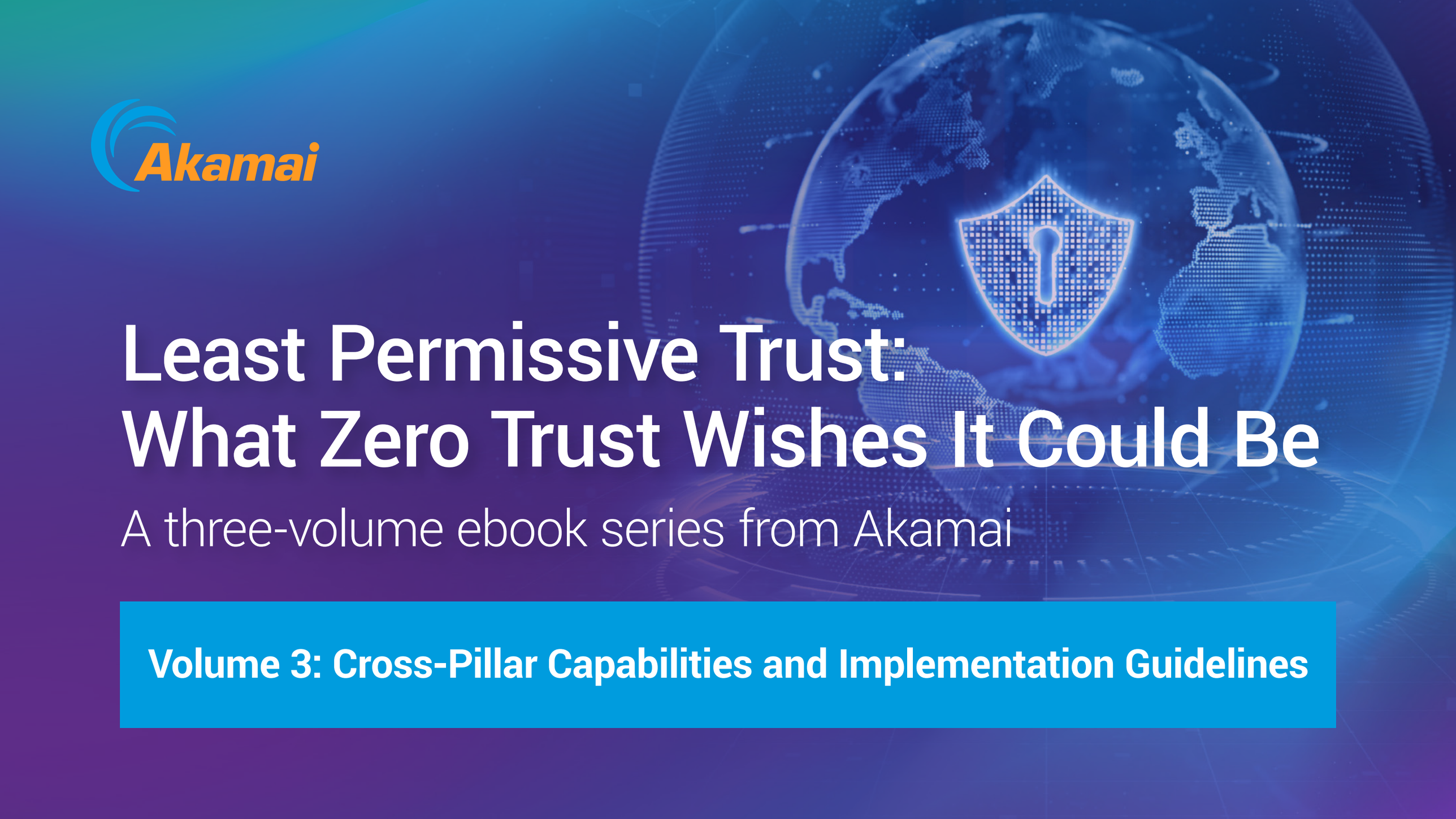


Least Permissive Trust: What Zero Trust Wishes It Could Be

A three-volume ebook series from Akamai

Volume 3: Cross-Pillar Capabilities and Implementation Guidelines

In Volume 1 of this ebook series, **Least Permissive Trust** was introduced as an important concept for federal agencies and departments implementing the Cybersecurity and Infrastructure Security Agency's (CISA's) **Zero Trust Architecture**. Volume 2 continued the discussion, exploring the concepts of identity management, application access, and microsegmentation. In Volume 3, we examine the need for **cross-pillar integration** in cybersecurity and present practical Least Permissive Trust **implementation guidelines**.

