aws marketplace

WHITEPAPER

Building a Successful Zero Trust Strategy for Data Analytics

Explore the core elements of a zero trust strategy for access and control in AWS.

AWS Marketplace Introduction

In the "Building a successful zero trust strategy for data analytics" webinar, SANS and AWS Marketplace explored how to combine the elements of zero trust controls and technology into a best-practice architecture to build and protect your cloud.

In this whitepaper, SANS analyst and senior instructor, Dave Shackleford, dives deeper into network-based services and the variety of controls that help you build a sustainable, layered zero trust model in AWS.

Included is an overview of the NIST cybersecurity framework and how to align its zero trust tenants, network access controls (NACs) and identity controls, use cases, and next steps.

AWS Marketplace will share how you can build and deploy a zero trust strategy with solutions from independent software vendors in AWS Marketplace.

The featured solutions for this use case can be accessed in AWS Marketplace:

Okta

Zscaler

SANS

Analyst Program

Whitepaper

Building a Successful Zero Trust Strategy for Data Analytics

Written by **Dave Shackleford**

April 2022

aws marketplace

Introduction: What Is Zero Trust, and What Does It Mean in AWS?

In today's highly diverse technology environment, uniquely quantifying the meaning of zero trust can be challenging. For cloud-based scenarios, which are becoming more common than ever, zero trust tends to be split between cloud-centric access control (between and among resources) and user-based access to the cloud (for any variety of services). In Amazon Web Services (AWS), it's possible to run a vast array of services and applications. Safely provisioning end user access to these services is a top priority for organizations with a workforce that's working more remotely than in the past. At the same time, the types of workloads, assets, and services in AWS have grown significantly, and numerous elements of access limitation between these cloud components are driving renewed interest in zero trust architecture and controls.

For access to AWS services and applications, the majority of zero trust controls will center on brokering services and client-based controls that identify who or what the client is, where the client is coming from, and what the client is trying to access (and potentially when this is taking place). For AWS, there is a much broader array of services and controls that can monitor and manage lateral movement, unauthorized access attempts, and overly broad permissions and network access, as well.

In this paper, we explore the core elements of a zero trust strategy for access and control in AWS, including network-based services and controls, identity-focused controls, and additional cloud-native and third-party controls that can help organizations build a successful zero trust model.

Building a Sustainable, Layered Zero Trust Model in AWS

To achieve a balanced and manageable zero trust model for AWS, organizations will likely make use of a range of different controls as well as security and operational program elements, some of which are built into AWS and others that are procured from AWS Marketplace partners, offering best-in-class security and cloud services.

With AWS, critical pieces of any zero trust strategy include identity awareness, flexibility in workload and asset protection, and trustworthiness. Key elements of an AWS zero trust strategy should include:

With AWS, critical pieces of any zero trust strategy include identity awareness, flexibility in workload and asset protection, and trustworthiness.

- Granular identity-based and context-based controls, including user and service authentication and authorization and role assignment
- Flexible network segmentation and microsegmentation within the cloud infrastructure
- Monitoring and deep visibility into all activity in the environment to best facilitate detection and response

It's helpful to design a strategy around an industry framework for cybersecurity, if possible, and one framework that works well in helping to categorize and define a zero trust approach is the NIST Cyber Security Framework (CSF).[1] The NIST CSF outlines five categories of controls and security program components that organizations should use in building a comprehensive approach, and we can build a zero trust model for AWS comfortably using these. The five categories include:

- **Identify—**Focuses primarily on core governance and risk management principles, along with asset management (mainly inventory and discovery controls), and defines cybersecurity roles and functions within the organization.
- **Protect—**Covers several major areas, including identity and access management (IAM), security awareness training, data security and information protection, and a mix of additional controls, including logging, network protection controls, and more.
- **Detect—**Focuses on event management and monitoring, which includes behavioral baselining of network traffic and other activities, malware detection, vulnerability scanning; and defines security event and incident detection processes and analyst roles for managing these.
- **Respond—**Emphasizes mainly incident response plans and processes, including investigations, forensics, and coordination/communication aligned with response efforts.
- **Recover—**Covers post-event and post-incident updates and improvement efforts aimed at remediation and continuous improvement in the cyber security program overall.

