim to establish a foothold within the perimeter, and from there propagate. The wider they can get, the more damage they can cause. With a perimeter model, the risk is that once the foothold is established, lateral movement is relatively easy due to the inherent trust that the foothold grants the attacker or the attacking malware.

All the challenges for the perimeter-based security model are trending: Insider threats are as real today as they have ever been and both BYOD, Cloud deployments and remote working are all growing in demand by the business units for productivity reasons. Security units relying on a perimeter-based model are therefore faced with the choice to either restrict these trends at the cost of productivity or allow them at the consequence of a weakened security posture. The Zero Trust security model provides much better risk mitigation of all the previously mentioned challenges which is why Zero Trust is a hot topic today: It eliminates the classical perimeters, which makes lateral movement much more difficult, hampering both insider and outsider threats. It automatically assumes a multi-tenant environment and moves security to the device/machine-level, making Zero trust very suitable for Cloud deployments. With the removal of perimeters, VPNs become obsolete, promoting increased agility for remote work.

An example of a successful Zero Trust implementation:

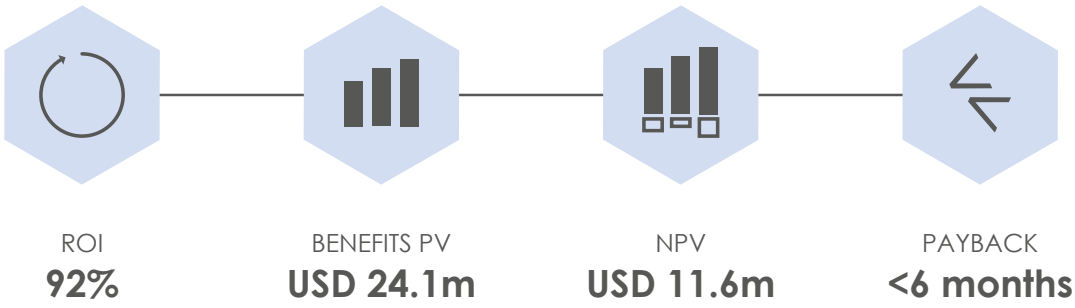
Following the Operation Aurora cyber attacks, Google was in need of a more agile and mobile security model that not only allowed employees to work with BYOD but also access remotely from anywhere. Google went on to redesign their whole security approach based on Zero Trust which they named BeyondCorp.

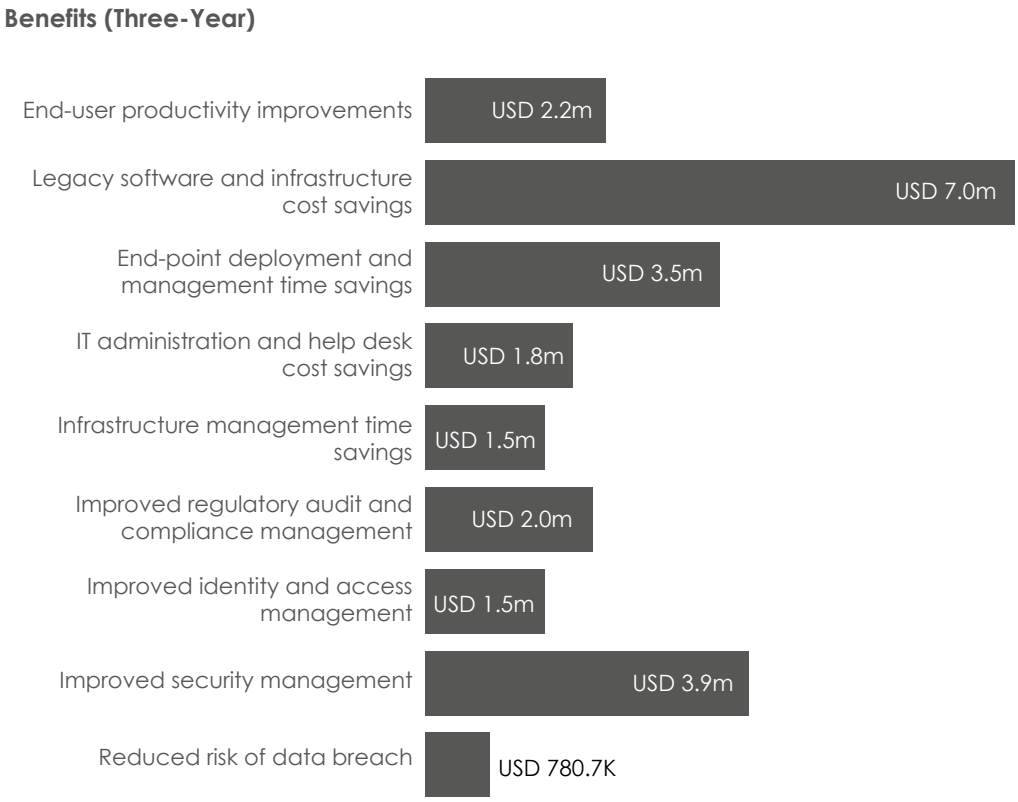
Due to the requirement to verify all requests, a Zero Trust organization needs to have a strong understanding of its IT resource landscape such as assets, users and applications, this includes asset and application management systems, Identity and Access Management tools and streamlined processes for life-cycle management of IT resources.

