# THE GUIDE TO IDENTITY DEFINED SECURITY

IDENTITY DEFINED
SECURITY ALLIANCE

# TABLE OF CONTENTS:

# 1. WHY READ THIS EBOOK?

Being a security leader in today's dynamic environment is a challenge. They are constantly fending off increasingly sophisticated attacks, usually with limited resources and minimal Board support. The attack surfaces are expanding as organizations support a remote workforce, adopt cloud strategies, and take on digital transformation initiatives. The consequences of a breach are shifting from reputational damage, which can indirectly impact profits, to significant financial penalties in the form of fines or ransomware payments.

The vast majority of data breaches making headlines are the result of a compromised credential. Capital One, SolarWinds, and Colonial Pipeline, to name a few. These breaches often involved poor identity security, such as weak or previously compromised passwords, not leveraging multi-factor authentication and single sign-on, or leaving standing privileges open. According to the *2021 Trends in Securing Digital Identities* report, 79% of organizations reported suffering an identity-related breach within the last two years, and 93% believe they may have prevented or minimized security breaches if they had implemented specific identity-related security outcomes.

This ebook will discuss the challenges facing organizations today, why an Identity Defined Security program is essential, and the steps to get started leveraging the Identity Defined Security Framework. Read this ebook for advice on reducing the risk of a breach while at the same time helping your organization transform how you do business and, more specifically, if you:

- Have experienced an identity-related breach in the last two years.
- Are developing a security strategy that focuses on reducing the risk of an identity-related breach.
- Are considering or implementing a Zero Trust approach with a focus on improved user experience and identity security.

> **"Identity-related attacks continue to be the hacker's favorite technique, as stolen or compromised valid credentials are an easier and stealthier way of gaining persistent access. As practitioners, the 2021 Trends Report is encouraging and supports our decision to prioritize strong identity-focused security controls like the ones recommended by the IDSA."**
>
> ***- Clint Maples, CISO, Robert Half***

# 2. WHY IDENTITY DEFINED SECURITY?

The challenges posed by the worldwide pandemic and the need to support a distributed, remote workforce have highlighted the need for improved identity security. The increased use of cloud services and personal devices means more users have the ability to access data from anywhere using systems that may not be under corporate control. Managing access using a traditional perimeter-based approach is no longer feasible. Combined with the prevalence of credential theft, these factors make putting identity at the center of security strategies vital.

Today's investments in security solutions are yielding some positive results, but several emerging forces play a role in complicating security and expanding the attack surface.

Organizations and external threats have been evolving in numerous ways, including:

- Explosion in users, devices, identities (human and non-human), and environments (multi/hybrid cloud)
- Workforces that are overwhelmingly outside of the network perimeter
- Increased interconnectedness with customers and partners
- Massive amounts of data outside of IT controls
- Consumer-oriented technologies and concepts moving into the enterprise
- Malicious actors are becoming more sophisticated and organized
- Insider threats that are as real and perhaps even more lethal than outsider attacks

This explosion of cloud, mobile devices, and connected things, as well as the consumerization of information technology (IT), has increased the risk of cybersecurity attacks due to compromised identities, accounts, and credentials.

> **"Safeguarding identities is not just about preventing attackers from penetrating your network. It is also about limiting the damage they can do once they are inside your environment,"**
>
> ***- Den Jones, Senior Director of Enterprise Security, Cisco***

## The numbers speak for themselves

**81%**

of hacking-related breaches leverage weak, stolen, or otherwise compromised credentials.

***[Verizon Data Breach Investigations Report]***

**79%**

of organizations have experienced an identity-related security breach in the last two years, and 93% said they were preventable with better identity-related security controls

***[Identity Defined Security Alliance]***

**74%**

of data breaches involve access to a privileged account.

***[Centrify]***

**73%**

of users use the same password for multiple sites, and 33% of people use the same password every time.

***[DigiCert]***

**$51-$72 Billion**

in losses to the worldwide economy could be eliminated through the proper management and protection of identities.

***[AIR Worldwide]***

A high-profile breach can lead to significant financial and reputational harm. Many of these incidents can be traced back to a stolen credential or abuse of privileges. While attackers focus on ways to compromise passwords, the pressure is on for enterprises to protect the human and machine identities in their environment. However, while the number of users and devices that need to be secured presents a challenge, it also presents an opportunity.

