Gain Confidence in Your Security with Zero Trust

Learn how AWS services and AWS Partners can help you apply a Zero Trust security model

Table of contents

Zero Trust is the Foundation of Modern Cybersecurity

Given the new distributed environment, a new model of security mechanisms are vital. Traditionally, enterprises have relied upon securing a specific perimeter of trust, including trusted users, devices, and network infrastructure. Zero Trust is prompting enterprises to take into account identity, authentication, and other context indicators such as device state and health – in order to make real and meaningful security improvements over the status quo.

In an ideal world, Zero Trust is a security model where access to your computing resources and data are not granted solely based on network location. Levels of trust are clearly and constantly evaluated and amended in real time to enable secure access to enterprise resources. See our definition of Zero Trust below.

Zero Trust has been around for more than a decade. Given the increasing regulations for data protection and information security, and the emergence of distributed, remote working as a way of life, Zero Trust has resurfaced as a model to help organizations make meaningful security improvements.

In fact, Zero Trust has gained such prominence that in May 2021, President Biden signed an Executive Order mandating that all federal agencies establish plans to drive adoption of Zero Trust architecture.1 This has spurred organizations to speed up their adoption of Zero Trust principles. Now, the need for products that support Zero Trust is growing so fast that the global Zero Trust security market will grow from $27.4 billion in 2022 to $60.7 billion by 2027.2

The traditional castle-and-moat metaphor has disappeared, replaced instead by software-defined microsegmentation so that user, application, and device can connect securely from anywhere to anywhere.

In the rest of this ebook, we'll show how you can approach implementing a Zero Trust security model in your enterprise, the building blocks Amazon Web Services (AWS) recommends for doing so, and specific use case examples.

AWS definition of Zero Trust

Zero Trust is a security model centered on the idea that access to data should not be solely made based on network location. It requires users and systems to strongly prove their identities and trustworthiness, and enforces fine-grained, identity-based authorization rules before allowing them to access applications, data, and other systems. With Zero Trust, these identities often operate within highly flexible identity-aware networks that further reduce surface area, eliminate unneeded pathways to data, and provide straightforward outer security guardrails.

[1] The White House. "Executive Order on Improving the Nation's Cybersecurity." May 12, 2021.
[2] MarketandMarkets. "Zero Trust Security Market." 2021.

Your Zero Trust Journey

Organizations often begin their Zero Trust journey when faced with security considerations such as protecting against ransomware or creating a secure perimeter that won't slow down remote work. Here are some common triggers that compel many organizations to begin strategizing around Zero Trust.

Protecting against ransomware is a tremendous concern, causing companies to direct more time, effort, and money into ensuring their digital presence and files are secure.

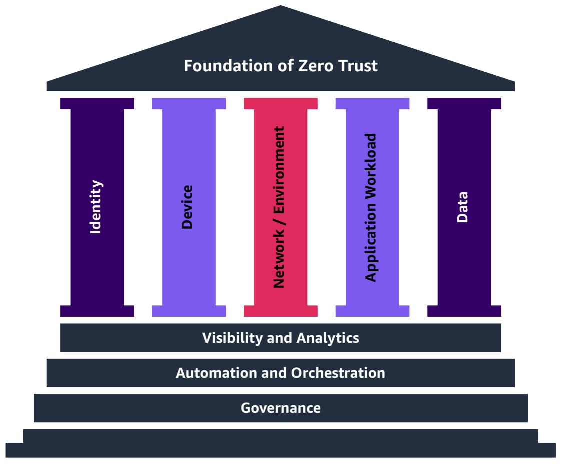
Keeping remote workers secure as they connect to the organization from multiple devices, oftentimes starting through the internet.

Merging and acquiring companies can lead to a patchwork of security systems and present new challenges, especially when an acquisition has weaker security controls.

Migrating on-premises resources to the cloud often prompt organizations to review compliance regulations and reevaluate their security policies.

