IDENTITY DEFINED
SECURITY ALLIANCE

WHITEPAPER

THE PATH TO ZERO TRUST STARTS WITH IDENTITY

INTRODUCTION

The concept of Zero Trust is not new. Some call it a movement, while others call it a model. No matter what your point of view, Zero Trust is a reality. Recently, Zero Trust has taken on a larger than life persona fueled by the endless cycle of data and identity breaches in the news, big buzz from vendors preaching their technologies, and the customer rush (and often knee-jerk reaction) to adopt a Zero Trust strategy.

While there are many references and publications describing Zero Trust, for the most part, they articulate security from a single vendor's vantage point. This whitepaper represents the collective experience and thought leadership of the Identity Defined Security Alliance (IDSA), which represents over 20 identity and security vendors, and offers a unique and practical approach to understanding Zero Trust. At the core, the IDSA believes that identity serves as the keystone in any Zero Trust based strategy.

In order to clarify the haze surrounding Zero Trust, we must explain the core principles of Zero Trust from a practitioner's point of view. More importantly, we need to understand the core technology blocks that Zero Trust relies on, and the benefits it offers in the context of identity-centric frameworks.

A BRIEF HISTORY OF ZERO TRUST

When the Jericho Forum was founded in 2004, its mission was to define the problem and solution for de-perimeterization. In 2010, Forrester analyst John Kindervag coined the term "Zero Trust" in his research – emphasizing that all network traffic is untrusted and that any request to access any resource must be done securely.[1] The original concept of Zero Trust was based on a data-centric network design that leveraged micro-segmentation to enforce more granular rules and ultimately limit lateral movement by attackers.

As the concept of Zero Trust continued to evolve, a more identity-centric approach started to gain prominence. This trend accelerated with the adoption of mobile and cloud technologies. In 2014, Google published its BeyondCorp model as part of a research project motivated by Google's own initiative to implement Zero Trust for its employees. The approach revolves around the idea that perimeter security and a protected intranet is no longer sufficient. In doing so, the BeyondCorp model shifts access controls from the perimeter to individual devices and users. For many enterprises embracing this model, the primary objective is to remove the need for a traditional VPN, while still allowing users to work securely from any untrusted network.[2]

Since inception, the concept of Zero Trust has extended the original model beyond traditional infrastructure, databases, and network devices, to include cloud environments, big data projects, DevOps environments, containers, and microservices. Analysts across the board have all revised and enhanced their approaches, including Gartner, who in 2017, evolved their Adaptive Security Architecture to CARTA - Continuous Adaptive Risk and Trust Assessment, which provided a framework to manage risk, while taking advantage of the new digital world.[3]

In 2018, Forrester analyst Dr. Chase Cunningham and his team published the Zero Trust eXtended (ZTX) Ecosystem report which extends the original model beyond its network focus to encompass today's ever-expanding attack surface. The extended ecosystem includes the following elements and associated processes:[4]

- Zero Trust Networks
- Zero Trust Data
- Zero Trust Workloads
- Zero Trust Devices
- Zero Trust People
- Automation and Orchestration
- Visibility and Analytics

In all cases, the approaches are becoming increasingly more risk-based and identity-centric.

IDENTITY AT THE CENTER

When conducting post-mortem analysis, it becomes apparent that today's breaches are not highly sophisticated. Cyber criminals no longer hack into enterprise networks; they target the weakest links and simply log in using stolen or otherwise compromised credentials. Once inside the target network, criminals expand their attack and move laterally across the network, hunting for privileged accounts and credentials that help them gain access to the organization's most critical infrastructure and sensitive data.

It only takes one compromised credential to potentially impact millions — whether it's millions of individuals or millions of dollars. Undeniably, identities and the trust we place in them, are being used against us. Identity has become an Achilles heel for cybersecurity practitioners. In fact, over 80 percent of security breaches involve privileged credentials according to Forrester Research.[5] According to Gartner, 65 percent of enterprises allow for the unrestricted, unmonitored, and shared use of privileged accounts.[6]

The easiest way for cyber-attackers to gain access to sensitive data is by compromising a user's identity, which should be a driving principle for Zero Trust which includes users, service accounts, IoT devices, etc. If a stolen identity belongs to a privileged account that has broader access, or the "keys to the kingdom," the potential for damage is much worse.