The additional NIST publication SP 800-207,[2] which focuses on a zero trust architecture model, states that the following tenets of a zero trust architecture be in place during design and deployment:

1. **All data sources and computing services are considered resources.** While somewhat self-explanatory, this principle is important as a starting point as the basis of policy that defines resources and data sources around which access control models are built.
2. **All communication is secured regardless of network location.** This principle primarily focuses on protecting network traffic through the use of encryption and other technology controls.
3. **Access to individual enterprise resources is granted on a per-session basis.** In keeping with the zero trust theme, each attempted connection is vetted and evaluated against defined policy before access is granted.
4. **Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.** As highlighted earlier, identity is a core aspect of zero trust in every way and forms the basis for many policies and access decisions (along with other behavioral aspects of connections, such as location, system labels and types, and data types).

---

[1] NIST Cybersecurity Framework, U.S. General Services Administration, www.gsa.gov/technology/technology-products-services/it-security/nist-cybersecurity-framework-csf

[2] "Zero Trust Architecture," National Institute of Standards and Technology, https://csrc.nist.gov/publications/detail/sp/800-207/final

5. **The enterprise monitors and measures the integrity and security posture of all owned and associated assets.** This component of zero trust focuses on system and service configuration and lockdown, as well as some degree of monitoring to ensure that the desired configuration state is maintained over time.
6. **All resource authentication and authorization are dynamic and strictly enforced before access is allowed.** In alignment with the previous item focused on IAM, user access will need to have authentication controls in place that are dynamic and integrated into policy decisions.
7. **The enterprise collects as much information as possible about the current state of the network infrastructure and communications and uses it to improve its security posture.** An enterprise would collect data about network traffic and access requests, which is then used to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.

While a zero trust architecture and program won't be immediately relevant to every aspect of the NIST CSF, many core controls and technologies align with the framework. We cover those next.

Identify

The Identify phase of the NIST CSF includes several sub-categories that organizations should include in their planning and design for a zero trust architecture in AWS. This category aligns with the following NIST SP 800-207 zero trust tenet:

- *All data sources and computing services are considered resources.*

The sub-categories are described in the following sections.

Asset Management

The emphasis in this category is on discovery and inventory of personnel, devices, systems, and facilities that an organization uses. Several important aspects of building out a zero trust model in AWS align with this category. First, workloads and other services and assets in AWS are easily discoverable, because they're coupled to the AWS fabric. Organizations can easily see the types of objects in each AWS account via a variety of services such as AWS Config,[3] Amazon Inspector, or AWS Command Line Interface (AWS CLI) queries. This is enormously valuable in helping to manage the life cycle of compute nodes, storage nodes, and more, as well as minimizing the potential proliferation of shadow IT in a large, growing environment. Second, cloud access security brokering (CASB) and zero trust network access (ZTNA) solutions that end users connect to for access to cloud resources can track (and control) user access to AWS, providing visibility into user accounts and originating devices alike. One of the first steps in building a zero trust design is ensuring that the cloud-based assets and the users and devices accessing those assets are visible and accounted for.

[3] This paper mentions solution names to provide real-life examples of how cloud security tools can be used. The use of these examples is not an endorsement of any solution.

Business Environment

For the most part, this category focuses on defining an organization's mission, its role in the supply chain, and its priorities, but it also stresses the need to establish a list of critical dependencies and services, as well as resilience requirements. When designing a zero trust architecture, some of the tools and controls that organizations implement to facilitate it will likely become mission-critical (for example, IAM policies, cloud brokering services, etc.) and should be included in planning discussions.

Governance

The governance category includes definitions of policy, cybersecurity roles and responsibilities, legal and regulatory requirements, and risk management processes that address cybersecurity risks. Very little here pertains directly to zero trust other than definition of privilege minimization and cybersecurity risk tolerance in policies and procedures.