Understanding your Zero Trust progress

Thus, while each organization's reason for adopting Zero Trust may be different, sticking to a unified framework can help you understand and assess your progress—as Zero Trust is an ongoing journey. The Cybersecurity & Infrastructure Security Agency (CISA) has developed a Zero Trust maturity model that represents a gradation of implementation across five distinct pillars, where advancements can be made over time. This maturity model provides a framework to help you evaluate how close you are to achieving Zero Trust, while always determining where you can improve. In this eBook, we are following the functional components as they pertain to NIST implementation architecture. There also are many security organizations that can help you assess your organization's level of Zero Trust and provide you with a Zero Trust score, giving you a goal to measure your enterprise against.



Source CISA Zero Trust Maturity Model June 2021

The AWS Perspective on Zero Trust

AWS infrastructure aligns with the National Institute of Standards and Technology (NIST) 800-207 Zero Trust architecture and and its principles were built into the foundation of AWS infrastructure since its earliest days. AWS not only provides Zero Trust building blocks but is also home to an extensive network of proven partners who can help you achieve your Zero Trust goals. So regardless of the progress your organization has made toward Zero Trust, AWS and AWS Partners can help you further your journey.

AWS uses Zero Trust building block

Signing AWS API requests: Every day, AWS customers interact confidently and securely with AWS, making billions of AWS API calls over a diverse set of public and private networks. Each one of these signed API requests is individually authenticated and authorized every single time at rates of millions of requests per second globally. The use of network-level encryption using Transport Layer Security (TLS) combined with powerful cryptographic capabilities of the AWS Signature v4 signing process secures these requests regardless of the trustworthiness of the underlying network.

Securing AWS service-to-service interactions: When individual AWS services need to call each other, they rely on the same security mechanisms that you use as a customer. For example, the Amazon EC2 Auto Scaling service uses a service-linked role in your account to receive short term credentials and call the Amazon Elastic Compute Cloud (Amazon EC2) APIs on your behalf in response to scaling needs. These calls are authenticated and authorized by AWS Identity and Access Management (IAM), just as your calls to AWS services are. Strong identity-centric controls form the basis of the security model between AWS services.

Adopting Zero Trust for internet of things (IoT): AWS IoT provides the foundational components of Zero Trust to a technology domain where unauthenticated, unencrypted network messaging over the open internet was previously the norm. All traffic between your connected IoT devices and the AWS IoT services is sent over Transport Layer Security (TLS) using modern device authentication including certificate-based mutual TLS. In addition, AWS added TLS support to FreeRTOS bringing key foundational components of Zero Trust to a whole class of microcontrollers and embedded systems.

Monitoring behavior with Amazon GuardDuty: Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts, instances, container workloads, users, and storage for potential threats. Using GuardDuty you can monitor user behavior and identify if an active user may pose a threat to your data. Whether it’s an IAM user making new and potentially dangerous API calls, a sudden change in an Amazon EC2 instance’s observable behavior, or indications of compromise in your environment, you can use GuardDuty findings to revoke a user or role's credentials thereby blocking all further authorization of API calls.

Managing access with AWS IAM: With AWS IAM, you can specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS. AWS IAM Identity Center (successor to AWS Single Sign-On) helps you securely create or connect your workforce identities and manage their access centrally across AWS accounts and applications. IAM Identity Center is the recommended approach for workforce authentication and authorization on AWS for organizations of any size and type. This is especially important when it comes to least privilege access, so that any user, device, workload, or process should only have the bare minimum privileges it needs to perform its intended action. Customers have full visibility into both the privileges that you're granting one service, as well as an AWS CloudTrail record of the use of those privileges. In addition, you also can grant temporary security credentials for workloads that access your AWS resources.

AWS Espouses Three Guilding Principles for Building Zero Trust

Now that you've seen some of the basic AWS building blocks that help get you closer to Zero Trust, it's time to see them in action. The AWS vision for Zero Trust can be broken down into three guiding principles that outline how you can apply a Zero Trust framework.

1. Use identity and network capabilities together

Overall, the best security doesn't come from making a binary choice between identity-centric and network-centric tools, but rather by using both effectively in combination with each other. When you choose AWS IAM authorization, you gain identity-centric controls. You can author standard IAM policies that define who can call your API and where they can call it from. For example, the AWS SigV4 request signing process, which is used to interact with AWS API endpoints, uniquely authenticates and authorizes each and every signed API request, and provides very fine-grained access controls.