In addition to the benefits of mitigating risks that are challenging to mitigate with the perimiter-based model, implementing Zero Trust enables easier adoption of modern authentication techniques such as password-less authentication[1&2]. This provides benefits such as:

- Reduced cost of lifecycle management of IT resources[3]
- Better user experience due to reduced authentication-prompt overhead for users
- Organisational cost savings, see figure 2

Figure 2:
Summary of Forrester's analysis: The Total Economic Impact Of Zero Trust Solutions From Microsoft





[1]Source Microsoft
[2]Source BeyondTrust
[3]Source Forrester

Identity & Access Management and Zero Trust

As mentioned previously, the main objective for any Zero Trust device is to verify the authenticity and authorization of any incoming request. To do so, the organization needs to be in control of both their users, assets and authorization policies. The securing of users, assets and security policies is crucial to prevent attacks in the Zero Trust model.

Asset and Access management and security
While the source of asset management should not reside within IAM space, IAM tools are ideal to provide access management, governance of authorizations and access policies.

Asset management itself should be provided by dedicated asset management tools, or if no such tool is in place, configuration management tool databases can be leveraged during early stages of the Zero Trust adoption journey.

Asset security is provided through a multitude of tools and techniques. For example: certificates/PKI, malware protection, software defined networking, end-point-protection, vulnerability scanning, patch and configuration management etc.

User and authorization management and security
Managing users as well as their accounts and access rights is what the IAM domain provides capabilities to achieve. With a mature IAM setup in place, you have tools and the ability to efficiently support Identity Governance and Administration of your users and access rights which is crucial to achieve the *always verify* part of Zero Trust.

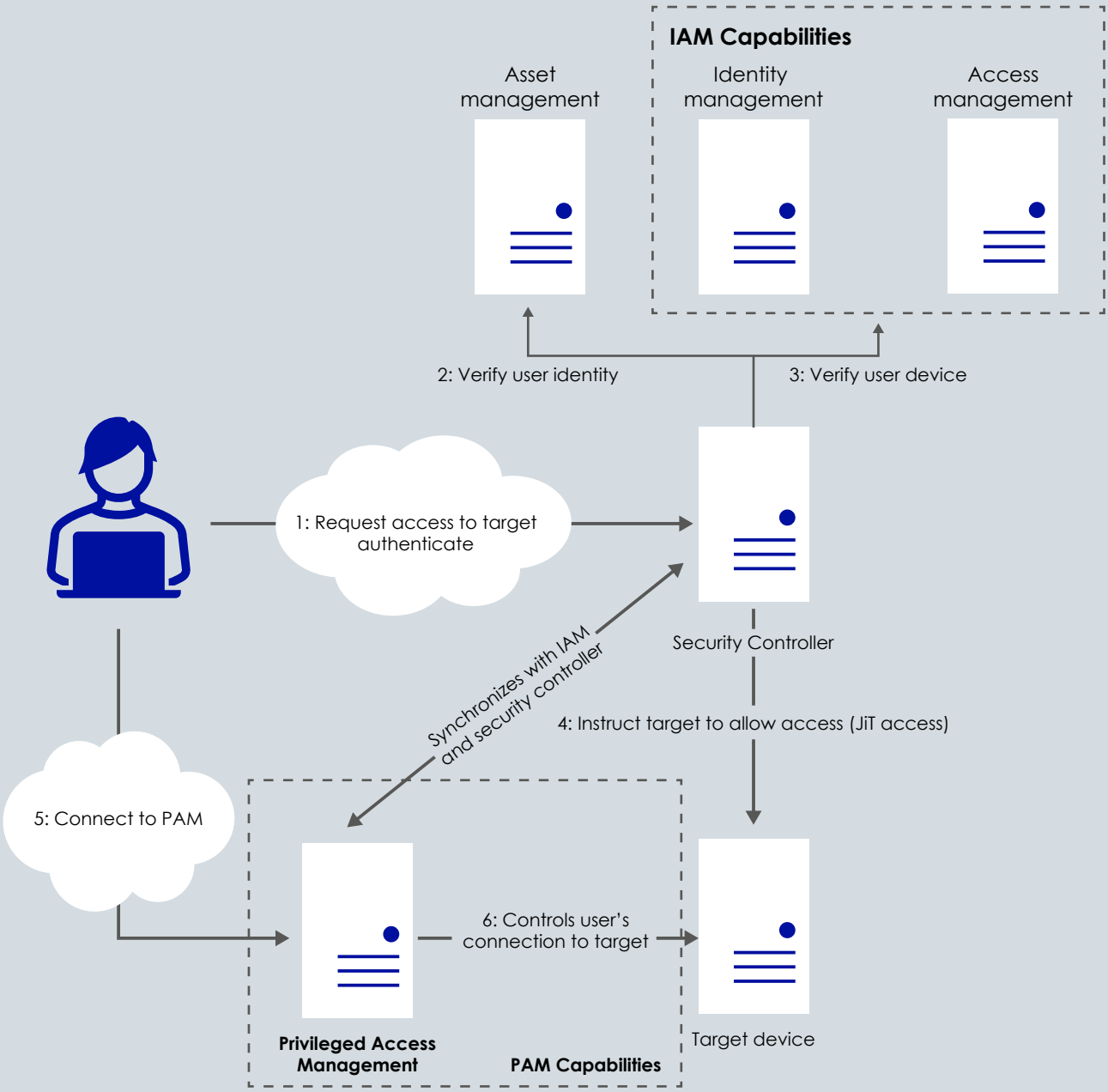
IAM brings controls that are indeed relevant for Zero Trust: It is highly recommended that Zero Trust access policies implement the **principle of least privilege** as well as **Just-in-Time (JiT)** access. With these two principles implemented, users should have no standing authorizations but are instead evaluated against authorization polices on a per-request-basis, to determine if their request should be fulfilled or not. This is very related to the mantra of *Never trust* within Zero trust – users are not inherently trusted and are verified for authorization at every request instead.

