How Zero Trust Can Solve the Cloud Security Riddle

MARKET TRENDS REPORT

govloop

sumo logic | aws

Executive Summary

President Joe Biden's recent **executive order (EO) on cybersecurity** made clear that the public sector must move in a new direction: cloud computing protected by zero-trust security. It's the best way to identify, deter and respond to increasingly sophisticated and malicious cyberattacks. The newer **Guidance on Federal Information Security and Privacy Management Requirements** makes the case even more strongly, detailing changes to the current approach of Federal Information Security Modernization Act (FISMA) oversight and metrics collection designed to improve risk-based decision-making with a zero-trust focus.

While the benefits of zero trust are clear, it can be difficult to know where to start. First, embracing zero trust isn't simply a matter of adopting certain technologies – no one tool will do the trick. Instead, achieving true zero trust requires an open mind, strong convictions and modern technology.

To adopt cloud and zero trust simultaneously, agencies will need to balance their current investments with some new and perhaps unfamiliar tools for analyzing, monitoring and governing access to their data and other IT resources.

To learn more about how to make zero trust work, GovLoop teamed with Sumo Logic, which helps organizations incorporate continuous intelligence into their digital futures.

By The Numbers

81%

of public-sector organizations now **include and/or define** a zero-trust approach to cybersecurity.

88%

of IT and cybersecurity professionals say that their cybersecurity program **must evolve** to protect their cloud-native and public cloud workloads.

29%

of IT professionals say that they still **use manual processes** to manage cloud security.

"The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access. It is a dramatic paradigm shift in philosophy of how we secure our infrastructure, networks, and data, from verify once at the perimeter to continual verification of each user, device, application, and transaction."

- **The Defense Department's (DOD) Zero Trust Reference Architecture**

81%

of federal IT leaders say that **increased telework** has accelerated their agencies' use and deployment of network visibility solutions.

46%

of respondents said that **inadequate security visibility** makes it difficult to differentiate between vulnerabilities that pose real threats versus those that do not.

41%

of agencies are still in the early stage of understanding **who or what is accessing** their networks and applications.

Approaching Zero-Trust Cloud Security Intelligently

The Challenge: A Constantly Shifting Environment

As agencies turn to a zero-trust model to strengthen cloud security, they are likely to encounter four obstacles:

- ***Lack of visibility.*** Achieving zero trust requires visibility into every part of the environment – data, networks and devices. This can be difficult to achieve in multi-cloud environments where resources are spread across multiple private and public clouds along with on-premises locations.
- ***Legacy tools.*** Although it's tempting to use the same security tools and processes in the cloud that were effective in on-premises environments, it's not always a good idea. Often, these on-premises solutions weren't built to collect, analyze and act on cloud-based workloads. Instead, they were built to work in a perimeter-based security model – the opposite of zero trust.
- ***Shifting attack surfaces.*** While multi-cloud environments provide many benefits like agility, scalability and cost management, the growth of cloud has also significantly expanded the attack surface. This has required agencies to find better ways to manage risk by improving platform, network and application security.
- ***Hybrid workforces.*** Roughly a third of civil servants around the world will remain hybrid workers permanently, according to **research** from Forrester. This distributed model has required agencies to adopt more Software-as-a-Service (SaaS)-based business productivity apps like Office 365. Typically, employees working from home are accessing these applications via a web browser instead of a virtual private network (VPN). While this is progress, it also results in reduced visibility inside and outside of the traditional network or perimeter.

The Solution: Cloud-Native Zero-Trust Security

As more agency workloads move to the cloud, it makes sense to manage and secure those workloads with cloud-based tools, which are designed to scale and have the application programming interface (API) support that legacy tools don't.

This approach is true when it comes to zero-trust security. Approaching zero-trust security with a cloud-native, multi-tenant platform is the most effective way to continuously monitor data, networks, users and other IT assets in real time.

"When you move into the cloud, it's not uncommon to lose visibility to your data and applications, but that visibility is more important than ever because the cloud is a shared responsibility model where the agency has to take some ownership of security," said George Gerchow, Chief Security Officer (CSO) at Sumo Logic.

One way to improve that visibility is by standardizing on a security information and event management (SIEM) platform, which provides a single view of all data, no matter where it resides. With this view, it's easier to classify the data, understand who is accessing it and secure it.

In addition to real-time monitoring, a cloud-based SIEM platform also provides modern logging and analytics tools, which help correlate, normalize and parse data. Logging is an important way to keep track of events generated by all parts of the infrastructure, from cloud infrastructure and networks to containers and applications.

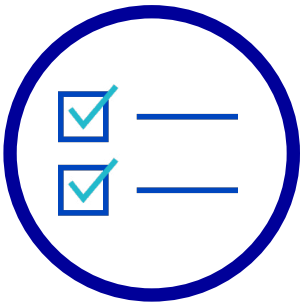
Some organizations choose to add a security operations and response (SOAR) system, which connects applicable tools to fully automate incident response. With this approach, security operations teams can pinpoint the most important incidents, leaving the rest to be handled automatically.

Zero trust doesn't happen overnight, and that's OK, Gerchow said. "When it comes to achieving zero trust, it's OK to use the 'crawl, walk, run' approach," he said.

Best Practices in Zero-Trust Cloud Security

Don't look for a turnkey approach to zero trust.

If a vendor tells you its technology will make your entire organization compliant with all principles of zero trust, don't believe it. That's because there are so many tools and processes that go into making zero trust possible – not only MFA and SSL, but network security tools and a modern, cloud-based SIEM platform. Just as important to achieving full zero trust is a change in policies and strategies; it requires people and the agencies they work for to treat all access and devices as potential threats.

