Getting Legacy Systems Up to Speed With Modern Security

MARKET TRENDS REPORT

govloop

KARSUN
SOLUTIONS
Enterprise Modernization Experts

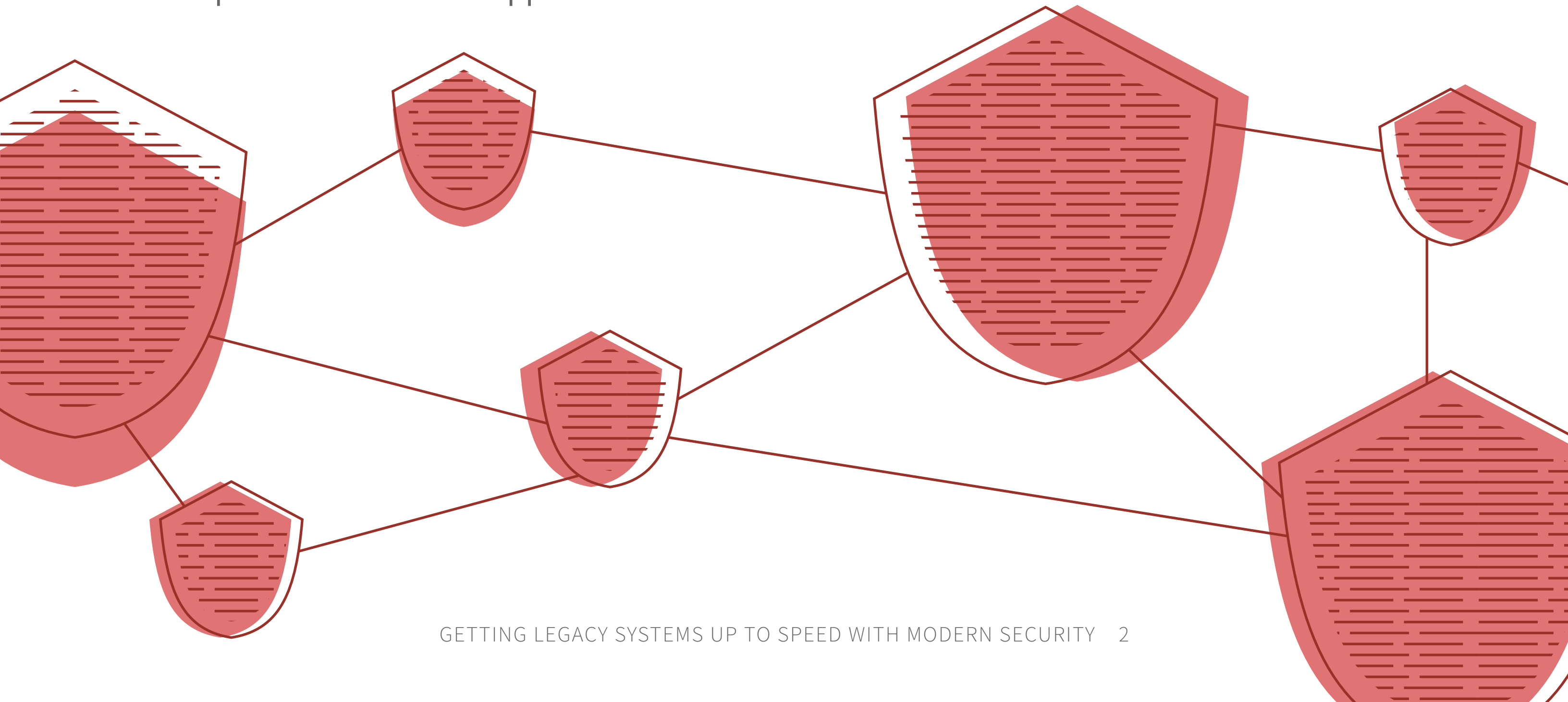
Introduction

Government agencies have an urgent need to strengthen their cybersecurity postures, spurred by the mounting cyberthreats targeting government and the mandates of the White House Executive Order on Improving the Nation's Cybersecurity. At the core of those modernization efforts is adopting a zero-trust architecture (ZTA), which focuses on the continuous verification of people and devices that are accessing applications, data and systems.

A ZTA, however, can be difficult to implement, especially when compounded by the presence of legacy agency systems and applications that aren't made for a distributed, cloud-based environment.

An effective way to solve that problem is through the use of a service mesh, an infrastructure layer that connects different parts of an application or system, allowing them to communicate with one another. While most commonly used for cloud-native capabilities such as microservices and containers, a service mesh can be the most efficient way to bring legacy systems into the ZTA fold.

To learn more about how a service mesh approach can integrate legacy systems into a ZTA, GovLoop partnered with Karsun Solutions, a modernization company that applies innovative approaches to help achieve agency missions. We'll examine how a service mesh can help meet security goals, detail best practices in using it to implement a ZTA and offer a specific example of how Karsun's approach has worked.



By The Numbers

59%

of organizations that have implemented zero trust say they still have difficulty identifying users and devices on an ongoing basis.

80%

of C-level executives say zero trust is a priority for their organizations.

25%

of organizations say they are still too reliant on virtual private networks.

33%

of organizations that have implemented zero trust say they have not been able to integrate their on-premises and cloud operations.

> ***"Shifting from perimeter defense to ZTA is not as easy as flipping a switch; it is a complex undertaking. … Making such a shift requires adopting new policies, processes and structures."***

— Center for Strategic & International Studies

94%

of executives say they are in the process of implementing zero-trust strategies.

77%

of executives say they are increasing spending on zero trust over the next 12 months.

$2.5 billion

the amount allocated to the Cybersecurity and Infrastructure Security Agency in the proposed fiscal 2023 federal budget to support the transition to zero trust

How to Keep Legacy Systems From Being Exposed

Challenge: An Expanding Attack Surface

Cloud environments and the introduction of automation and Internet of Things (IoT) devices have greatly expanded the attack surface. “There are a lot of points of entry now,” said Raghurama Pantula, Director of Information Security for Karsun Solutions. “So, there’s a high residual risk.”

One of the most important goals of zero trust is to prevent the kind of credential compromises that hackers have been exploiting in ransomware and other attacks by requiring continuous authentication and authorization of identities – human and non-human – on the network. “If I were to put it in a single phrase, it’s trust upon verification,” Pantula said.

But legacy hardware and software, which abound in government agencies, can create a barrier to implementing zero trust. “Legacy applications never were focused on anything like zero trust, because that was not a philosophy that existed at that point of time,” he said.

A Government Accountability Office report issued in June 2021 noted that most of the federal government’s $100 billion fiscal year spending on IT went to maintaining and operating existing technology, including old, unsupported systems with known vulnerabilities.

Among the key challenges:

- Centralizing identity and access control with application-aware policies
- Unifying access controls into a single dashboard
- Strengthening security through comprehensive endpoint posture and automated penetration testing
- Reducing website exposure with intelligent Forcepoint technology
- Achieving high performance at scale

The Solution: A Service Mesh Approach

A service mesh approach can enable agencies to incorporate legacy applications and systems into a ZTA with minimal retrofitting.

In a containerized environment, like those built on Kubernetes, a service mesh solution has two distinct component behaviors: a data plane and a control plane. Every instance of a service is associated with a proxy, which delivers a dedicated domain-agnostic infrastructure layer (abstraction) for capabilities like observability, traffic management and security without adding them to your code. The data plane is a collection of such proxies. The proxies are deployed alongside each instance of a service to communicate with the other services in the system, handling all calls to and from a service, including authentication and authorization, encryption and others.

The control plane is responsible for managing the configuration of the data plane proxies. It provides an interface for a human user to configure the behavior of the proxies and makes that configuration available to proxies via another application programming interface (API).

Until now, non-containerized legacy applications required a lift-and-shift approach necessitating migration to a virtual machine. Now, new tools like HashiCorp Consul allow even these non-containerized apps to follow the same principle applied to containers.

A service mesh approach, by performing tasks abstracted from existing applications, allows agencies to implement the principles of zero trust across the enterprise. It enables enterprise-managed accounts, while ensuring that activity on the network is consistently tracked and assessed through regular logging, monitoring and auditing.

It also can help ensure that:

- Network traffic between and within isolated agency systems is reliably encrypted
- Enterprise applications are tested internally and externally, and can be made available to staff securely via the internet
- Federal security and data teams can work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information

Implementing a ZTA with a service mesh infrastructure can be aligned closely with CISA’s five pillars of zero-trust maturity:

Identity: Ensuring only validated access to networks.

Devices: Implementing compliance monitoring, access controls and asset management to all devices.

Networks: Maintaining network segmentation while allowing authorized communication between components.

Applications and Workloads: Conducting testing and vulnerability assessments of applications.

Data: Allowing agencies to inventory, categorize and label all data.

Best Practices in Implementing ZTA

Roles and Responsibilities

An essential feature of zero trust that some organizations ideally should be following already is that of least privilege – ensuring that users have access only to the data and applications they need to do their jobs. Along with multifactor authentication, it can go a long way toward preventing credential-based attacks.

Under least privilege, only authorized users are given access to certain systems, and even then are given only the minimum privileges required to perform their tasks. Privilege creep – in which users are given more permissions than they really need – is a widespread problem in enterprises in every sector. Attackers who compromise those users' credentials can often move freely about a network.