Privileged Access Management
Another particularly interesting aspect of IAM and Zero Trust is privileged access ie. actions that reach beyond capabilities of regular users: Privileged access should be treated with extra care, due to the increased impact if a privileged account is compromised or abused. To mitigate the high risk associated with privileged access, Privileged Access Management (PAM) tools, processes and controls can be leveraged. PAM is well in-line with Zero Trust methodology, since Zero Trust aims to establish trust based on the risk-level of the user's request, matched against the access policies.

Due to the nature of privileged access requests being higher risk, Zero Trust mandates stronger access controls and a more restrictive access policy to be applied to privileged access requests. For this reason, PAM is highly relevant because PAM tools can be used to implement password-less access, JiT access and least privilege as well as help detect risky or malicious activities and provide strong audit trails for privileged users. PAM is therefore crucial to enhance user and authorization management and security for the users with the highest risk profiles within the organization.

On the next page you will find a conceptual Zero Trust model showing the user's request to gain server administrative access to a target server. In this scenario, the request prompts interaction with the Zero Trust security controller which in turn integrates with the Zero Trust components to evaluate and grant or deny access. As the figure shows, several of the Zero Trust components involved are within the IAM and PAM domains.

Figure 3:
How IAM relates to Zero Trust



Source: ICY Security

Getting started with IAM-Zero Trust

Getting started with a Zero Trust Journey can be a daunting yet important task. We recommend leveraging what you already have, to avoid having to start from scratch. As previously discussed, IAM and PAM capabilities can be utilized to provide some of the core functionality of Zero Trust security, albeit IAM and PAM should be perceived as part of a greater whole and not standalone solutions that can provide Zero Trust alone.

We recommend considering Zero Trust as three major activities:

1. Network-based Zero Trust: This includes activities that are classically known as micro segmentation and software defined networking.
2. Identity-based Zero Trust: Activities related to asset, identity and access management to build a strong identity story enabling verification in a Zero Trust hostile environment.
3. Building a security management plane or security control system to integrate network security with identity security, enabling the two domains to provide a unified Zero Trust experience.

With these three primary activities in place, you are well underway on your Zero Trust journey, leveraging your existing IAM and PAM capabilities for a head-start.

Want to know more?

If you want more information about Zero Trust and suggestions on solutions to support your Zero Trust journey such as utilizing Identity Governance and Administration and Privileged Access Management, contact ICY Security at

www.icysecurity.dk

ICY
Security