In addition, network-centric tools such as Amazon Virtual Private Cloud (Amazon VPC), security groups (which provide highly dynamic, software-defined network micro-perimeters for both north-south and east-west traffic), AWS PrivateLink, and VPC endpoints are straightforward to understand and use, filter unnecessary noise out of the system, and provide excellent guardrails within which identity-centric controls can operate.

Ideally, these two kinds of controls should be aware of and augment one another. For example, VPC endpoints provide the ability to attach a policy that allows you to write and enforce identity-centric rules at a logical network boundary—in that case, the private network exit AWS Network Firewall or Amazon VPC on the way to a nearby AWS service endpoint.

2. Work backwards from your use cases

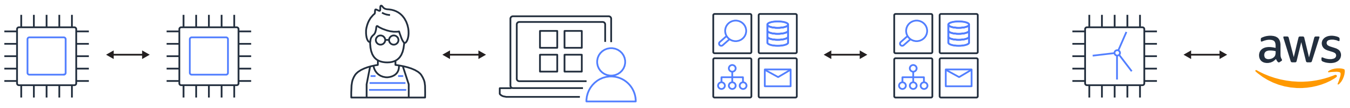
Zero Trust can mean different things depending on your use case. By working backward from what you are trying to achieve, you can determine the optimal Zero Trust patterns, tools, and approaches to use. Consider these three very different use cases.

Machine-to-machine: Authorizing specific flows between components to eliminate unnecessary lateral network mobility. By eliminating unnecessary communication pathways, you are applying least privilege principles to better protect critical data. Depending on the nature of the systems, you can construct these architectures through dynamic microperimeters built using Security Groups, request signing through Amazon API Gateway, private connectivity through AWS PrivateLink, AWS Network Firewall, and more.

Human-to-application: Enabling friction-free access to internal applications for your workforce. You can accomplish this with services like Amazon WorkSpaces or by securely connecting your internal applications directly to the Internet, using services like AWS Shield and Application Load Balancer with OpenID Connect (OIDC) authentication. This allows you to integrate with your existing Identity provider (IdP), control application access through strong user and device authentication, leverage modern identity standards, and provide friction-free end user access.

Software-to-software: When two components don't need to communicate, they should not be able to, even when residing within the same network segment. You can accomplish this by authorizing specific flows between the components. By eliminating unnecessary communication pathways, you are applying least privilege principles to better protect critical data. authentication, leverage modern identity standards, and provide friction-free end user access.

Focus on use cases



Machine-to-machine **Human-to-application** **Software-to-Software** **Digital transformation**

Same: Technical principles
Different: Technical principles

Focus: What we're solving for
Avoid: Getting mired in low-value discussions

Digital transformation: Creating carefully segmented microservice architectures inside new cloud-based applications. Digital transformation projects often connect sensors, controllers, and cloud-based processing and insights, all operating entirely outside of the traditional enterprise network. To keep your critical IoT infrastructure protected, the family of AWS IoT services can provide end-to-end security over open networks, with device authentication and authorization offered as standard features.

3. Remember one size doesn’t fit all

Zero Trust concepts must be applied in accordance with the security policy of the system and data being protected. But Zero Trust isn’t one size fits all and it’s continually evolving. Our advice? Don’t apply blanket controls to your organization because an inflexible approach might not allow for growth.

Over time, the application of the Zero Trust conceptual model and associated mechanisms will continue to improve defense in depth and augment the security controls you already have by providing increased visibility via the software-defined nature of the cloud.

Starting by strongly adhering to least privilege and then strictly applying the tenets of Zero Trust can significantly raise the security bar, especially for critical workloads. Think of Zero Trust concepts as additive to existing security controls and concepts, rather than as replacements.

Zeroing in on Zero Trust

Done right, a Zero Trust framework enables building a flexible, identity-aware network that reduces your attack surface, eliminates unneeded pathways to data, and provides straightforward outer security guardrails. Using building blocks from AWS you can apply Zero Trust concepts on a continuous basis to make meaningful security improvements over the status quo.

No matter where you are in your Zero Trust journey, AWS services and AWS Partners can help. Find an AWS Security Competency Partner to get started today.