"One of the primary things is having established roles and responsibilities that are implemented efficiently," Pantula said. A person requesting access to perform a system administration job, for instance, must have that role. Access is granted only after verification has been completed. "It's deny all, verify and then allow," he said.

Continuous Monitoring

Cybersecurity is an ongoing process, because cyberthreats don't sleep. Logging, monitoring and auditing are essential components of maintaining security.

Access logs provide insights into web traffic and can identify anomalies that could indicate vulnerabilities. Monitoring should be applied to users, devices and services as a way to detect and identify malicious activity (whether originating inside or outside the network), rogue devices and other attempts to access or exfiltrate data. "Continuous monitoring is a very important factor," Pantula said.

Audits can assess the quality of a zero-trust framework and identify where improvements may be needed. They also can detect unknown traffic on the network, which is the first step in determining whether it is hostile.

Access Controls

Just as users' passwords should be rotated every 90 days or so, security keys need to be changed with regularity. Effective key management requires that cryptographic keys have a designated lifespan, and that they be replaced on schedule. Secure storage also is required to protect access to the keys.

Zero-trust frameworks work on the assumption that attackers have already gained access and the network is hostile. Logging, monitoring and access controls help prevent damage from being done, while also helping to improve network performance.

How Service Mesh Brings Zero Trust to the Enterprise

Many service mesh implementations have been purpose-built for Kubernetes container environments, most often working with microservices.

Karsun has expanded on that approach, building a service mesh-based ZTA that can be applied to legacy apps in enterprise environments, whether they're operating in the cloud or within on-premises data centers. It's designed to require minimal retrofitting in order to adapt those applications to a zero-trust environment.

In one example of how its service mesh approach works, Karsun Solutions worked with an organization to develop a service-mesh ZTA for identity and access management to control service-to-service communications. The solution could be hosted on Windows servers or involve Linux-based applications and containers operating within Kubernetes.

Outbound communications from the cluster could also be controlled with the help of egress controllers, which are designed to prevent insiders from sharing information with unauthorized users. Both ingress (traffic arriving from outside the network) and egress activities are controlled by policies managed by the service mesh administrators.

Importantly, services started out with no trust and no allowed routes. All traffic was configured via policies to ensure that only authorized sources and destinations get access to the services. This created a smaller attack surface that prevents even a threat actor with access to a compromised set of credentials from doing much damage by limiting the attacker's movements.

Users and applications were authenticated at the ingress gateway even before their request reached the servers that deliver services, thus ensuring that unauthenticated requests never reached sensitive areas deep within the network.

HOW KARSUN SOLUTIONS HELPS

The enterprise modernization experts, Karsun Solutions is an innovative modernization company that has extensive experience working with government agencies, enabling enterprise transformation for customers including the Department of Homeland Security, Federal Aviation Administration and the General Services Administration.

It has developed a service mesh approach to ZTA that allows for the integration of legacy systems and applications. Like most service mesh implementations, Karsun's approach can be used for container-based solutions, but using products like HashiCorp Consul, the company also provides similar implementations for non-containerized legacy solutions running on Windows or Linux servers, both in the cloud and on premises. In addition to HashiCorp, Karsun can use AWS App Mesh, Istio, Linkerd, Open Service Mesh (OSM) and other similar service mesh products.

Karsun's solutions adapt and stay relevant by using secure digital architecture that's built to last. Its software development methodology is appraised at CMMI v2.0 Level 5 Maturity Level, allowing for data-driven processes that optimize delivery to an organization's customers. It's also validated for Amazon Web Services Government and Migration Competencies.

Conclusion

Cybersecurity essentially has no boundaries anymore. “There is no inside or outside,” Pantula said. “Problems can come from anywhere.” Security can no longer focus on the network perimeter because there is no perimeter when the environment includes everything from on-premises systems to the cloud and containers at the edge.

A zero-trust architecture, built on the idea that nothing and no one can be trusted until verified, is the best way forward for protecting data and systems. Implementing a ZTA can be complicated enough for agencies, but the vast array of older, often unsupported legacy systems makes the job even more challenging.

Taking a service mesh approach to ZTA simplifies that process, applying a cloud-native technique mostly used in container environments to enterprise systems, including legacy systems and applications. By enabling the components of the enterprise to communicate, a service mesh infrastructure allows zero-trust policies and practices to be applied throughout an organization.

KARSUN SOLUTIONS
Enterprise Modernization Experts

ABOUT KARSUN

Karsun modernizes enterprise systems enabling agencies to make the next technological advancement their next opportunity to elevate mission capability. IT solutions from Karsun are tailored to meet agencies’ unique needs and optimize operations. These solutions adapt and stay relevant with current trends while using secure, digital architecture built to last. Karsun is a proven modernization partner whose expertise elevates agency capabilities and ensures every next opportunity is within reach.

https://karsun-llc.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