Risk Assessment

Zero trust is a comprehensive strategy to increase the security posture of cloud users and assets, and should factor into everything from the collection of threat intelligence through monitoring services and information sharing, identification and evaluation of cloud asset vulnerabilities of all types, internal and external threats to cloud assets and services, and impacts of security events being realized.

Risk Management Strategy

Zero trust should be a factor in determining an organization's risk tolerance, because organizations should make operational and security-focused commitments to enable the strategy.

Supply Chain Risk Management

AWS, AWS cloud-native services, and associated cloud security services and solutions that are part of implementation of a zero trust strategy should be considered vital elements of the supply chain. As with any third-party services, these components should be included in resilience and recovery planning, security and risk evaluation of the services themselves, and contracts management.

In total, the Identify category of the NIST CSF is primarily about building a sound, balanced cybersecurity strategy and ensuring that all assets are known and accounted for. For many types of AWS assets and cloud access, zero trust concepts should be considered by customers in policy and procedure definitions, the discovery and monitoring of all assets and users, and understanding the associated risks related to use cloud infrastructure and applications.

Protect

The Protect category of the NIST CSF includes the majority of controls that make up a zero trust design in AWS, namely IAM and network access controls. The Protect category aligns with the following NIST SP 800-207 zero trust tenets:

- *All communication is secured regardless of network location.*
- *Access to individual enterprise resources is granted on a per-session basis.*
- *Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.*
- *All resource authentication and authorization are dynamic and strictly enforced before access is allowed.*

The following sub-categories are part of the Protect focus area.

Identity Management and Access Control

IAM is really the practice of defining who needs access to what and then controlling the entire life cycle of user and access management across resources. Because both users and cloud assets and services have identity associations, this category is a lynchpin for building a sound zero trust strategy in AWS.

