White Paper

axis security

NIST Zero Trust Architecture Compliance

Apply a Zero Trust Model Using Application Access Cloud

Executive Summary

Zero Trust is a network security framework that has gained remarkable traction in the last few years. It suggests that administrators trust no one and subject all users to full authentication and authorization prior to any user-to-application request. The National Institute of Standards and Technology (NIST) has published several papers recommending best practices that organizations can put in place to minimize their cyber risk and exposure.

Axis Security adheres to multiple NIST guidelines by adopting the latest cloud technologies to enable rapid, easy, and secure remote access for increasingly mobile workforces. Whether enabling secure partner access, accelerating organization mergers and acquisitions, replacing aging mobile VPN solutions, or seeking frictionless cloud migration, Axis Security complies with NIST guidelines to mitigate, reduce, and enhance secure access for your organization.

Introduction

The global COVID-19 pandemic has only made this situation more acute. Employees, contractors, and consultants have rapidly transitioned to remote locations. And, they are using multiple devices to access business-critical applications increasingly in the cloud, [often their own]. To enable and encourage such productivity — while ensuring proper security and protection — administrators need a simple, secure, and rapidly deployable solution that enables and encourages remote work without exacerbating application and network security issues.

Traditionally in such situations, administrators might provide remote access VPN capabilities to every user. However, VPNs were developed many years ago when privacy and security concerns were not nearly as top-of-mind as they are today. Leveraging a complex client that each user installs on every device, VPNs also typically require substantial configuration to enable access. Rather than restricting access to a specific application, VPNs allow network-level access that can expose many sensitive applications and resources to both authorized and unauthorized users. Moreover, VPNs can be difficult to manage when bringing on new users and are relatively inflexible to control and administer. And as NIST guidelines and requirements have changed, VPNs have fallen increasingly out of compliance to become a risk themselves.

With this in mind, a new solution is needed that streamlines access to public and private cloud as well as on-premises applications. The solution should be simple to deploy, offers a significantly better user experience and protection than VPNs, and provides detailed security controls to administrators.

Zero Trust

Networks were initially designed to facilitate and streamline communication. Users were granted permission to access information, typically from an office location. Over time, however, users became more mobile and began using more devices. Today, workers are more mobile than ever, working from "offices" like airports, hotels, and — especially due to COVID-19 — home.

Because the average cost of a data breach now approaches $4M USD[1], the concept of Zero Trust emerged. It is a framework, or paradigm, rather than an industry standard. It holds that trust should never be granted outright to either a user or a device. Rather, each user should be subjected to continuous authorization and authentication throughout the transaction.

Axis Security's Application Access Cloud™

The Axis Security solution enables organizations of all sizes to allow employees and 3rd parties instant access to applications and resources across clouds and on-premises, regardless of their location. It does not require agents or clients, nor does it require network reconfiguration. The Application Access Cloud monitors and logs all user behavior, implements Zero Trust application access, isolates vulnerable applications from exposure to the internet or internal network, brokers application requests to disarm attacks, and eliminates network-level exposure of assets by keeping users off the network, even while it ensures user productivity.

[1] Ponemon Institute, IBM Security "Cost of a Data Breach Report 2020"

NIST Cybersecurity Framework Guidelines

The National Institute of Standards and Technology (NIST) developed a detailed framework on cybersecurity for organizations of all sizes to mitigate security risks and possible sensitive data loss or leakage. The guidelines cover five risk areas:

Identification
What matters most to the business and what are the biggest threats?

Protection
What actions can be taken to ensure key aspects of the business are safe?

Detection
What threats, events, or disruptions can be determined that might affect the business?

Response
How can the business respond if factors arise that may threaten the business?

Recovery
How can the business resume normal operations as quickly as possible?

Naturally, these guidelines apply widely to different business needs depending on resources, workforce flexibility, and technology adoption. But, several recommendations apply when considering how to protect and enable secure remote access for employees and partners.

How Axis Security Adheres to NIST Guidelines

Identification

Axis can be widely deployed to any number of users for many types of application protocols, often without requiring a client or agent. The agentless approach means faster on-boarding and fewer help-desk calls because users can access applications with any device (laptop, smartphone, tablet) through a browser. The App Access Cloud continuously evaluates and manages who is able to access specific applications, keeping track of individual users through IP addresses, time of day, location, history, and applying metrics from identity and endpoint management integrations.

Protection

Axis Security grants access to individual applications on a per-session basis. It operates at the application-layer to apply granular policies that govern access to specific applications using context-based policies based on time, user location, user activity, the request itself and more. Applications are published through Axis and are not exposed directly to the internet or the internal network. This process, known as application whitelisting, prevents promiscuous application discovery — unlike VPNs and other cloud-based security solutions which allow users to find and/or access applications they may not have privileges to.