Organizations that adopt an identity-focused approach can create a more flexible, secure, and productive workforce. With the traditional perimeter effectively dead, identity is the connective tissue that binds together systems, users, and applications. By laying the groundwork with an effective identity and access management architecture supported by technologies such as multi-factor authentication, single sign-on, and user activity monitoring, organizations can embrace the cloud, BYOD culture, and a remote workforce more confidently.

A comprehensive strategy for protecting identities and the resources that are being accessed is essential to combatting today's threats and enabling organizations to digitally transform their operations while staying secure.

# 3. PROTECTING IDENTITIES AND THE RESOURCES THEY ACCESS

This new approach to cybersecurity is grounded in four foundational concepts:

- Identity is a critical cybersecurity technology
- All aspects of cybersecurity must fundamentally work together if they are to achieve meaningful effectiveness
- Every business transaction, attack surface, or target involves a credential and a service or piece of data
- Given the cumulative investment in security, each new investment is increasingly measured for its ability to make the whole more effective

It's these foundational concepts that have led to a new way of thinking about security – threading identity through end-to-end cybersecurity investments. This new approach:

- Leverages increasingly open and API-first technology stacks
- Steers the focus away from single point defense mechanisms to include a broader set of identity and security components
- Delivers a fresh, balanced set of detective and preventive controls
- Enables organizations to tackle security with a more precise, identity-aware, and identity-specific approach

There is a general realization in the industry that two distinct but related disciplines are at play in the world of identity. The first is the lifecycle, definition, and protection of an identity itself that we will refer to as **Identity Security**. The second is the use of identity in a contextual manner when enforcing security across various components of the stack that carry out an action or transaction, which we will refer to as **Identity Defined Security**.

## Identity Security: Establishing a Trusted Identity

***Identity Security: Protect and properly manage an identity and its related credentials.***

The term "identity security" is not new, but the concept of managing an identity and its related attributes throughout the identity lifecycle, also known as the "joiner, mover, and leaver" cycle, has become a widely adopted discipline. The types of identities have evolved to include humans with elevated privileges, as well as non-human (or machine) identities that encompass physical devices, applications, and processes, just to name a few.

Identity Security ensures that identities are properly set up and protected. An identity, be it human or non-human, is typically associated with one or more identifiers and a set of attributes. Identity Security means making sure the identity being referenced is not compromised. An identity can be compromised when it falls into the wrong hands or is misused in the "right" hands. Therefore, preventing identity compromise means we prevent gratuitous disclosure of personal information and make sure it cannot be used to impersonate a general or privileged user.

# Identity Defined Security: Protecting Access to Resources through Identity

***Identity Defined Security: Use a trusted identity to protect other resources in the system.***

Identity Defined Security relies upon the use of a trusted identity and its context propagating downstream to the various enforcement points to further protect and secure other assets. These assets can be confidential data, guarded resources, or applications that are protected by a set of access policies. The policies dictate which identity or groups have access to the resource, for how long the access should be granted, and any special factors that can limit this access. These factors can be dynamically adjusted, but this adjustment is always a function of the identity making the request. As such, identity security is a prerequisite of Identity Defined Security. Furthermore, unlike identity security that only deals with the establishment and protection of the identity itself, Identity Defined Security or identity-centric security applies to everything that validates the trust of an identity.

While Identity Security can protect an identity through mechanisms such as multi-factor authentication or identity proofing and reduce the risk of impersonation, we know that bad actors are working to stay one step ahead of these controls and, in some cases, are trusted insiders.

However, through Identity Defined Security, additional security controls can be applied to protect the resources being accessed in the event a bad actor is able to impersonate a legitimate user. For example, allowing access to cloud data based on the identity of the entity making the request or analyzing user behavior and comparing it to a baseline before granting access to an application.

The remainder of this ebook will focus on Identity Defined Security and how to implement it in your organization.

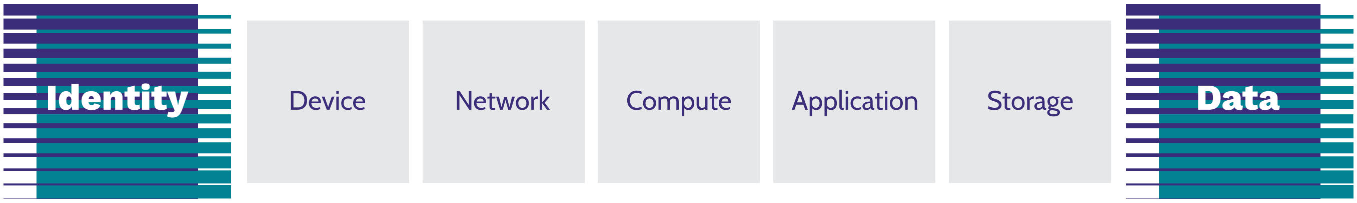
## How it works

With users accessing and interacting with enterprise networks in so many ways, integrating the Identity and Access Management (IAM) infrastructure with security solutions enables businesses to make more intelligent decisions about access and policy enforcement.

Critical to this strategy is the ability to propagate the identity context between the actor and the resource through different technology layers, such as endpoints, applications, APIs, and network infrastructure. Details such as geographic location, device characteristics, and login attempts all represent pieces of a transaction and should follow the user as he or she tries to access a particular application or system.

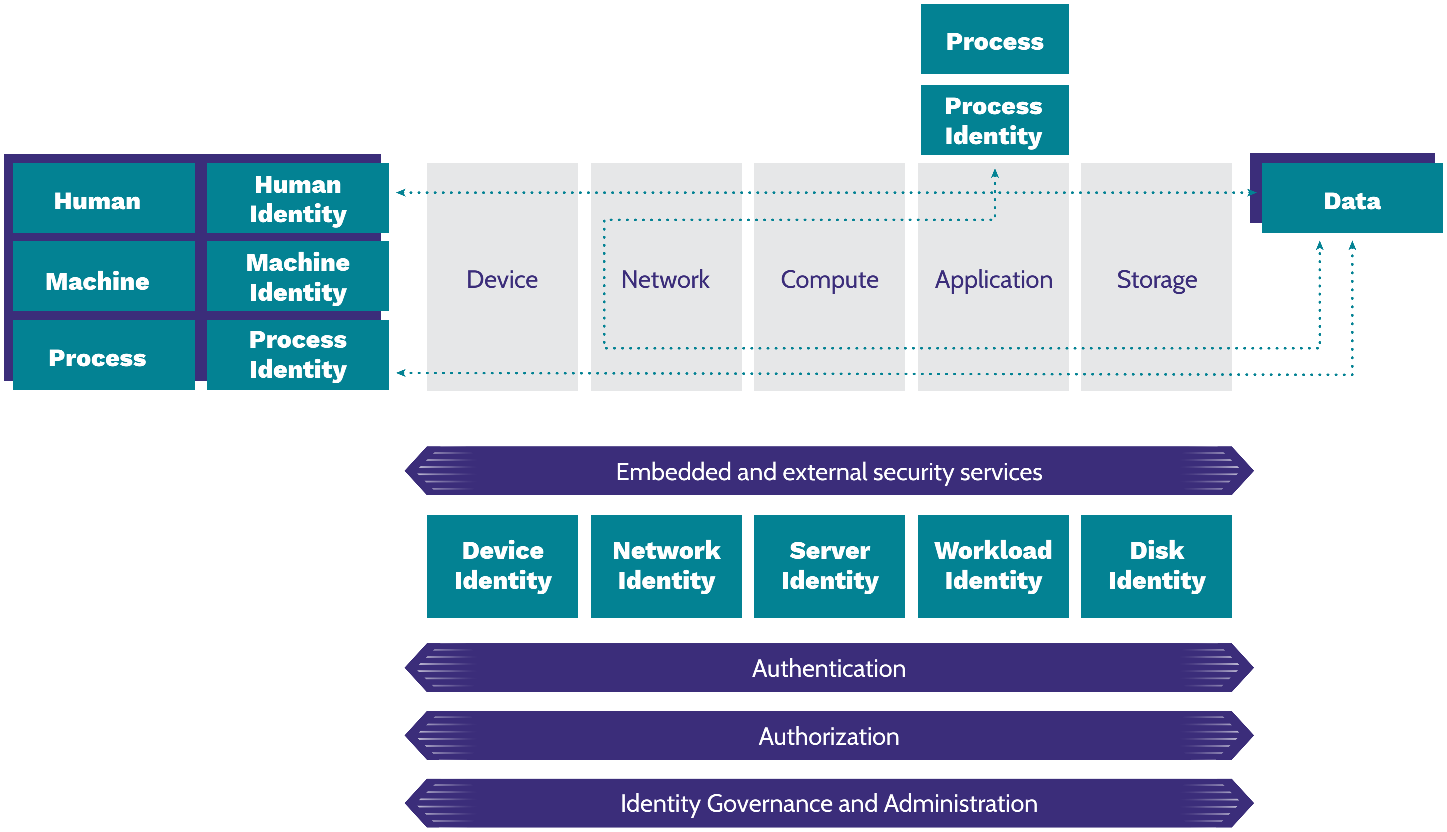
It starts with a set of core technology components. These components are similar to those used in many discussions around digital transformation, hybrid access, Zero Trust, etc. These core technology components serve two primary purposes. They capture the different ways data is accessed across technology components, illustrating the interaction between various actors (users, machines, processes, etc.) and the target data.