In AWS, the AWS Identity and Access Management (AWS IAM) service is the primary policy engine for controlling user and service access within the context of an AWS account. AWS IAM users are associated with credentials for making API calls to interact with cloud services and can be enabled for application access to AWS resources too, not just as actual interactive user accounts. Once service-oriented users are created, they should be placed in defined groups. Permissions and privileges can be directly assigned to groups for simplified management and maintenance. For service interactions within the environment, however, cloud security teams should focus on defining specific roles that are used to interact with services, other AWS accounts, and federation services and single sign-on (SSO) providers. An example of a simple IAM policy that blocks access to AWS services originating from any IP addresses other than those specified is shown in Figure 1.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "aws:SourceIp": [
                    "192.0.2.0/24",
                    "203.0.113.0/24"
                ]
            }
        }
    }
}
```

Figure 1. A Simple AWS IAM Policy

Another important zero trust concept within the AWS IAM engine is that of permissions boundaries. These auxiliary policies can augment assigned policies to create limitations on what permissions can be enabled and set and are useful in restricting access to limit privilege escalation. Permissions boundaries are also commonly used to delegate permissions to privileged users for accomplishing certain tasks while maintaining restrictions to sensitive services and/or data that don't align with job roles and functions. An example would be developer accounts that have extensive permissions to create and manage resources in dev and test environments but are prevented from creating or modifying IAM policies themselves. Figure 2 shows the application of a permissions boundary along with an administrator policy. The two are applied in tandem to create the effective permissions the user will actually have.

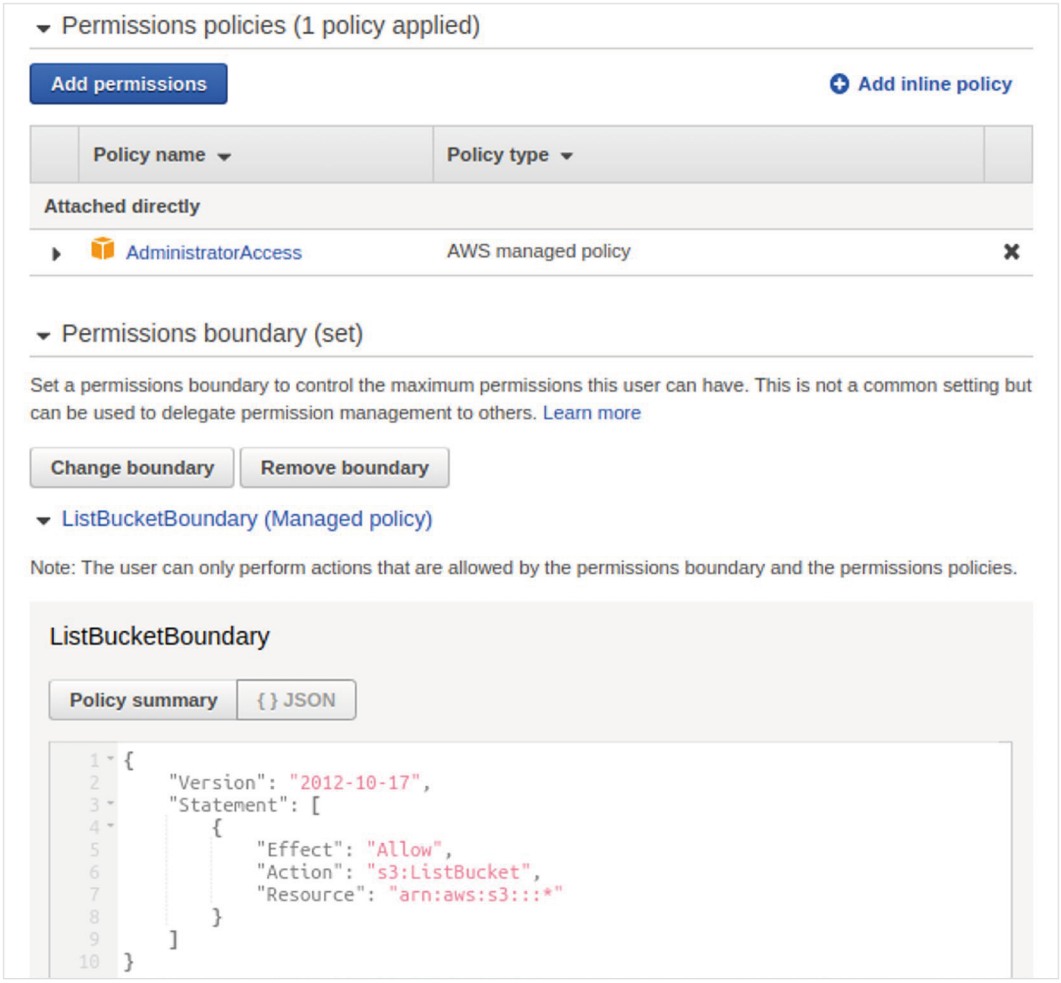


Figure 2. Permissions Boundary in AWS IAM

For organizations with larger deployments and those looking to create an even more robust means of isolating assets with a zero trust identity focus, individual accounts can be created to isolate assets and create least-privilege identity policies within accounts and for interactions between them. AWS Organizations is the service that enables this advanced functionality. Creating a centralized policy model in AWS Organizations allows security administrators to create different and least-privilege policies for the appropriate accounts and assign and/or revoke them effortlessly.

AWS Organizations accounts are placed into organizational units (OUs) that can be nested up to five layers deep. The AWS Organizations admin then sends out invitations to accounts to become part of the organization (via email or through account ID), and, when those invitations are accepted, the accounts are automatically provisioned with the appropriate privileges and policies. This segmentation and least-privilege capability is implemented through what are known as service control policies (SCPs) that govern the use of other IAM policies. AWS Organizations can control the entire account, group, and

role life cycle with regard to policy application, and can do so for accounts that need to interact or have some relationship. This can truly facilitate identity-based zero trust principles at an extremely large scale for accounts in AWS. An example of an SCP is shown in Figure 3. This policy explicitly denies IAM users from accessing or making use of a role policy called **`StorageAccess`**.

For centralized account access to cloud services, AWS offers an integrated SSO service called AWS Single Sign-On (AWS SSO). This service integrates with AWS Organizations or user directory services to federate groups of user identities to common SaaS applications, such as Box and Microsoft 365, and to internal AWS applications and services, as well. When configured for multiple AWS accounts, AWS SSO also configures and maintains the necessary permissions for AWS accounts automatically. Many third-party solutions in AWS Marketplace offer centralized identity-as-a-service (IDaaS) capabilities that include federated access and SSO, as well.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/StorageAccess"
      ]
    }
  ]
}
```