WHERE TO START

While implementing Zero Trust is a journey that cannot be achieved overnight, it also doesn't require a complete redesign of existing network architectures. Models like Google's BeyondCorp can be achieved by gradually modifying current infrastructures over time and augmenting existing security controls. But where do you start?

This is where the IDSA comes in. The IDSA is a consortium of identity and security vendors with components designed to secure the network, data, devices, workload, and people (also known as identity), while providing visibility into security threats and automating, as well as orchestrating remediation.

Securing only endpoints, firewalls, and networks provides little protection against identity and credential-based threats. Until organizations start implementing identity-centric security measures, account compromise attacks will continue to provide a perfect camouflage for data breaches. Thus, the initial step in your Zero Trust strategy should be focused on:

- Granting access by verifying who is requesting access
- Understanding the context of the request
- Determining the risk of the access environment

This never trust, always verify, enforce least privilege approach provides the greatest security for organizations.

IDSA FRAMEWORK

In order to shift away from the large corporate perimeters, with layered-in or bolted-on compensating security controls, Zero Trust forces enterprises to evolve to a model made up of many micro perimeters at each identity domain. Instead of building many layers of security from the outside in, Zero Trust proposes the idea of protecting data from the inside out and building out security controls only where you need them.

In other words, rather than focusing on a perimeter-based defense, practitioners should focus the controls on sensitive data stores, applications, systems, and networks themselves; thereby directly guarding assets that matter. The goal of the IDSA is to define a framework for Identity Defined Security that provides practitioners with a set of fundamental building blocks along with blueprints and best practices that help achieve security outcomes that support the needs of the business.

Identity Defined Security Outcomes

An Identity Defined Security Outcome is a desired result that improves an organizations security posture through identity-centric security and reduces the risk of a breach or failed audit.

Identity Defined Security Approach

Identity Defined Security Outcomes can be achieved through many different Identity Defined Security Implementation Approaches. These approaches are well-defined patterns combining identity and security capabilities that help organizations leverage an identity context to improve security posture.

Best Practices

The foundation of an identity-centric approach to security ideally begins with a mature Identity and Access Management (IAM) program but is not always required. An initial set of best practices defined by the IDSA focused on IAM fundamentals, serve as recommended hygiene tips related to the people and process, as well as the technology aspects of an IAM program, and augment the foundation of an identity-centric approach to security.

Identity Defined Security Technology Components

The Identity Defined Security Technology Components are similar to those used in many discussions around digital transformation, hybrid access, Zero Trust, etc. These core technology components serve two main purposes. They capture the different ways data is accessed across technology components illustrating the interaction between various actors (users, processes, etc) and the target data. They also provide the foundation for the Identity Defined Security Reference Architecture.