Identity Defined Security begins with an "identity" whose objective is to get access to "data," as represented by the two red boxes in the figure below. Identity is the "actor" in most transactions.



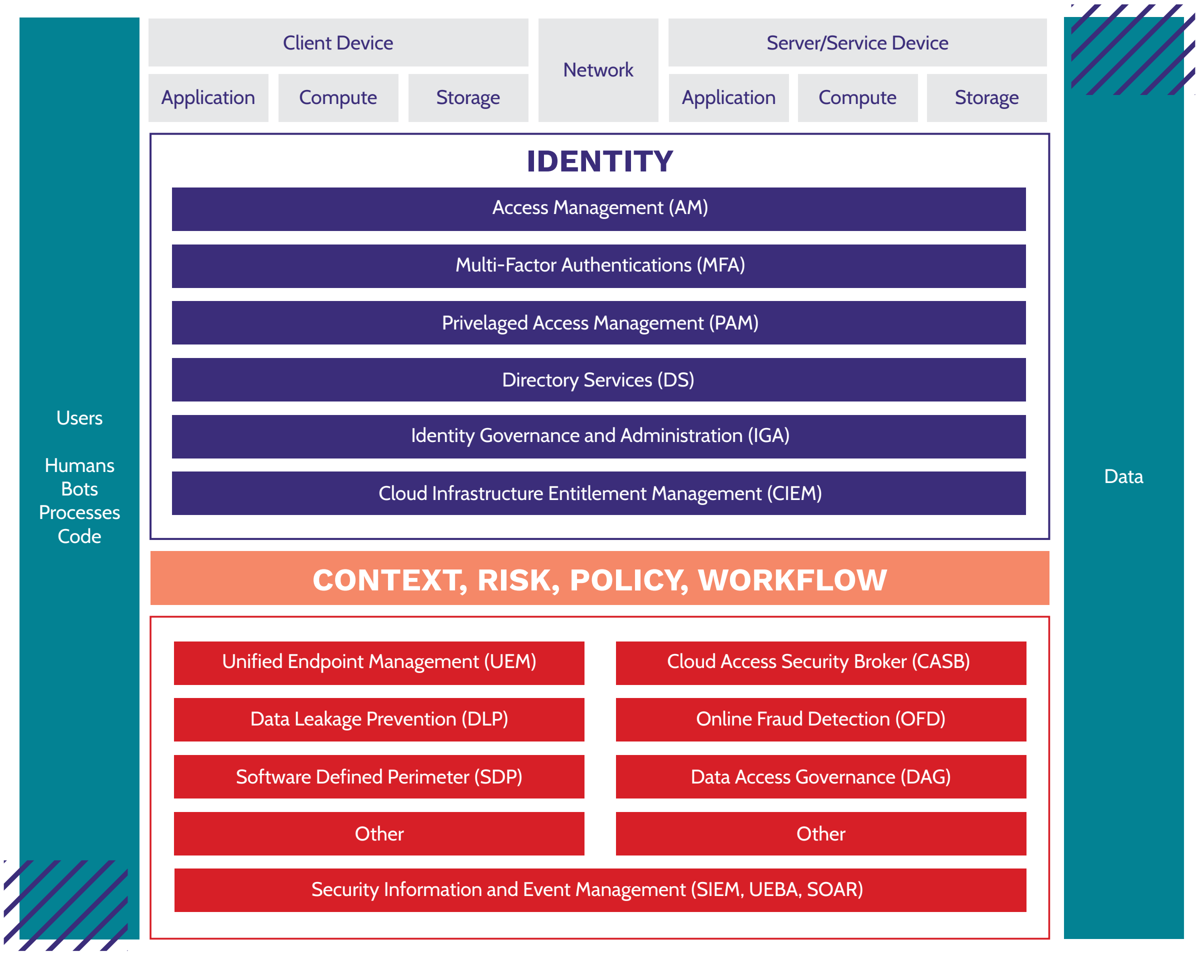
*Identity Defined Security Technology Components*

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 illustrate the interaction between the actor and target data. Access to data includes retrieval, deletion, and modification of data. An identity is not restricted only to human users but also includes machines and processes. Since they often act on their own to access valuable data, they must also be considered as a valid "actor."