Figure 3. An Example Service Control Policy in AWS Organizations

Awareness and Training

For zero trust in AWS, the only changes to security awareness and training would likely focus on cloud engineering and operations teams that may need to understand the privilege limitations and other controls being enacted.

Data Security

In the context of zero trust, data security would be a limitation of privileged access (or any access) to data objects and storage services, accomplished with AWS IAM and AWS Organizations policies.

Information Protection Processes and Procedures

The majority of control areas under information protection are focused on configuration and change management for processing and workloads in the environment. Fortunately, tools such as AWS Systems Manager can be used to group and control resources, manage application configurations, automate and manage changes across entire fleets of workloads, patch systems, and manage configuration for workloads. Controlling access to AWS Systems Manager and related tools via IAM and other access limitations would align with a zero trust strategy.

Maintenance

The Maintenance sub-category requires logging and monitoring of system and asset maintenance, but it has little relevance to a zero trust design.

Protective Technology

In the Protect sub-category of protective technology, the most critical elements relating to zero trust are network access controls and network security.

The first important type of network-oriented zero trust is zero trust *via* the cloud, usually through brokering services offering ZTNA and CASB capabilities. Reasons why this model of zero trust access is growing in importance include:

- **Diverse endpoints and users—**With the addition of more contractors and third parties, as well as BYOD endpoints, the diversity of both systems and users has increased significantly, making access control and monitoring more challenging.
- **Remote access—**Many organizations began to question the traditional hub-and-spoke VPN model for employees who were increasingly accessing external services. Many security controls have been predominantly located on-premises, though, necessitating a change in access control and monitoring strategies.

This type of zero trust is centered on end-user access *to* cloud applications and services. It usually involves the following types of capabilities:

- Strong authentication and authorization of both endpoint systems and user accounts
- Adaptive access policies that evaluate group membership and privileges, access behaviors, and known malicious/suspicious indicators
- Browser isolation and sandboxing to prevent malware events and other browser-based events
- Content filtering and data loss prevention (DLP) controls to monitor for sensitive data exposure or access to anomalous or known unauthorized sites

In addition, some cloud brokers also support SaaS-specific monitoring capabilities, as well as controlled access to on-premises applications and services.

The second major type of zero trust networking controls are those available *in* the cloud via cloud-native services. Cloud-native network access controls can be used to control and restrict traffic into and out of the cloud infrastructure, as well as between internal workloads and services, helping to achieve zero trust for cloud-based assets in AWS. The first area to focus on for AWS zero trust network isolation and segmentation should be network isolation zones known as *virtual private clouds (VPCs)*, and they can contain any number of distinct network subnets. VPCs can also be peered to one another and connected through AWS Transit Gateways and AWS Direct Connect circuits. Subnets within each VPC can be configured to communicate as needed through routing and cloud-native access controls.

Within each VPC are two built-in types of network access and isolation controls: security groups and network access control lists (network ACLs or NACLs). Security groups and NACLs can be used to control traffic into and out of network deployments. Security groups apply to instance workloads and are stateful, while NACLs apply to VPC subnets and are stateless. Security groups start with a network access control policy of "deny all," and enterprises can then add rules to allow only those types of network access needed. We recommend following this approach for designing a zero trust cloud-native network strategy in AWS:

- Isolate at a broad scale (business units or specific services and applications) at the VPC level. VPCs cannot communicate with one another unless explicitly permitted to do so.
- Within each VPC, create subnets for more granular grouping and asset identification. NACLs can be created to expressly allow or deny traffic into/from/between subnets. Creating too many explicit NACL rules can be unwieldy to manage in large environments, though, so it's recommended to create explicit allow or deny rules sparingly.
- For workloads within each subnet, localized policies for network traffic access can be applied with security groups (in some ways, the last line of network cloud-native defense for workloads).