Moreover, Axis Security's policies subject every user to further security controls such as session limits, visual recording, and activity logging. Policies may restrict permissions to download, copy/paste, or print content based on the context of the request. Session limits may restrict access to one or more applications for a period of time, while visual recording offers administrators visibility into a users' activity. Connections may be subject to termination because each is continuously analyzed for proper security posture.

Detection

Axis Security provides continuous authorization, authentication, and validation for any user accessing applications in multi-cloud or on-premises via the Axis Cloud. The centralized access policy management governs exactly which users can access specific applications — and tracks all activity — to provide detailed views of network and application behavior.

Because all activity is tracked, administrators can build detailed views of user and application risk analytics. This level of visibility significantly reduces the possibility of data loss or leakage through unauthorized users and provides data and information for incident investigations and future capacity planning.

NIST 800-207

Recently, NIST published "Zero Trust Architecture", a paper that discusses Zero Trust in detail and offers guidance for enterprises seeking to implement zero trust technologies and architectures. While less prescriptive than other NIST documents, 800-207 suggests that enterprises "establish a continuous diagnostics and mitigation (CDM) or similar system to monitor the state of devices and applications". The authors also encourage organizations "to have Identity, Credential, and Access Management (ICAM) and asset management systems in place." And, that systems should aggregate "asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems."

Section 2.1 in the NIST 800-207 paper outlines the **following 7 basic tenets for a Zero Trust architecture:**

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location
3. Access to individual enterprise resources is granted on a per-session basis
4. Access to resources is determined by dynamic policy
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

Capabilities of the App Access Cloud that address Zero Trust tenets outlined by NIST

Monitors and logs all user and app activity throughout the session including view, open, upload, plus many other user actions uniquely monitored to ensure proper access procedures are followed.

Integrates with SIEM and SOAR systems to detect and mitigate risk to the organizaiton and improve the efficacy of the security team

Detailed authentication and authorization processes to ensure users, regardless of their location or device, are fully verified pre-session before accessing applications.

Granular, dynamic policies that govern individual application access, restricting users to one or more specific applications rather than a group of them, or worse, network-level access to multiple applications like VPNS do.

Options to restrict actions such as copy/paste or download based on user context and device posture, protecting sensitive enterprise data.

Isolates applications (data and computing sources) and governs access to each resource individually. Further, communication between the user and the resource is secured and brokered regardless of the physical location of the resource or user.

Furthermore, Axis supports numerous use cases outlined in NIST 800-207 including:

Enterprise with Satellite Facilities, granting employee access to specific resources not located at that satellite location

Enterprise with Contracted Services or Non-employee Access, enabling contractors and third parties to access specific enterprise applications without compromising network security

Collaborating across enterprise boundaries, where employees or contractors may not be collocated yet need to share applications and data

NIST & Traditional VPNs

A common objection to new technologies like Zero Trust is that virtually all organizations have some level of VPN already deployed. However, it is important to note that most VPNs were designed years ago for much simpler access requirements and cannot address today's more stringent application-only access needs.

NIST's Zero Trust recommendations go beyond what typical VPNs offer. They provide network-level access, not application-specific access, and they do not offer next-generation zero trust features like restricting copy/paste or downloads like Axis does. Moreover, they require extensive configuration and management, especially in cloud and multi-cloud environments.

The table below illustrates how VPNs fall short when compared against next-generation access solutions such as Axis' Application Access Cloud:

	Axis	Traditional VPN
Cloud & On-Premises Enables full application access for Hybrid IT environments	Yes	On-Premise Only
End-to-end Zero Trust Ensures continuous authentication and authorization	Yes	No, one-time authentication
Adaptive Authentication Constantly monitors sessions to ensure appropriate access	Yes	No
Fine-grained Policy Enforcement Grants or denies application-specific access	Yes	No
Agentless Streamlines and simplifies user experience	Yes	No, Client Required
Application Access Restricts access to individual applications, rather than whole networks	Yes	No, network level only
Simplified Management Enables rapid deployment and tear down based on use case	Yes	No, typically complex
Anomaly Detection Mitigates and reduces the chance of malware propagation	Yes	No
Protocol Validation Automatically deconstructs and reconstructs app requests to eliminate malformed and potentially malicious requests	Yes	No

Summary

While Zero Trust is a relatively new term, the underlying concepts are not complicated: verify and authorize all users before they are allowed to access any resource; enforce the same policies for cloud and data center access; govern and restrict users' access to individual applications through policies. And, in fact, your organization has likely implemented one or more Zero Trust technologies already.

Axis Security, however, is designed from the ground up with Zero Trust in mind. It ensures that all application access adheres to Zero Trust tenets and requires minimal administration or management to make it all happen. Access to individual applications in the cloud or data center is provided to users without complicated policy rules, syntax, or network changes. And, without a complicated VPN.

axis security

Axis Security
3 East Third Ave, Suite 203,
San Mateo, CA 94401

Phone: +1-650-850-8991
Email: info@axissecurity.com