Integrating cross-pillar capabilities

As federal agencies and the Department of Defense (DoD) adopt modern security frameworks like **Zero Trust** and **Least Permissive Trust**, integration across all security layers becomes paramount. One of the main challenges with Zero Trust architectures, particularly when aligned with **CISA's Five Pillars** (Figure 1), is the risk of creating **technology silos**. Each pillar often operates independently, leading to fragmentation in security controls, policy enforcement, and threat detection.

For federal agencies managing highly sensitive data and complex infrastructures, this fragmented approach can introduce significant security risks. Attackers often exploit the lack of visibility between pillars or capitalize on inconsistent policy enforcement across different systems. To mitigate these risks, organizations must adopt a **unified, cross-pillar security model** that integrates **visibility and analytics, automation and orchestration**, and **governance** across all pillars, as shown along the bottom of Figure 1. This will ensure consistent policy enforcement and eliminate gaps that adversaries can exploit.

Akamai's **identity and credential access management (ICAM) solutions, Enterprise Application Access**, and **Akamai Guardicore Segmentation** can be integrated across these pillars to enable Least Permissive Trust in a cohesive, dynamic manner. By leveraging cross-pillar capabilities, federal organizations can prevent technology silos, streamline security operations, and dynamically enforce security policies across the entire network.

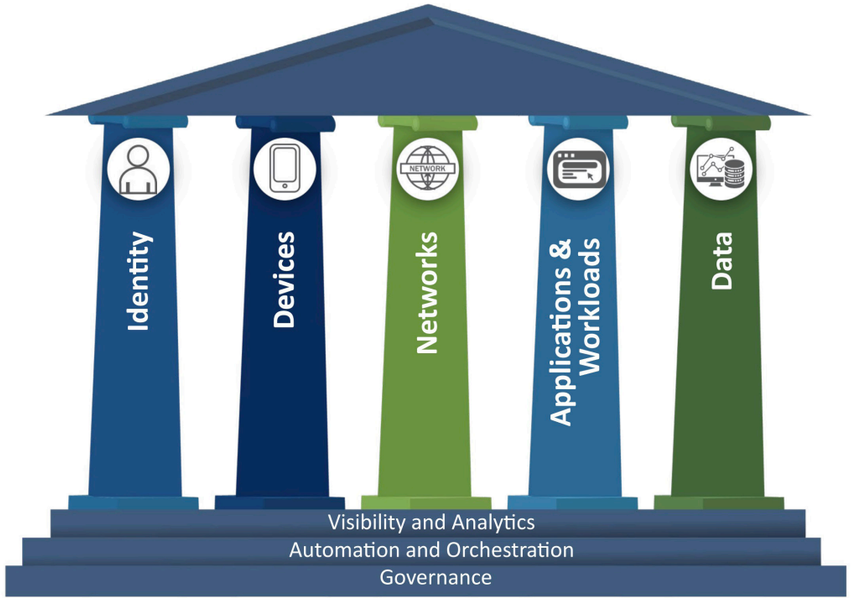


Fig. 1: Three cross-pillar capabilities support CISA's Zero Trust model (Source: CISA)

Why cross-pillar integration is essential

CISA's five pillars each serve distinct security purposes, but when treated in isolation, they can create significant gaps:

Siloed identity systems

Identity systems that only verify user credentials without considering network or device security can expose applications to unauthorized access.

Fragmented device management

Devices that are secured independently of network or application security might still allow malicious traffic or unauthorized data transfers.

Inconsistent application security

Applications that enforce strong access controls but lack integration with identity and network security can become vulnerable to attacks such as lateral movement or privilege escalation.

Cross-pillar integration addresses these issues by ensuring that all security controls are **coordinated, continuously updated**, and enforced based on real-time data from all layers. Instead of treating identity, device, network, application, and data security as separate entities, cross-pillar integration allows for **holistic, unified policy enforcement**. This ensures that every access request, data transfer, and user interaction is evaluated against comprehensive, real-time security intelligence from across the organization.