For many organizations, these core network controls (VPCs, subnets, NACLs, and security groups) act as a robust, layered zero trust strategy that can be applied in infrastructure-as-code (IaC) services such as AWS CloudFormation.

For access control between a larger scale of resources like VPCs and other internal AWS services, AWS PrivateLink enables users to connect resources across VPCs, but only traversing the AWS network. This can be useful to connect different accounts together, or to connect securely between entirely different network resources that need secure direct access enabled. This can also be useful to connect to hosted services in AWS Marketplace.

More advanced cloud-native controls in AWS include AWS Network Firewall and AWS WAF. AWS Network Firewall can be implemented as a firewall and network intrusion detection service layer, simplifying deployment and management of network traffic controls for traffic into and out of AWS (contributing to a zero trust model for some ingress-egress communications). AWS WAF is a web application firewall that is natively integrated into the AWS fabric and can protect web applications or APIs against common web security events that may affect availability, compromise security, or consume excessive application resources. AWS WAF makes it simple to create security rules that block security events such as SQL injection, cross-site scripting (XSS), authentication attempts, and more. In addition, custom rules that filter out specific traffic patterns you define are supported, as well, and packages of managed rules are available through AWS.

For these access controls (including security groups), centralized management through AWS Firewall Manager can help streamline operations across numerous accounts.

To summarize, the Protect category of the NIST CSF focuses primarily on identity and network-centric controls for a zero trust architecture and controls implementation. Identity controls should include end-user access control and monitoring to cloud infrastructure and applications with SSO and federation, along with internal identity policies for accounts, cloud assets, and cloud services. Network-based controls should include ZTNA for end-user access, as well as layered cloud-native controls such as VPCs, NACLs, and security groups, and more advanced options such as AWS Network Firewall and AWS WAF for controlling additional traffic into and out of the AWS infrastructure.

Detect

There are three sub-categories within the Detect category of the NIST CSF. These include:

- **Anomalies and Events—**Event monitoring and SOC analysis
- **Security Continuous Monitoring—**Malware detection and vulnerability scanning
- **Detection Processes—**Detection process definition and improvement

In an AWS zero trust architecture, detection and response through observability is another important theme. The Detect category aligns with NIST SP 800-207 in the following categories:

- *The enterprise monitors and measures the integrity and security posture of all owned and associated assets.*
- *The enterprise collects as much information as possible about the current state of the network infrastructure and communications and uses it to improve its security posture.*

In the realm of zero trust, a number of additional AWS and third-party services can aid in detection, threat analysis, and continuous monitoring. An important utility within AWS IAM that can greatly aid in evaluating many types of identities and role assignment is IAM Access Analyzer. IAM Access Analyzer can help discover identities and resources that may be accessible from outside an AWS account, and also validates public and cross-account access before deploying permissions changes. IAM Access Analyzer also continuously monitors for any new or updated policies, and analyzes permissions granted for numerous resource types, including Amazon S3 buckets, AWS Key Management Service (AWS KMS) keys, SQS queues, AWS IAM roles, AWS Lambda functions, and AWS Secrets Manager secrets. This can help identify changing configuration parameters and conditions within AWS that could erode zero trust policies and design.

Amazon GuardDuty analyzes log and intelligence data (both internal to AWS and from third parties) to deliver threat intelligence about account behavior. Results from Amazon GuardDuty can be integrated into Amazon CloudWatch and other event triggering systems in AWS or sent to the SOC or other locations for analysis with different tools.