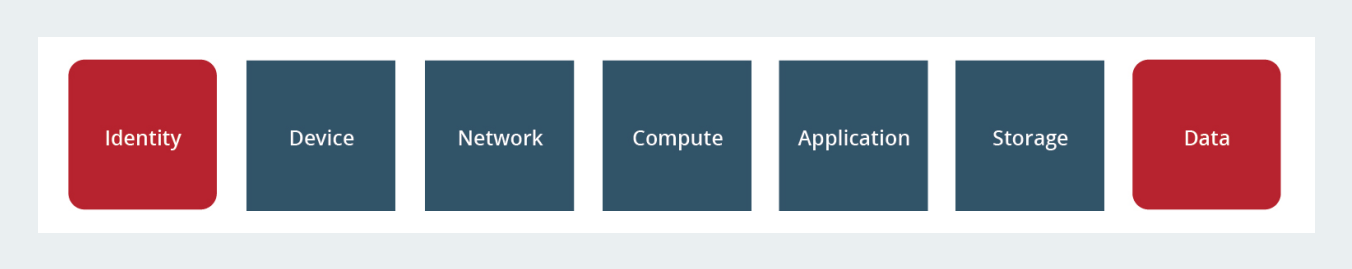

Figure 1: Identity Defined Security Technology Components

Identity & Data

Information security has been around for thousands of years, even back in medieval times where kingdoms were using new technologies to protect information such as ledgers, holy books and jewels (e.g. hardened fortifications, motes, and drawbridges). The mission has not changed, however many of an enterprise's crown jewels are now digital and protected with modern technologies (e.g. encrypted data stores). The difference between today and 1,000 years ago, is the amount of data we create and our inability to properly classify each "byte" of it, and that this data can be stored in multiple locations simultaneously.

At the heart of a Zero Trust strategy is to only allow entitled people access to appropriate resources (data) with proper authorization. Identity Defined Security begins with "identity" whose objective is to get access to "data" – represented by the two red boxes in the Figure 1. Identity is the "actor" in most transactions. Access to data includes retrieval, deletion and modification of data. An identity is not restricted only to human users, as processes often act on their own to access valuable data and must be considered as a valid "actor."

A Zero Trust approach must focus on protecting the company's most sensitive data first. When taking inventory of a company's data, sensitive data is usually a very small subset (e.g. customer data, financial, HR). Practitioners should ensure that all users who have access to this data are:

- Entitled to access the data
- Properly authenticated
- Properly challenged when necessary by additional factors of authentication

Another aspect to consider when identifying users, is their behavior. Users typically use the same resources with a regular pattern of activity. If a user has any anomalous behavior detected, such as a device being used in a different location, too many failed log-on attempts, or the user is trying to access a resource they don't typically use, the user should be prompted for additional and stronger factors of authentication.

Devices

Within the Zero Trust construct, it is important to recognize that devices that access data have identities as well. These devices include laptops, desktops, mobile devices and any other endpoint an end user might use on the network.

It is important for the enterprise to understand the device's posture when accessing the network in order to provide proper device level authentication and authorization. For instance, is the device properly managed by your enterprise with a hardened and secure OS image, virus protection, patching, an encrypted disk, and endpoint protection? Or is the device an unmanaged personal device (i.e. phone or laptop). Depending on the type of data that the user is accessing with his or her device, it may not matter. If the user only has access to non-sensitive or public information, the enterprise may not care that the device might have malware installed. However, if the user is trying to access sensitive financial or customer data, access should only be given to those devices that are managed, trusted and protected.

Network

The Network component includes technology related to the grouping of host servers, data connections, interfaces between hosts, network segmentation, intrusion detection, cryptography of flows between hosts (e.g. SSL, VPNs), and can also include more abstract concepts like "time of day" and proximity of multi-factor mechanisms in relation to the network. Within the Zero Trust construct it is important to understand that the network has an identity as well, in terms of whether it is trusted and the time of day that data is being accessed. An enterprise may have different access policies based on the location of the network traffic. For instance, if a user is trying to access sensitive data from a coffee shop on a public network, an enterprise may have a policy where that access is denied. By virtue of understanding the location of endpoints, security engineers can group sensitive on-premises resources into their own segments, and only give access to those users and roles that are both appropriate and authorized.

Compute & Application

The Compute and Application components are often seen as a single workload component that includes the operating system. The security focus is around hardening the endpoints, operating system, data loss prevention (DLP) and application security. Within the Zero Trust construct it is important to understand that the application is typically the interface to the data and that access controls need to be considered for this component – either course or fine grain access control depending upon the need. If the application is developed from a commercial vendor, either web-based or on-premises, there is likely a way to configure tighter controls for privileged roles that need access to sensitive data. If the application is homegrown or legacy, there is an opportunity to build in additional access controls to protect access to sensitive data. Regardless of where your workload resides, there is an opportunity to refine your access policy. Also, it is unlikely that all access policies can be managed in one place. Therefore, policies may need to be updated across multiple components (e.g. IAM, privileged access management, cloud access security broker, SaaS, on-premises applications). Additional steps can be taken to enhance trust in this domain. For example, use of smart cards, secure elements, trusted execution environment (TEE), and secure enclave computation (e.g. those based on Intel SGX) can make applications more trustworthy.

Storage

Data by itself cannot enforce security. The storage holding the data is one place where data security needs to be enforced. From a Zero Trust perspective, storage is an extremely important component that needs to be protected, especially when data is sensitive. If there is an ability to add additional controls around storage subsystems as well as sensitive data, it should be considered. The focus on storage security or data security has traditionally been around protecting the data "at rest" – ensuring proper data encryption, data masking, secure backups, etc., these can involve software and hardware-based mechanisms. The main goal is to protect storage from unauthorized access which includes modification, corruption and deletion. In many cases, enforcement of data security is a combined effort between the storage component and the application component. Access to data in the SaaS world is inexorably tied to the application interface which requires additional controls in place.

EXAMPLE IDENTITY DEFINED SECURITY SCENARIOS

With these core components established, scenarios capturing the different ways data is accessed can now be defined. The main focus here is to capture the correct components and to illustrate the interaction between the actor and target data.

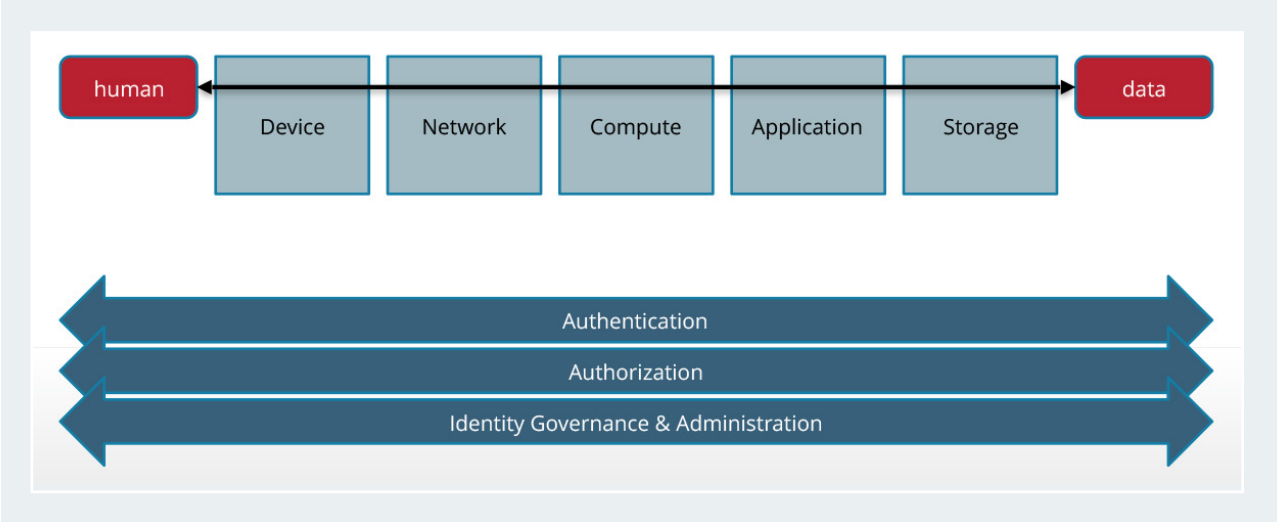

Figure 2: "Human to Data" Scenario

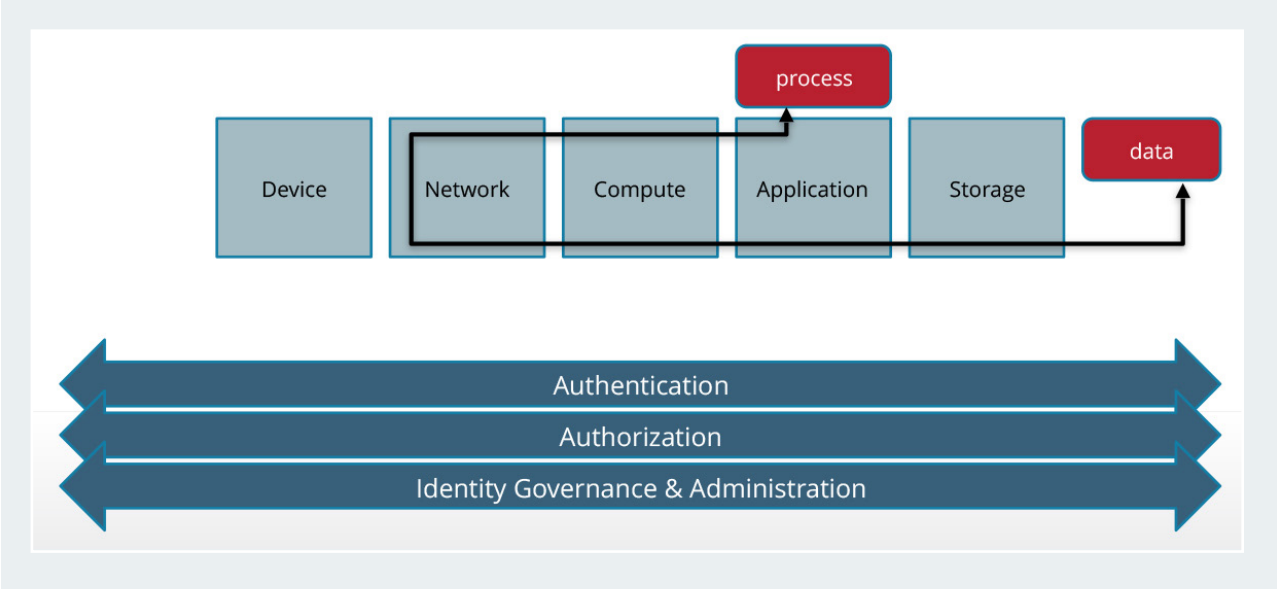

Figure 3: "Application/Server Process to Data" Scenario

Figures 2 and 3 are examples of high-level scenarios that provide a framework to achieve security outcomes on top of which approaches can be defined across components of the Identity Defined Security reference architecture. This reference architecture is illustrated in Figure 4.