Core elements of cross-pillar integration

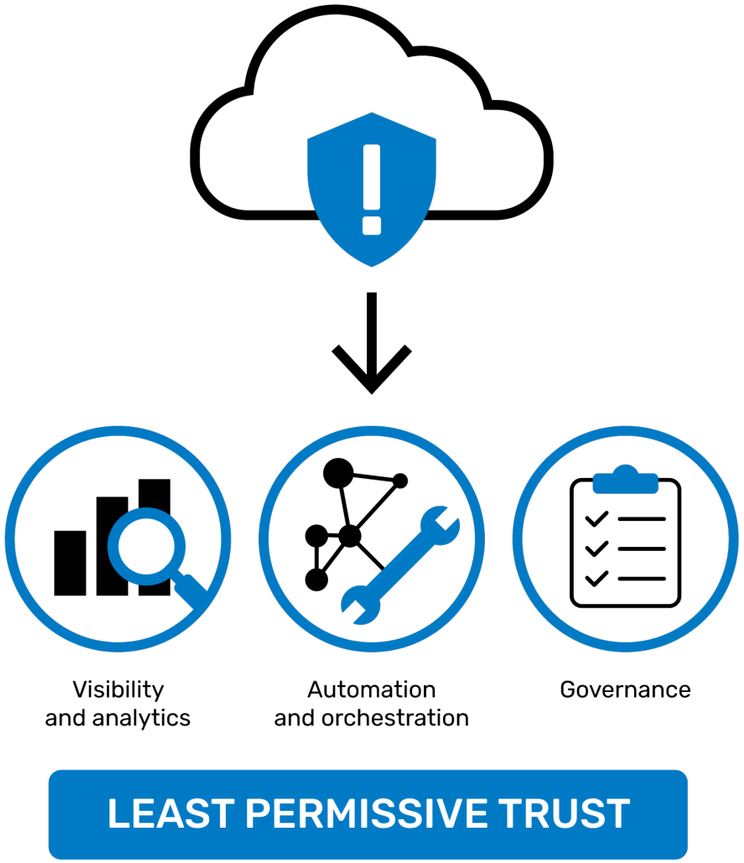
To achieve a unified security model, cross-pillar integration must focus on three key areas: visibility and analytics, automation and orchestration, and governance. These elements are essential for enabling Least Permissive Trust, where access and permissions are dynamically adjusted across all pillars based on real-time risk assessments.

1 Visibility and analytics

Visibility is critical for detecting threats, understanding user behavior, and enforcing dynamic security policies across all pillars. Without full visibility into how identities, devices, applications, and data interact, security teams are left in the dark, making it difficult to detect anomalous behavior or unauthorized access attempts. Akamai's ICAM solutions, Enterprise Application Access, and Akamai Guardicore Segmentation provide comprehensive, cross-pillar visibility:

- **Akamai's ICAM** solutions enable visibility into **user identities and credentials**, continuously verifying users' actions and access permissions across devices, networks, and applications.
- **Enterprise Application Access** provides insight into **application access patterns**, tracking how users interact with sensitive applications and ensuring that access is dynamically adjusted based on contextual data.
- **Akamai Guardicore Segmentation** monitors **network traffic between segmented workloads**, providing visibility into east-west traffic and detecting any attempts at lateral movement within the network.

By integrating these capabilities, federal agencies can **correlate data across all pillars**, enabling a unified view of security events. For instance, when a user requests access to an application, Akamai's solutions can check not only the user's identity but also the security of the device, the network they are using, and the real-time behavior of the application they are accessing. This **holistic visibility** allows agencies to detect potential threats faster, minimize the risk of privilege escalation, and ensure that permissions are dynamically adjusted in response to real-time risk assessments.



2 Automation and orchestration

In a traditional security model, responding to incidents and enforcing policies across multiple systems are often slow, manual processes. With Least Permissive Trust, security policies must be enforced dynamically across all pillars, which requires a high level of automation and orchestration. This ensures that as risk levels change, permissions are immediately adjusted to the minimum necessary level, reducing the chance of human error or delayed response.

Akamai's suite of solutions offers automated workflows that span identity, network, and application security:

- **Akamai's ICAM solutions** allow for the **automated adjustment of access permissions** based on real-time identity verification and contextual data. For example, if a user's behavior deviates from the norm, their access to critical applications can be automatically restricted.
- **Enterprise Application Access** automates the process of securing application access, ensuring that users can only access applications through a secure proxy and that permissions are continuously updated based on changing risk factors.
- **Akamai Guardicore Segmentation** offers **automated microsegmentation**, dynamically adjusting network segmentation policies based on real-time traffic patterns and detected anomalies. This ensures that any suspicious activity within the network is quickly isolated, preventing lateral movement.

By automating these processes, federal agencies can ensure that security policies are enforced consistently and rapidly, reducing the window of opportunity for attackers. Orchestration tools further enhance this capability by coordinating security operations across different systems, ensuring that changes in one area (e.g., identity verification) trigger corresponding actions in other areas (e.g., network access or application permissions).

3 Governance

Governance is the foundation of any security strategy, ensuring that policies are consistently enforced across the organization and that compliance requirements are met. In a cross-pillar model, governance must ensure that all security controls — across identity, devices, networks, applications, and data — are aligned with the principles of Least Permissive Trust.

With Akamai's solutions, federal agencies can implement **governance policies** that span all pillars, ensuring that access control, data protection, and compliance requirements are enforced holistically. This includes:

- **Identity governance:** Ensuring that all identity-based access controls are enforced consistently across devices, applications, and networks and that access permissions are periodically reviewed and updated based on real-time risk assessments.
- **Network governance:** Enforcing network segmentation and traffic-monitoring policies across all environments, including on-premises, cloud, and hybrid infrastructures. Akamai Guardicore Segmentation allows agencies to define network segmentation policies and ensure that they are applied consistently across the entire infrastructure.
- **Data governance:** Protecting sensitive data by ensuring that access is restricted based on **least privilege** and that all data transfers are continuously monitored for unauthorized access or suspicious activity.

By aligning governance policies across all pillars, federal agencies can ensure that their security strategy is not only effective but also **compliant with federal regulations** and **executive orders**, such as **Executive Order 14028** on improving the nation's cybersecurity.

Integrating Akamai solutions for Least Permissive Trust

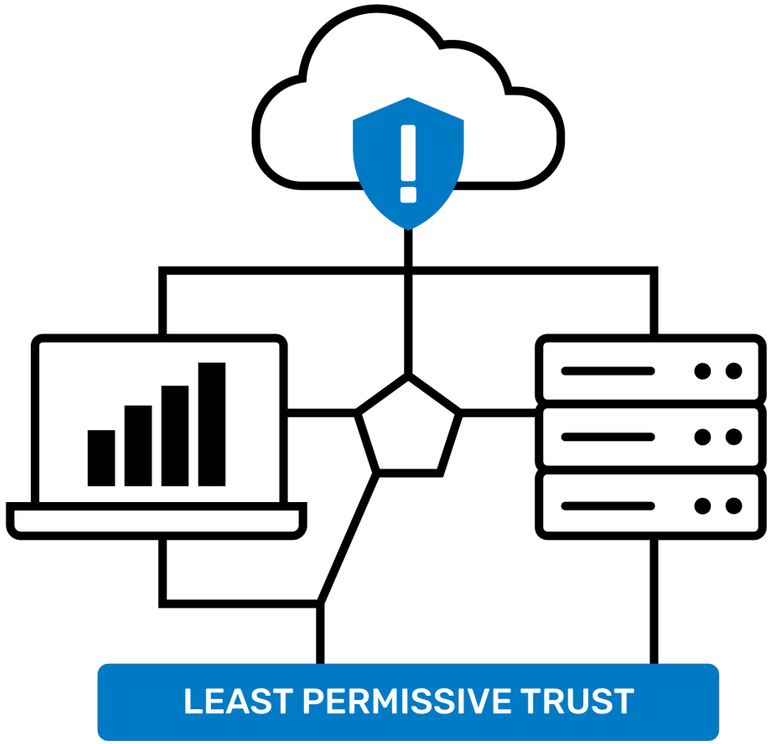
Akamai's technologies are designed to work together seamlessly, providing federal agencies with a fully integrated, cross-pillar security architecture that supports Least Permissive Trust.

1 Akamai's ICAM solutions

ICAM is the backbone of identity security, ensuring that users and devices are continuously authenticated and authorized to access specific resources. By integrating Akamai's ICAM solutions with other Akamai solutions:

- **Enterprise Application Access** can enforce identity-based access controls for applications, ensuring that users are authenticated before they access sensitive resources and that permissions are dynamically adjusted based on contextual data from the network and application layers.
- **Akamai Guardicore Segmentation** can leverage identity data to enforce **identity-based microsegmentation**, ensuring that network traffic is segmented based on who the user is and what they are authorized to access.

This integration ensures that identity, network, and application security are continuously aligned, reducing the risk of unauthorized access or privilege escalation.



2 Enterprise Application Access

Enterprise Application Access provides Zero Trust Network Access for applications, ensuring that users can only access applications through a secure proxy and that all traffic is continuously monitored and authenticated. By integrating Enterprise Application Access with Akamai's ICAM solutions and Akamai Guardicore Segmentation:

- **Akamai's ICAM** solutions can provide continuous identity verification for users accessing applications through Enterprise Application Access, ensuring that access permissions are updated based on real-time identity and behavioral data.
- **Akamai Guardicore Segmentation** can enforce **network segmentation policies** for applications, ensuring that traffic between applications is tightly controlled and that users can only access the specific applications they are authorized to interact with.

This integration ensures that application security is not treated in isolation but is continuously reinforced by identity verification and network segmentation policies.