*Identity Defined Security*

These high-level access scenarios depicted for humans, machines, and processes can provide the foundation for defining desired security outcomes, which can be achieved by leveraging the Identity Defined Security Reference Architecture illustrated below and the Identity Defined Security Framework.


Client Device
Application
Compute
Storage
Network
Server/Service Device
Application
Compute
Storage
Users
Humans
Bots
Processes
Code
IDENTITY
Access Management (AM)
Multi-Factor Authentications (MFA)
Privelaged Access Management (PAM)
Directory Services (DS)
Identity Governance and Administration (IGA)
Cloud Infrastructure Entitlement Management (CIEM)
Data
CONTEXT, RISK, POLICY, WORKFLOW
Unified Endpoint Management (UEM)
Cloud Access Security Broker (CASB)
Data Leakage Prevention (DLP)
Online Fraud Detection (OFD)
Software Defined Perimeter (SDP)
Data Access Governance (DAG)
Other
Other
Security Information and Event Management (SIEM, UEBA, SOAR)

## Identity Defined Security Framework

The Identity Defined Security Framework, developed by the Identity Defined Security Alliance in collaboration with leading vendors, solution providers, and practitioners, provides organizations with practical guidance on implementing an identity-centric approach to security. It 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 organization's security posture through identity and reduces the risk of a breach.

### *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 solid IAM foundation but is not always required. An initial set of best practices defined by the IDSA focused on fundamentals serve as recommended hygiene practices related to the people, process, and technological aspects of an identity program and augment the foundation of Identity Defined Security.

# 4. HOW DO I GET STARTED?

According to the latest research (*2021 Trends in Securing Digital Identities)*, security is taking a broader role in identity and access management, with positive effects. Sixty-four percent report that they have made changes to better align security and identity functions within the last two years, and most organizations report that the CISO has an IAM leadership role, which leads to better alignment of identity and security functions. But ownership and awareness are just the first steps in implementing Identity Defined Security. The path to Identity Defined Security will vary by business drivers and maturity. The following is the recommended approach for how to apply the Identity Defined Security Framework in your organization.

## Assess your organizational IAM practices

Establishing an identity-centric approach to security will be simpler and more effective when built upon a few IAM best practices. We recommend reviewing the complete list of Best Practices provided in the Identity Defined Security Framework, paying specific attention to the following:

- **Governance** – establish committees that provide oversight and policies for an organization-wide program. As part of this process, emphasize the need for dialogue and cooperation between teams to prevent security and operational silos.
- **IAM Technology Stack** – focus on building out an identity stack across your organization that supports current and future business needs. Utilize the Identity Defined Security Reference Architecture as a starting point for assessing your IAM technology foundation – access management, privilege access management, multi-factor authentication, directory services, and identity lifecycle and governance.
- **Foundational Best Practices** –
    - ***Discover, define, and examine identity types.*** Identities are not just tied to human beings. When developing an identity-centric strategy, organizations should consider all forms of identity—from end-users to scripts to applications.
    - ***Identify vulnerabilities and risks associated with those identity types.*** This step involves assessing the risk posed by each of the identity types identified in the previous phase and any potential blind spots.
    - ***Ensure the uniqueness of every human and non-human identity in your directory.*** This is the DNA of your IAM program for every service and function you will support (provisioning, certs, privileged access, physical access, etc.) for on-prem (mainframe, AD, etc.) as well as all cloud providers (SaaS, CSP's).
    - ***Proactively maintain current and accurate authoritative data for identities in accessible source repositories.*** Authoritative sources for identities provide essential data to make informed decisions regarding user access, including what access to provision and when to enable/disable that access.

## Evaluate the current state of security outcomes and create a roadmap

As part of an organization-wide identity-defined security strategy, core identity-related outcomes should be prioritized and adopted throughout the organization. The Identity Defined Security Outcomes defined by the IDSA are intended to be a set of options to select from based on your organization's security challenges and current situation. All organizations should consider the following core functions.