Amazon Detective collects and aggregates logs across AWS resources and performs deep analysis on them to detect behavior anomalies and other events for faster and more efficient root cause analysis and investigations. These services can also aid in providing detection and visibility of potential zero trust violations.

Amazon Inspector is a vulnerability scanning service in AWS that can identify assets and report on detected misconfigurations and known vulnerabilities for workloads in the AWS environment. This can help detect systems or other configuration details that could potentially violate zero trust models, as well.

While not directly focused on detection, AWS Resource Access Manager can help organizations share configured resources across a number of accounts, helping to better identify issues that could lead to zero trust violations.

A variety of third-party services available through AWS Marketplace can analyze and model privileges in use, as well as permissions to data stores and services. These can be highly valuable in tracking possible access and/or unauthorized activity pathways that violate zero trust principles in AWS.

Respond

The entire Respond category of the NIST CSF is focused on incident response planning, communications, analysis, mitigation, and improvement efforts. In the realm of zero trust, cloud-native controls that can help respond to and remediate any detected policy violations such as misconfigurations and overly permissive access models can aid in keeping a zero trust controls model in place and functional. One example is AWS Config, a configuration monitoring service for your AWS environment. You can define baseline workload images, monitor systems and services continually, and alert whenever a system or service configuration changes. Another key feature of AWS Config is its inventory capability. Cloud assets are software-defined and linked to the AWS backplane, making discovery and inventory of services, assets, and configuration state simpler than ever. AWS Config can be set up to help keep the AWS control plane and assets more secure by monitoring and remediating any policy violations detected.

Recover

The final category of the NIST CSF, Recover, doesn't have any direct bearing on zero trust design other than to implement any possible improvements that could be made in zero trust policies and controls post-incident (as applicable).

Zero Trust Use Case in AWS

An organization that is planning to build a zero trust model for access to and within AWS first carefully identifies roles and responsibilities for all cloud engineering, DevOps, and security team members that would need access to the cloud infrastructure. These privileged users are given access through federation and SSO services (AWS SSO or third-party services) for role integration into AWS, and the organization assigns predefined policies from the AWS IAM catalog that match these administrative roles whenever possible, because these are the most accurate and well-structured to start with. Permissions boundaries are implemented to restrict access even more based on privilege reduction policies and requirements. Identity controls and policies between workloads and services in AWS are carefully evaluated using tools such as AWS IAM Access Analyzer and third-party identity policy analysis services to ensure that a least-privilege, zero trust model is in place for all access.

The organization then evaluates the types of network access required from the internet for customers/clients and end users. This requires a review of application and service architecture to define data flows with TCP/UDP ports and application behavior profiles that could be used to carefully restrict the types of traffic needed for operations. The organization starts with cloud-native networking controls such as security groups and NACLs, which allow for a layered zero trust approach that can be managed through IaC templates such as AWS CloudFormation. To best control end user access to the cloud, the organization enables a cloud brokering solution offering ZTNA policies and enforcement that analyze behavior, authentication and authorization of user profile and systems, and cloud application and service security posture. This solution also integrates with SSO options to help centrally manage identities and access through a single portal for all user types (including the privileged users, where applicable).

The organization decides to implement numerous separate AWS accounts managed by AWS Organizations to apply SCPs that could enforce specific application use cases. AWS Resource Access Manager is implemented to share IAM users and roles, network configurations, and other cloud configuration options across these accounts and centrally manage them.

Within AWS, the organization enables numerous detective controls, including Amazon GuardDuty and AWS Detective for event monitoring and analysis, Amazon Inspector for vulnerability scanning, and AWS Config for remediation of detected events across workloads and other resources that don't meet zero trust policy requirements.

Next Steps: Why Zero Trust Is the Right Direction for Cloud Access Management

The zero trust model starts with the premise of privilege reduction and stringent access controls, emphasizing user and device validation for access to workloads and services. Following the NIST CSF, when building a zero trust model in AWS, organizations should consider these points regarding each CSF category:

Identify Determine what types of access are warranted and needed, and how the organization will build policies and govern ongoing access to the cloud and within it.