3 Akamai Guardicore Segmentation

Akamai Guardicore Segmentation provides the **microsegmentation** needed to protect east-west traffic within a network, ensuring that users, devices, and applications are isolated from one another unless explicitly authorized to communicate. By integrating Akamai Guardicore Segmentation with Akamai's ICAM solutions and Enterprise Application Access:

- **Akamai's ICAM solutions** can enforce **identity-based segmentation**, ensuring that only authorized users and devices can communicate within specific segments of the network.
- **Enterprise Application Access** can leverage Akamai Guardicore Segmentation's segmentation capabilities to ensure that access to applications is tightly controlled, preventing lateral movement between applications or workloads.

By combining Akamai Guardicore Segmentation's segmentation capabilities with identity management and application security, federal agencies can achieve a **holistic, least-permissive security model** that reduces the attack surface and minimizes the risk of internal threats.

CASE STUDY

Cross-pillar integration in a federal agency

A large federal agency faced significant challenges with fragmented security policies across its identity, network, and application layers. Different systems managed identity verification, application access, and network segmentation, leading to inconsistent enforcement of security policies and gaps in visibility. By adopting Akamai's integrated solutions, the agency was able to:

- **Unify identity and application security:** Akamai's ICAM solutions and Enterprise Application Access were integrated to ensure that application access was always authenticated based on real-time identity data. This allowed the agency to dynamically adjust application permissions based on user behavior and device health.
- **Enforce dynamic network segmentation:** Akamai Guardicore Segmentation was deployed to segment network traffic based on identity and application access, preventing lateral movement between sensitive systems and ensuring that permissions were continuously updated based on real-time risk assessments.
- **Enhance visibility and automation:** The agency used Akamai's integrated analytics and automation tools to gain full visibility into its security posture and automate policy enforcement across all pillars.

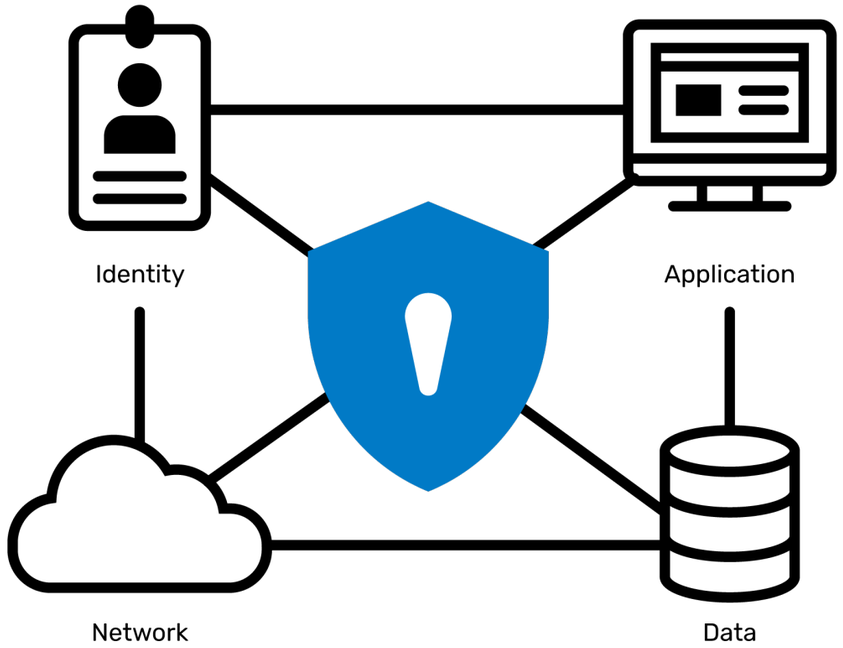
As a result, the agency reduced its attack surface, improved incident response times, and achieved **full compliance** with federal security regulations. This case demonstrates the power of cross-pillar integration to transform a fragmented security architecture into a cohesive, dynamic security model that supports Least Permissive Trust.

Achieving unified security through cross-pillar integration

The integration of cross-pillar capabilities is essential for federal agencies to implement Least Permissive Trust and protect their networks, applications, and data from increasingly sophisticated threats. By breaking down technology silos and ensuring that identity, network, application, and data security are continuously aligned, federal agencies can achieve a more resilient, adaptable security posture.

Akamai's ICAM solutions, Enterprise Application Access, and Akamai Guardicore Segmentation provide the tools needed to enable this integration, offering **holistic visibility, dynamic policy enforcement**, and **automated orchestration** across all pillars. By leveraging these technologies, federal agencies can reduce risk, prevent lateral movement, and ensure that access is always restricted to the absolute minimum necessary, without compromising operational efficiency.