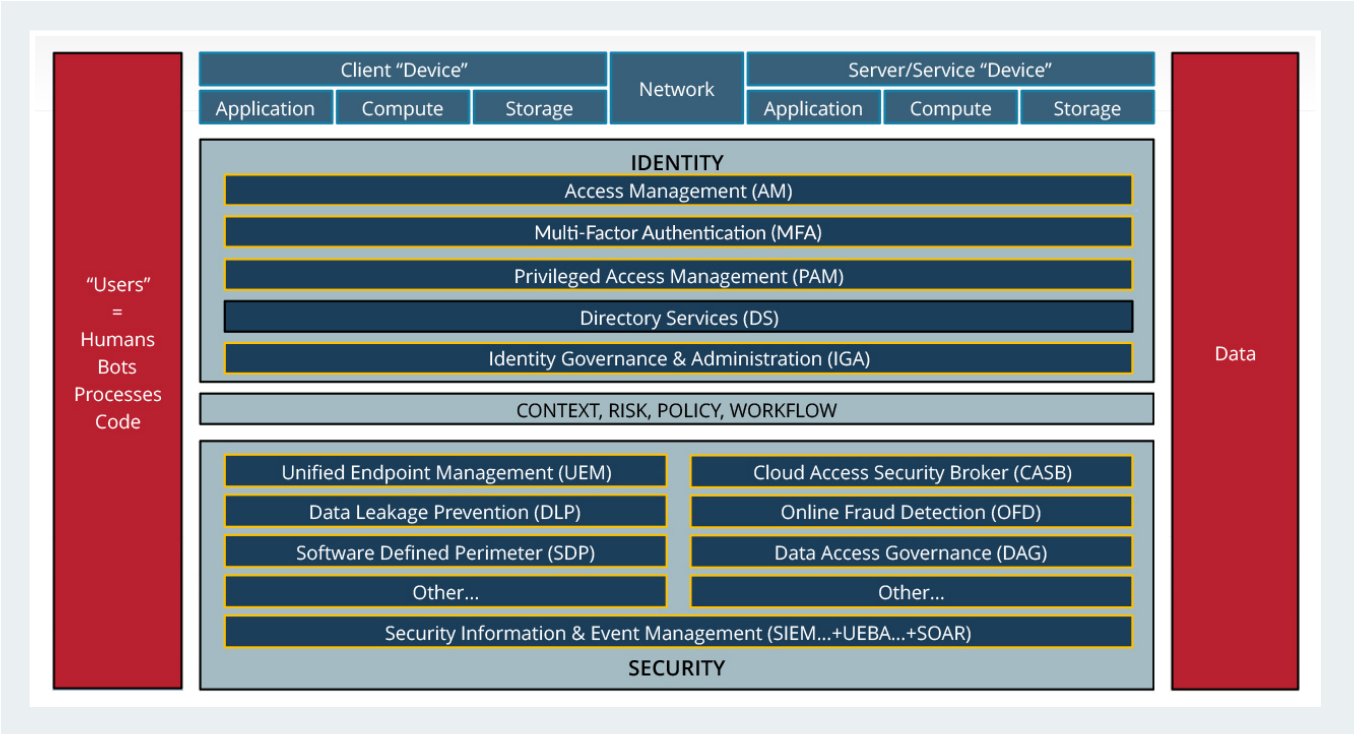

Figure 4: Identity Defined Security Reference Architecture

EXAMPLE SECURITY SCENARIOS

With this reference architecture, well-defined patterns combining identity and security capabilities, also known as identity defined security approaches, can be used to construct your Zero Trust strategy. They provide concrete patterns for practitioners on how to leverage two or more of the identity and security components within the architecture. Here are a few examples of security approaches to achieve security outcomes related to Zero Trust:

Outcome: All Privileged Access Requires Multi-Factor Authentication

Description: Privileged accounts are accounts that have special rights (e.g. admin rights) or are regular user accounts but are more sensitive because of the high impact in case of breach (e.g. CEO account).

Value: Provides additional security for accounts that are accessing the most sensitive assets.

Approach: Delegated MFA using an external identity provider.

Components: Multi-factor Authentication (MFA) + Privileged Access Management

Description: The MFA capability is loosely integrated between the solution that offers privileged access, and an external identity provider, using the following protocols:

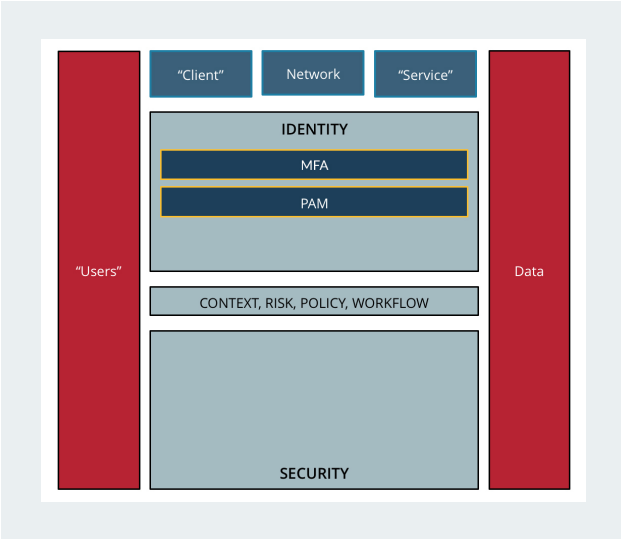

Figure 5: Approach using AM and PAM.

1. Federated model using SAML
2. Federated model using OIDC
3. Non-federated model using RADIUS

In all cases, privileged access is granted only after a successful MFA response from the Identity Provider.

Outcome: Access is revoked upon detection of a high-risk event.

Description: Security related alerts or events captured by systems indicating that a potential breach of policy has occurred should result in the violating identities access being revoked in an expedited manner.

Value: Organizational exposure to defined policy breaches is monitored and reduced.