- **Multi-factor authentication (MFA).** Deploying MFA capabilities for all users can't be stressed enough. Some companies avoid it because users don't like it or because it slows down productivity flow, yet it is the one outcome that should be deployed for every resource in an organization.
- **Privileged access reviews.** Accounts with privileged access are at the top of the food chain for cyber-attackers. Staying on top of who has expanded access is critical to protecting an organization's most sensitive assets.
- **Revoke access.** Revoke access immediately if there is a high risk associated with an identity or if the identity is no longer affiliated with the organization. High-profile data breaches and cyber incidents like SolarWinds are believed to be caused, in part, due to an orphaned identity.
- **Device characteristics for Authentication.** Information about the device being used to access resources can provide important clues as to whether the device or the identity has been compromised. One extra step in the authentication process because a device seems suspicious could prevent a breach.
- **User behavior.** All users have unique characteristics, whether it is the time of day they access accounts or their keystrokes when typing. Recognizing user behavior could help prevent many types of attacks that use a valid username and password.

Prioritize where to put your focus and budget according to your needs. Additional inputs into prioritization are available in the 2021 Trends Report, including the outcomes that could have prevented recent breaches and where companies are planning to invest over the next two years. Done well, each step of the road map will build upon previous efforts and maximize your security investment.

## Implement security outcomes

Once your roadmap is established, review and determine your implementation approach for each security outcome. Identity Defined Security Approaches are well-defined patterns that combine identity and security capabilities, providing flexibility in how outcomes can be achieved.

Each implementation approach provides the technology components and prerequisites required, as well as the IDSA members who support the approach. The technology components required for each implementation approach can also be used to guide the build-out of your IAM technology stack.

Make it a habit to periodically reevaluate where you are on the journey to Identity Defined Security. As your organization grows, the best way to achieve identity-centric security may change too.

# 5. APPLYING IDENTITY DEFINED SECURITY TO ZERO TRUST

Layer each of these security outcomes on top of one another, and you will have a foundation for Zero Trust. As the name implies, Zero Trust revolves around building a security architecture where devices, users, and services are not trusted by default. Whereas the traditional approach to perimeter security assumed that only traffic from outside the organization's network should be untrusted, with Zero Trust, all traffic is treated the same way.

Identity is at the core of Zero Trust. Fundamentally, Zero Trust is about making sure users, applications, and devices have the appropriate level of access to the network. Rather than build defenses from the outside in, Zero Trust layers security from the inside out by establishing micro-perimeters around sensitive data stores, applications, systems, and the network itself. Done correctly, it reduces the opportunities for threat actors to move laterally if they manage to penetrate the network and improves the chances of blocking malicious activity.

Identity-related attacks are posing a serious cybersecurity threat. Many of the breaches reported in the *2021 Trends in Securing Digital Identities* report were related to phishing attacks (68%). Respondents also cited inadequately managed privileges, brute force attacks, and social engineering, among other issues. Identity and access management is a critical security function, made all the more vital because of the increasing adoption of cloud services and mobile devices.

Responding to this threat landscape requires rethinking the traditional perimeter security model. Never trust. Always verify. Those words represent the motto of forward-thinking security organizations. That concept is at the root of Zero Trust. The IDSA's *2021 Trends in Securing Digital Identities* report also revealed that 93% of IT security experts felt that Zero Trust is strategic to securing their organizations, and 97% agreed identity is a foundational piece of Zero Trust.

Adoption of the Security Outcomes advocated by the IDSA takes organizations further down the path of establishing a Zero Trust environment. As an example, the IDSA recommends analyzing device characteristics to enable more granular control. This capability allows organizations to make smarter authentication decisions based on deeper levels of contextual information about devices, such as device behavior or location. Another example is the continuous attestation of identities and devices, which empowers organizations to monitor user access rights and the state of devices so that they can either deny access or apply additional security challenges in response to anything suspicious.

To get started on your Zero Trust journey, your initial 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

Protecting an organization's most sensitive data and systems is a primary focus of a Zero Trust framework. These assets—and all users who are entitled to have access to them—must be identified, and safeguards should be implemented to ensure those requesting access to them are properly authenticated and challenged when necessary. All access privileges should be granted according to the principle of least privilege, with particular attention paid to privileged accounts.