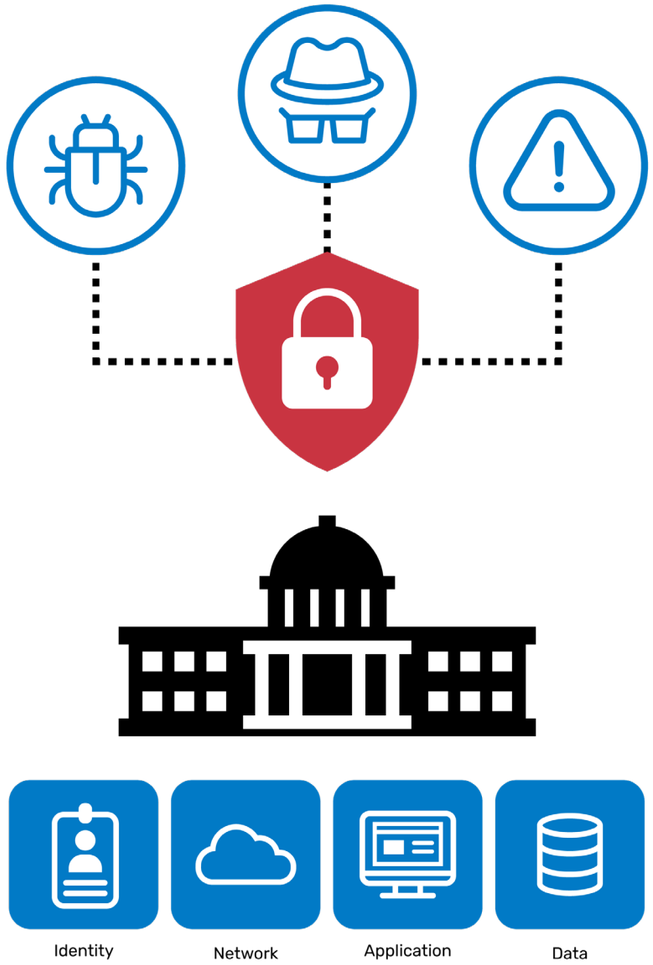
As the federal government continues to modernize its cybersecurity framework, cross-pillar integration will be key to building a security architecture that is both flexible and secure, ensuring that Least Permissive Trust is enforced across the entire organization.



Government and DoD implementation of Least Permissive Trust

Federal agencies and the DoD are prime targets for advanced cyberthreats from nation-state actors, organized crime groups, and insider threats. In response, cybersecurity strategies have shifted from traditional perimeter-based defenses to more robust models such as Zero Trust and, more recently, Least Permissive Trust. Executive Order 14028, titled “Improving the Nation’s Cybersecurity,” underscores the urgency for federal agencies to adopt Zero Trust architectures to secure their infrastructures. However, as cyberthreats continue to evolve, so too must security strategies.

The concept of Least Permissive Trust takes the Zero Trust model further by ensuring that **access is not only continuously verified but also dynamically restricted to the minimum necessary** across every layer — identity, network, applications, and data. Implementing this model in federal environments, especially within the DoD, presents both unique challenges and opportunities. Given the critical nature of government operations, the stakes are high, and the move to a dynamic, least-permissive security model is essential for safeguarding national security and sensitive information.



Challenges to implementing Least Permissive Trust in federal agencies

While the need for enhanced cybersecurity is clear, the path to implementing Least Permissive Trust across federal agencies is fraught with challenges. These challenges include:

1 Legacy systems and infrastructure

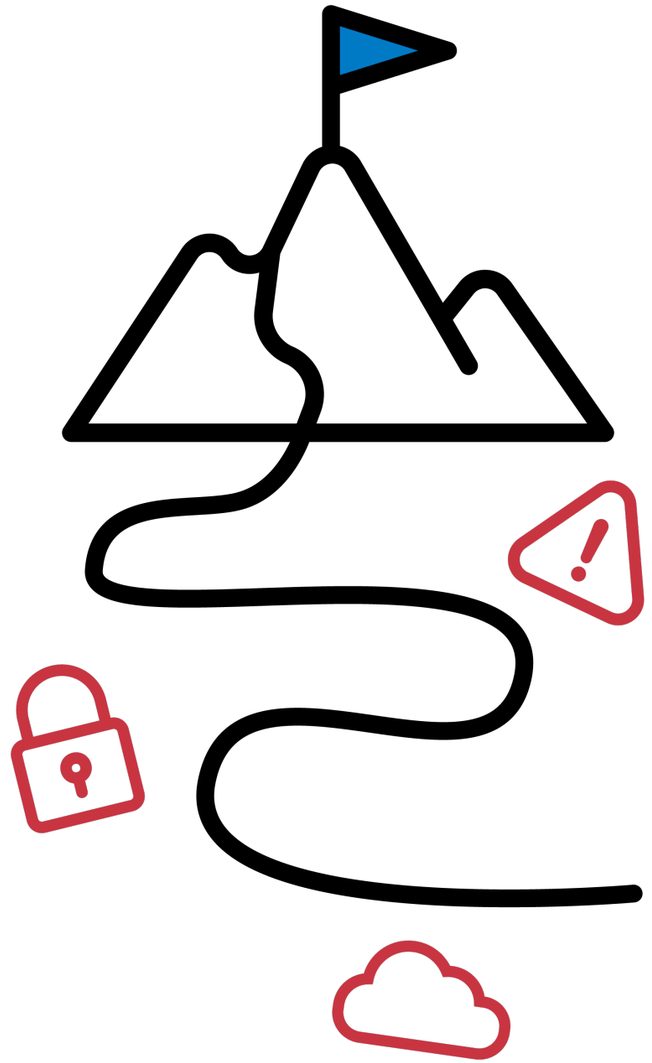
Many federal agencies and the DoD still rely on **legacy IT systems** that were not designed with modern cybersecurity models in mind. These systems often lack the necessary flexibility to support dynamic policy enforcement and cross-pillar integration. Implementing Least Permissive Trust in these environments requires significant modernization efforts, including the migration of legacy applications to more secure, cloud-based platforms or the integration of additional security layers to compensate for the limitations of older systems.

2 Complexity of multicloud and hybrid environments

As federal agencies adopt **multicloud and hybrid infrastructures**, maintaining consistent security policies across diverse environments becomes increasingly challenging. Applications and data are spread across on-premises systems, private clouds, and public cloud services, making it difficult to ensure that security policies are enforced consistently. Implementing Least Permissive Trust in such environments requires solutions that can seamlessly integrate security controls across **cloud and on-premises systems**.

3 Siloed security operations

Many federal agencies operate with **siloed security teams**, where separate groups are responsible for handling identity management, network security, and application security. This fragmentation makes it difficult to implement a unified security model, as there is often a lack of coordination and communication between teams. Least Permissive Trust requires cross-pillar integration and collaboration, making it essential for agencies to break down these silos and adopt a more holistic approach to security operations.



4 Compliance with federal mandates and executive orders

Federal agencies are subject to a wide array of cybersecurity regulations and standards, including **NIST Special Publication 800-207** (which defines Zero Trust architecture principles) and **OMB Memorandum M-22-09** (which directed agencies to implement Zero Trust by 2024). Achieving compliance with these mandates while also moving toward Least Permissive Trust can be a complex and resource-intensive process. Agencies must balance the need for regulatory compliance with the goal of enhancing security posture through dynamic, real-time policy enforcement.

5 Resistance to change

Finally, like any significant shift in security strategy, the move to Least Permissive Trust can be met with **cultural resistance** in federal agencies. IT and security teams may be accustomed to traditional security models and may be hesitant to embrace new technologies or approaches that require more dynamic, continuous oversight. Overcoming this resistance requires strong leadership, clear communication, and a phased approach to implementation.

A roadmap for implementing Least Permissive Trust

To successfully implement Least Permissive Trust in federal agencies and DoD environments, a clear, phased roadmap is essential, as illustrated in Figure 2.