Approach: Integration of systems with security monitoring capabilities with identity provisioning capabilities

Components: Security Information and Event Monitoring (SIEM) + Identity Governance and Provisioning (IGA)

Description: A SIEM deployed in an organization's environment with security monitoring capabilities is integrated with Identity Governance initiating the remediation provisioning process.

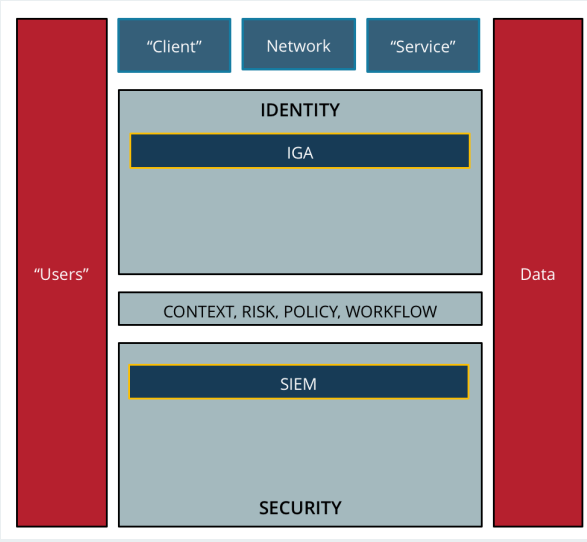

Figure 6: Approach using IGA and SIEM.

1. A security policy is defined
2. Monitoring tool detects user violation of this policy
3. Monitoring tool creates alert/event
4. Details of alert/event sent to Governance solution
5. Governance solution revokes user entitlements/permissions used in violation through certification or direct de-provisioning
6. User cannot continue to violate policy based on reduction of entitlements

CONCLUSION

Despite its origin almost 15 years ago, Zero Trust is more relevant today due to the distributed and virtual nature of the world that we live in. Our user communities have expanded, the amount of data being created is growing exponentially, and the traditional network perimeter has disappeared. It's no longer feasible to protect our most sensitive assets behind a single network wall and the fast path for a hacker to acquire data is through a compromised identity. If we approach Zero Trust by leveraging identity-defined security concepts, we are protecting the weapons that are being used against us.

Forward thinking organizations are achieving Zero Trust through the integration of existing identity and security technologies. They have implemented architectures that share identity context and provide risk-based access to critical resources, improving security without compromising the user experience. Learn more about how these organizations are succeeding.

Identity-defined Zero Trust is a complex topic that touches almost every aspect of an organization's IT and security infrastructure. We'll be exploring additional elements including best practices to prepare for identity-defined Zero Trust, core methods, and how to approach deployment in enterprise organizations through upcoming blogs, webinars and whitepapers. Join our on-line community to stay in touch and contribute to these ongoing initiatives.

ABOUT IDSA

The IDSA is a group of identity and security vendors, solution providers and practitioners that acts as an independent source of thought leadership, expertise and practical guidance on identity centric approaches to security for technology professionals. The IDSA is a nonprofit that facilitates community collaboration to help organizations reduce risk by providing education, best practices and resources.

We deliver on our mission through…

1. Cross vendor collaboration
2. Thought leadership content
3. Identity Centric Security Framework
4. Customer implementation stories
5. Virtual community for sharing experiences and validation

For more information about the IDSA visit www.idsalliance.org.

REFERENCES

1. Kindervag, Forrester Research: Build Security Into Your Network's DNA: The Zero Trust Network Architecture, 2010

2. Ward, Byers, Google, BeyondCorp: A New Approach to Enterprise Security, 2014

3. McDonald, Ahlm, Krikken, Gartner, Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats, 2017

4. Cunningham, Forrester, The Forrester Wave™: Zero Trust eXtended (ZTX) Ecosystem, 2018

5. Forrester, The Forrester Wave™: Privileged Identity Management, Q4 2018

6. Kelley, Gaehtans, Gartner, Best Practices for Privileged Access Management Through the Four Pillars of PAM, 2019