Protect Build a strong zero trust isolation strategy founded on account isolation and IAM policies with AWS Organizations and SCPs, IAM policies and permissions boundaries, and federation and SSO. Enhance this with ZTNA for end users and devices, as well as cloud-native controls such as VPCs, NACLs, and security groups. For core ingress and egress traffic control, services such as AWS WAF and AWS Network Firewall can help further restrict and control access to resources.

Detect Building guardrails in the cloud monitoring for unusual behavior that may indicate issues with the zero trust strategy is also important. Amazon GuardDuty, Amazon Detective, and Amazon Inspector can help monitor and evaluate the environment and alert security professionals when necessary. AWS Resource Access Manager can help proliferate and share secure configurations across accounts.

Respond Services such as AWS Config can help automatically remediate any misconfigurations and issues that could compromise a zero trust security posture.

Recover Zero trust is a continually evolving model, and organizations should evaluate what works best for them to improve and refine their controls and strategy over time.

It's possible to build an in-depth and capable zero trust architecture in AWS using a combination of cloud-native and third-party tools and services. Be sure to keep the principle of defense-in-depth in mind, following a layered approach that accommodates various types of resources, users, and use cases.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace

Explore the core elements of a zero trust strategy for access and control in AWS

Build your successful zero trust model with AWS services and third-party solutions

To achieve a balanced and manageable zero trust model for AWS, organizations will likely make use of a range of different controls as well as security and operational program elements, some of which are built into AWS and others that are procured from AWS Marketplace partners, offering best-in-class security and cloud services. These security solutions can be integrated with AWS Services and other existing technologies, enabling you to deploy a comprehensive security architecture across your AWS and on-premises environments.

How AWS customers are leveraging Okta as part of their zero trust security architecture

Okta Integration Network includes more than 7,000 pre-built integrations with cloud and on-premises systems to help organizations modernize their IT, build seamless customer experiences, and protect against data breaches. Key services of Okta Integration Network include:

- **Directories that security store users and attributes at scale.**
- **The broadest, deepest set of over 7,000 integrations** with the frameworks, templates, and tools that make it easy for applications to connect to Okta.
- **Insights that aggregate, analyze, and disseminate data** from Okta and our partners.
- **Identity Engine,** which powers customizable access experience, including authorization, authentication, and registration.
- **Workflows that automate identity-centric processes** like employee onboarding and offboarding using conditional logic.
- **Devices that collect device identify and context** for use in access decisions and passwordless experiences.

Okta

Zscaler

The Zscaler Zero Trust Exchange is an integrated platform of services that acts as an intelligent switchboard to secure user-to-app, app-to-app, and machine-to-machine communication—over any network and any location. Gartner awarded Zscaler the highest position on its Magic Quadrant™ for their "Ability to Execute" for Security Service Edge (SSE).

AWS Marketplace is a digital software catalog that makes it easy to find, try, buy, deploy, and manage software that runs on AWS. AWS Marketplace has a broad and deep selection of security solutions offered by hundreds of independent software vendors, spanning infrastructure security, logging and monitoring, identity and access control, data protection, and more.

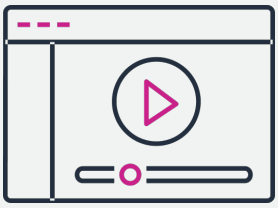
Customers can launch pre-configured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.

How to get started with zero trust security solutions in AWS Marketplace

Security teams use AWS native services and seller solutions in AWS Marketplace to help build automated, innovative and secure solutions to address relevant use cases and further harden their cloud security footprint.

The following solutions can help you get started:



Watch the Webinar

Building a Successful Zero Trust for Data Analytics in AWS.

View On-Demand

Discover Solutions

Find the tools you need to implement a Zero Trust Model for Data Analytics Applications in AWS.

Visit AWS Marketplace

Talk to an Expert

Get connected with a solution architect that can share best practices and help solve your business challenges.

Get Connected