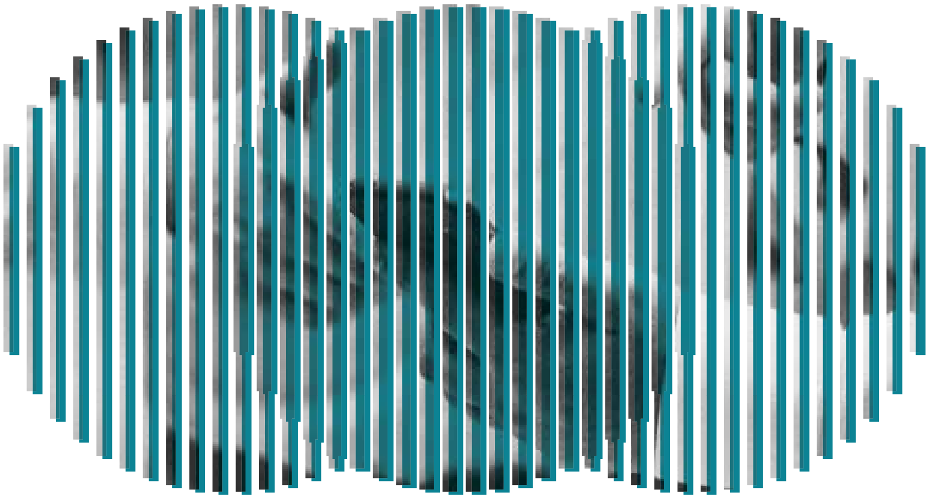
The journey to creating a Zero Trust architecture need not be completed in a single day, nor should it cause organizations to break their budget. Zero Trust is a layered approach to security that can be taken in small steps without a complete overhaul of your security. Regardless of where your organization is on the journey to Zero Trust, however, an Identity Defined Security approach will power every step it takes.

# 6. ALIGNMENT WITH COMMON CYBERSECURITY FRAMEWORKS

Depending on the industry and nature of a business, organizations are required to follow compliance frameworks to meet state and federal regulatory guidelines, such as HIPAA for healthcare and PCI-DSS for organizations that handle credit card data. However, a number of cybersecurity frameworks have emerged that provide organizations with a system of standards, guidelines, and best practices to manage risk in the digital world, for example, the ISO 27000 series, Mitre ATT&CK framework, Center for Internet Security (CIS) controls, and the National Institute of Standards and Technology (NIST) cybersecurity framework.

According to research conducted in 2020 with over 500 identity security leaders (The State of Identity: A Work in Progress), 42% of organizations with more than 1000 employees follow the NIST cybersecurity framework. In April 2018, the most recent version of the Framework for Improving Critical Infrastructure Cybersecurity (Framework) was published by NIST. While the Framework was developed to improve cybersecurity risk management in critical infrastructure systems, it can be used by organizations in any industry.

For organizations utilizing the Framework and other publications from NIST and interested in further boosting their security posture through Identity Defined Security, we've provided a mapping of Identity Defined Security Outcomes to NIST Cybersecurity Framework v1.1, SP 800-207 Zero Trust Architecture, SP 800-63 Digital Identity Guidelines. You can find the references to these documents in each of the applicable Identity Defined Security Outcomes and mappings. In addition, there are mappings to the NIST Cybersecurity Framework v1.1 and Digital Identity Guidelines to Identity Defined Security Outcomes.



# CONCLUSION

Between the growth of cloud services, mobility, and remote working, identity has become a critical focus for IT security leaders. Users can access data from all types of devices and from anywhere in the world, making controlling access to data, cloud assets, and on-premise systems more complex. Just like human identities, machine identities are at risk, too, and protecting communication between technologies and keeping pace with the speed of changes has only become more challenging. Adding to these challenges are the activities of cybercriminals, many of whom have their eyes on user credentials. Compromised credentials are not just for breaking into the network; once inside the network, they are also used to move laterally. If they can acquire privileged access, their next target is sensitive data. It only takes one compromised identity to lead to a significant data breach.

It is not enough to invest in traditional perimeter security to address this problem. Among a growing number of organizations, the days of identity being siloed from security are drifting into the past. In place of these approaches is Identity Defined Security and the potential of building a more secure environment protected by a Zero Trust architecture. As organizations move into the future, adopting an identity-centric security strategy like the  Identity Defined Security Framework will remain critical to keeping pace with attacks.