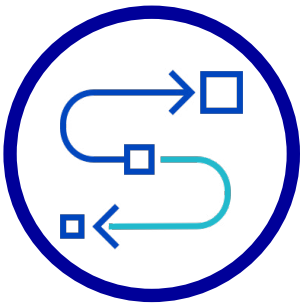


Look for modern FedRAMP solutions.

Achieving certification under the Federal Risk and Authorization Management Program (FedRAMP) is a point of pride for cloud vendors, and it's a great way to ensure that solutions are fully secure. Yet today, many FedRAMP-certified solutions were developed for on-premises environments, while agencies are actively looking to move more workloads to the cloud. That doesn't mean you have to forgo FedRAMP, but it does mean working a little harder to find those FedRAMP-certified cloud solutions. They are out there, and more are available every year.

Require a software bill of materials.

While it's critical to ensure that your own applications, infrastructure and data are fully secure, that's not enough. The security of the tools you use and the **partners** you rely on is equally important. The recent EO spells out its importance, requiring agencies to fully vet every partner and third-party product. That means requesting a software bill of materials for each product. "The executive order woke people up to the fact that agencies have to look at how the platform is built, how the coding works, what vendors are involved, how much open source is being used, whether it includes things like container vulnerability scanning and whether bug bounties and pen testing are being performed," Gerchow said.



Understand that zero trust is a journey not a destination.

Threats change, technology changes and missions change. Any or all these things will cause changes to zero-trust strategies and technologies. To keep things on track, Gerchow suggested choosing metrics important to the organization and measuring them quarterly. For example, if you find that fewer employees have access to resources that they shouldn't during a quarterly access review (QAR), it's probably a sign that you're on the right track.

Use Cases for Cloud-Native SIEM

Implementing a cloud-native SIEM is one of the best ways to keep cloud workloads secure and move toward zero trust. Here are a few examples of what this technology can do:

Tracking changes and identifying security events. As agencies move more workloads to the cloud, it's not uncommon to run into problems effectively tracking changes in active directory objects like users, groups and policies. During this transition period, it can also be difficult to identify security events quickly and consistently, like failed logins. By adopting a cloud-native SIEM, IT staff can gain deep visibility into the agency's active directory deployment. The platform also makes it easier to root out and fix undesirable changes and fine-tune alerting around security incidents.

Bringing together disparate sources to quickly confirm security events. Keeping cybersecurity incidents to a minimum requires full visibility. Typically, a system might alert security staff if it sees a user logging in from London and California at the same time. That's helpful, but it's not enough. To detect whether a breach is occurring, it's important to have additional information, such as whether MFA or a VPN is involved. By centralizing, correlating and parsing all available information, agency analysts can easily determine whether a brute force attack is taking place.

Protecting sensitive data. With the increase in both nation-state and insider threats, agencies that must protect the personal data of millions of citizens are on high alert. Instead of cobbling together a group of security tools and procedures, many of which were designed for on-premises environments, more agencies are choosing the SIEM route to protect that data, focusing on cloud-native SIEM platforms to accommodate the transition of critical workloads to the cloud. This approach presents all ingested data in a consistent, understandable and correlated format that pinpoints critical threats requiring immediate investigation.

HOW SUMO LOGIC HELPS

Sumo Logic's focus on continuous intelligence helps agencies build, run and secure modern applications and cloud infrastructures. Its solutions are fully certified at the FedRAMP-Moderate level, and have achieved SOC2, HIPAA, ISO and Cloud Security Alliance (CSA) STAR certification.

With a cloud-native multi-tenant SaaS architecture, its automated Cloud SIEM Enterprise platform consolidates siloed operations and disparate security information across users, networks, devices, alerts, cloud services and applications. Cloud SIEM Enterprise uses pattern and threat intelligence matching with correlation logic, statistical evaluation and anomaly detection to filter raw records down to signals in near real time. With this information always consolidated and available, security staff can analyze security data real time, resulting in faster, more effective decisions.

Sumo Logic's Cloud SOAR connects disparate tools to fully automate incident response and leave time-consuming, manual tasks behind. Playbooks highlight appropriate courses of action, reducing the time needed to remediate incidents.

Agencies also have the option of adding threat-hunting and response as a service, which essentially adds an elite cyber threat-hunting team to the agency's security staff. This provides instant access to SpecOps analysts, advanced threat-hunting and rapid response.

Learn more: **https://www.sumologic.com/public-sector/**

Conclusion

Achieving zero trust results in better data protection, fewer vulnerabilities, continuous compliance and less organizational risk. Many agencies are now weighing in; recently, the Defense Department (DoD) announced plans for **a new zero-trust portfolio management office** to help Defense agencies meet zero-trust goals.

At the same time, agencies are being encouraged to move data, infrastructure and applications to the cloud when it makes sense. Adopting cloud and zero trust is challenging, but the result is greater visibility and security across the board. It's OK to start small by adopting security strategies like MFA and SSL, but eventually, all agencies will have to make the leap.

Adopting a cloud-native multi-tenant SIEM platform paired with a SOAR solution is a good way to achieve both goals for agencies moving forward.

sumo logic

ABOUT SUMO LOGIC

Sumo Logic Inc., (NSDQ: SUMO) is the pioneer in continuous intelligence, a new category of software, which enables organizations of all sizes to address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,100 customers around the world rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy. For more information, visit www.sumologic.com.

aws

ABOUT AWS

For 14 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 175 fully featured services for compute, storage, databases, networking, analytics, robotics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 77 Availability Zones (AZs) within 24 geographic regions, with announced plans for 15 more Availability Zones and five more AWS Regions in India, Indonesia, Japan, Spain, and Switzerland. Millions of customers— including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

govloop

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop