VION®
Building your enterprise solutions

Forcepoint

WHITEPAPER

The Journey to Zero Trust: Know Where You Are & The Road Ahead

Introduction

91% of all federal leaders say securing multicloud will be a top priority over the next two years, according to Meritalk's Redefining Cyber Playbook. And 83% are increasing multicloud adoption in response to the increase in remote work because of the pandemic. As federal agencies face more pressure to move to multicloud, security questions naturally rise to the surface. These are the top five priorities federal leaders are focused on to safely move to multicloud:

1. Federal Compliance

2. Vulnerability Management

3. Risk Management

4. Automated Analytics for Cyber Intelligence

5. Network-Centric Operations

Many of these priorities can be addressed with a focus on zero trust security. Zero trust is the security concept that organizations should not trust anyone or anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems.

Contents

What is Zero Trust?

NIST defines zero trust as the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets and resources. A Zero Trust Architecture (ZTA) uses zero trust principles to plan enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet).

The first rule of zero trust is: make no assumptions – about the level of security in your cloud and the integration of your monitoring systems needed for this security approach.

The first rule of zero trust is: make no assumptions – about the level of security in your cloud and the integration of your monitoring systems needed for this security approach. Many agencies have great tools but a false sense of protection. Customers believe they're getting more than they actually are from their cloud service provider and that protection is in place because they have access logs and identity providers. But ultimately, the business owner is responsible for security in the cloud, and with budget constraints, lack of a skilled cyber workforce and an increased attack surface, that responsibility quickly gets heavy. In turn, it calls each agency to action in evaluating what their level of protection truly is with the existing products and services they regularly use.

Because security is a process – not a product – agencies can't buy a product that "makes you secure," and protects data, people, applications and overall operations from application to application. This is where the journey begins.

Pandemic Hastens a Shifting Definition of Zero Trust

The industry is running from a perimeter concept and toward adaptive zero trust models that grant users access by trust level and how they behave.

Zero trust before Covid-19 was focused on identity and network access. Traditional perimeter defense allowed access to everything or nothing, but when people went home, the VPN was extended back to the perimeter. Achieving security in this "perimeterless world" created a lot of "noise" because everyone took IT home. This propelled human-centric security and the advent of truly adaptive security that is really a risk-based access and control mechanism around the user and the asset (server or workstation). It's in alignment with what Gartner analysts have argued in recent years with their Continuous Adaptive Risk and Trust Assessment (CARTA) strategy and the need for a "new way" because of these three factors affecting security:

1. Increased users outside of the enterprise accessing services
2. Higher number of unmanaged devices connecting to services
3. Consumption of more apps delivered from outside of the enterprise network

This is where the industry is now, in part because of natural changes but also in part because of the changed routines of 2020. The industry is running from a perimeter concept and toward adaptive zero trust models that grant users access by trust level and how they behave.

Zero Trust Cannot Work Without Continuous Monitoring

Zero trust is dependent on continuous monitoring – understanding what users are doing and where data is accessed and moving away from centralized data – focusing less on logs, more on adaptive response and profiling. Users can be individuals or non-person entities, or service accounts used by applications that are easy to profile. What access should new employees have over longstanding managers? What behaviors and patterns are typical and what are red flags?

According to Meritalk, only 37% of federal agencies say their visibility into cloud environments is excellent.

According to Meritalk, only 37% of federal agencies say their visibility into cloud environments is excellent. And as government is already struggling to staff their cyber needs, the issue can easily persist. To be successful, agencies have to be able to scale their monitoring approach without relying on dramatic changes to staffing. This sets the stage for why automated profiling and behaviors monitoring are critical. Adaptative security with continuous monitoring grants users access based on needs, controls and records or potentially blocks access without human intervention to reduce the stress on resources. With the right automated data collection, even some of the decision-making can be automated as well.

Understanding these profiles enables agencies to automate and identify triggers that can prevent security events. This kind of adaptive security focused on behaviors moves agencies past an "all or none" approach to accessing vulnerability and risk at many deeper levels. Much like a credit card company emphasizes fraud protection by monitoring for unusual activity and responding quickly to these triggers, adaptive security creates a system to monitor users and assets and all the variables that come with the territory to better distinguish outsider from insider threats and change remediation to prevention.

Creating a Layered Defense – The Virtual "Credit Score"

In the past, cyber has been careful to not impede or impact the user by making a block or a phone call to prevent access. But as organizations get so large with thousands of IoT devices on the table, it becomes imperative to score both the asset and the credential used with that asset to determine its relative level of risk.

This is creating the current paradigm shift from making security more checklist-based or compliance-based versus risk-based. In order to bake security in, it has to be built in early. Agencies can do this by developing a virtual "credit score" to enable zero trust with assets and user monitoring which provides a better, more integrated picture of what activity to focus on. Perhaps an application developed has a low credit score because it's not as trusted or it's using credentials it shouldn't be – this is the definition of being vulnerability and risk-based versus checking the boxes.

For example, if a user uses their admin to connect to a server and an active directory and then pivots to go down other paths, a user that has been "scored" could be caught much earlier as they go beyond typical behaviors.

Behavioral analytics technology can provide the missing piece of identifying high-risk behavior from structured and unstructured data to prevent malicious users.

The bottom line: context matters and so does intent. Behavioral analytics technology can provide the missing piece of identifying high-risk behavior from structured and unstructured data to prevent malicious users. More mature organizations are achieving improved security performance with this kind of layered defense integrating the identity and network tools for more insightful, continuous monitoring using analytics.

What’s Holding Agencies Back from Adaptive Security

With the detailed profiler, users can get a grasp of performance conditions and the statistical communication status of the MPI in the specified section.

The industry has typically emphasized the importance of orchestration in security, but in reality, this could be automating the same problems the industry has already faced, which is delivering more events and data without focusing on individual understanding of risk and integrating tools to determine that risk.

Integration of identity, network providers and continuous monitoring is the key to success. No vendor has a complete zero trust solution despite the claims in the market but all of them provide a component. In the case of identity providers, they do a good job of telling IT leaders who is granted access, but not about what happens after that access or how that user’s risk may have changed based on recent shifts in behavior (downloads, etc.) after access. These providers stop short of identifying what the user’s cyber fingerprint can tell the organization about their level of risk. This is why integration is critical for getting the full story in the hands of decision makers.

The biggest hurdle to adaptive security is the teams that acquire the identity and network technology are typically in different parts of the organization – so many CIOs and CISOs are moving toward standing up “trust teams” with the right organizational structure to move away from the siloed approach. This is an essential part of the journey – recognizing the connection and continuous monitoring of disparate pieces.

Where to Go from Here?

As more organizations are moving to a hybrid multicloud environment and as-a-Service, it's imperative to weave in zero trust services as a practice. In a recent study with Meritalk, federal agencies said if they were given the chance to rebuild their cyber strategy, they would start with zero trust from the beginning. But zero trust is not a product, it's a journey that requires context and analysis of data across users and assets. It's a cultural shift that mandates tying individual pieces together including:

No vendor has a complete zero trust solution despite the claims in the market but all of them provide a component.

- Confirming identities – the people and their behaviors in your environment.
- Getting access visibility – seeing who is accessing what and ensure security around accounts and devices.
- Continuous monitoring – with the right users, visibility and security of the devices being used, agencies can understand adaptive security.

The integration of these key tenets is impacting the way organizations acquire technology and bring together different business units for the common goal of preventing breaches, proactively identifying potential threats and focusing on active and responsive risk and vulnerability assessments over a traditional security checklist. The perimeter is no longer set, but constantly morphing, and the security approach has to do the same to keep pace.

About ViON Corporation

ViON Corporation is a cloud service provider with over 40 years' experience designing and delivering infrastructure as-a-Service for government agencies and commercial businesses. The company provides a large portfolio of IT as-a-Service, including infrastructure, multi-cloud and artificial intelligence (AI) solutions that extend from the edge to the core to the cloud. Focused on supporting the customer's IT modernization requirements, ViON's Cloud Services is changing cloud management for the market, providing a streamlined platform to audit and control technology in an evolving multi-cloud world. The ViON Marketplace™ allows customers to research, compare, procure, manage and report a full range of everything as-a-Service solutions from leading manufacturers via a single platform. ViON delivers an outstanding customer experience at every step with professional and managed services, backed by highly trained, cleared resources. A veteran-owned company based in Herndon, Virginia, the company has field offices throughout the U.S. (vion.com).

About Forcepoint

Forcepoint user protection solutions can both directly ingest relevant context from identity and access management (IAM) solutions and (optionally) enrich them with risk user information to dynamically enforce policies. Two IAM/IDaaS ecosystem partners that integrate with Forcepoint's Behavioral Analytics and are now available for use are Okta and Ping. The combined solution delivers enriched visibility into user activities, enhances risk scoring, and enables risk adaptive authentication policy for joint customers. Forcepoint plans to continue to add technology alliance partners to its ecosystem. We plan to enable customers to drive risk-adaptive authorization to key enterprise resources such as critical data. Stay tuned for exciting developments in this area.