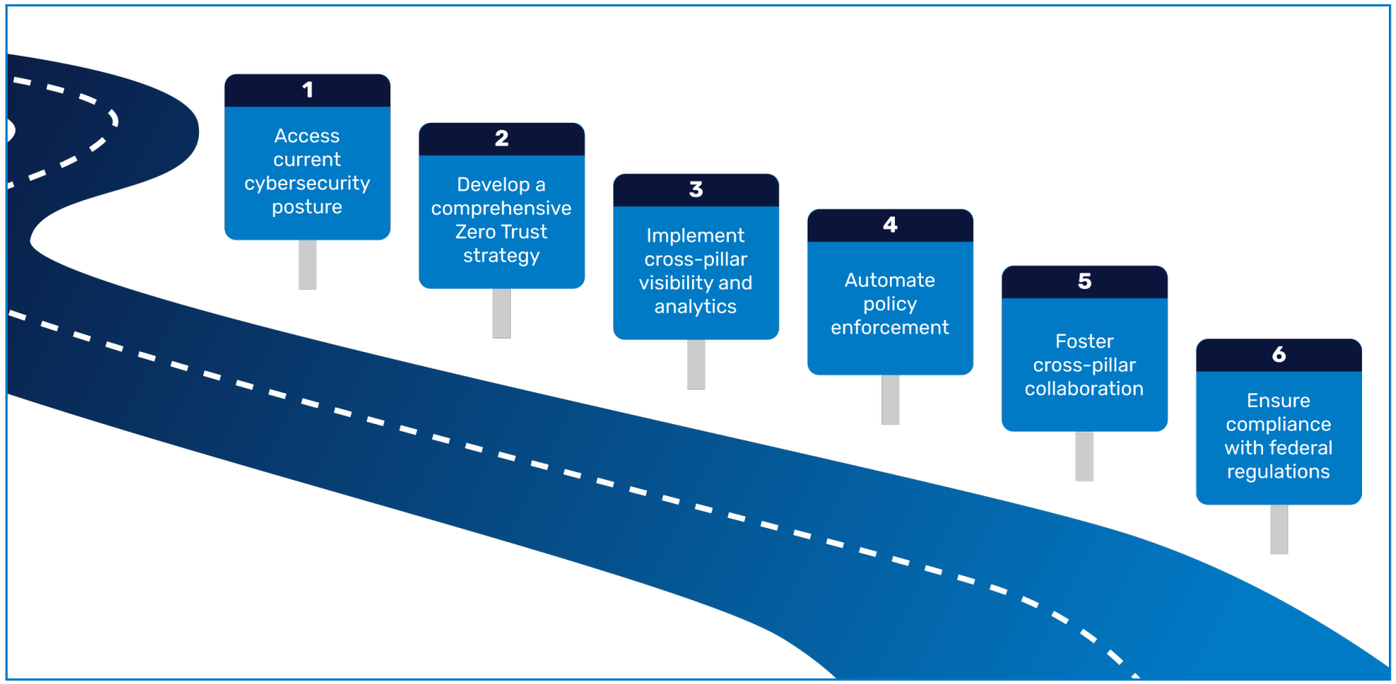


Fig. 2: Roadmap to implementing Least Permissive Trust in federal environments

The following steps outline a comprehensive approach to achieving this goal:

1 Assess current cybersecurity posture

Before embarking on the journey toward Least Permissive Trust, federal agencies should conduct a thorough **assessment of their existing cybersecurity posture**. This includes:

- **Inventorying all applications, devices, and users:** Understanding what assets are in play is the first step toward securing them.
- **Assessing current access controls:** Are users and devices granted more access than they need? Are access controls static or dynamically adjusted based on context and behavior?
- **Identifying gaps in cross-pillar integration:** Where are silos creating security blind spots? How well are identity, network, application, and data security integrated?

2 Develop a comprehensive Zero Trust strategy

Based on the results of the assessment, agencies should develop a Zero Trust strategy that serves as a foundation for implementing Least Permissive Trust. This strategy should focus on:

- **Strengthening identity and access management:** Implementing robust ICAM solutions is key to ensuring that users are authenticated and authorized in real time.
- **Securing application access:** Solutions like **Enterprise Application Access** can enforce application-specific access controls, ensuring that users can only access the applications they need.
- **Segmenting the network:** Use **Akamai Guardicore Segmentation's microsegmentation** capabilities to control east-west traffic within the network, preventing lateral movement and isolating threats in the event of a breach.

3 Implement cross-pillar visibility and analytics

Visibility is a crucial component of Least Permissive Trust, as it allows agencies to monitor user behavior, application traffic, and network activity in real time. By implementing **cross-pillar visibility** solutions, such as those provided by Akamai, agencies can gain a unified view of their entire security environment, allowing them to detect threats faster and respond more effectively. For example:

- **Akamai's ICAM solutions** ensure that agencies have visibility into user identities and access patterns, enabling dynamic adjustments to access controls based on real-time risk assessments.
- **Enterprise Application Access** provides visibility into application access, ensuring that users are interacting with applications as expected and that any anomalous behavior is flagged immediately.
- **Akamai Guardicore Segmentation** offers deep visibility into network traffic between segmented workloads, allowing agencies to detect and isolate suspicious activity.

4 Automate policy enforcement

Manually enforcing security policies across a complex federal environment is impractical and prone to errors. Automation is key to ensuring that Least Permissive Trust principles are enforced consistently and dynamically across all pillars. Akamai's solutions offer **automated policy enforcement**, ensuring that access permissions, network segmentation, and application controls are adjusted in real time based on changing threat conditions.

For example, **Akamai Guardicore Segmentation's automated microsegmentation** can dynamically adjust network policies to isolate compromised segments of the network, while **Enterprise Application Access** can automate the process of revoking or granting access to applications based on real-time identity verification.

5 Foster cross-pillar collaboration

Breaking down silos within security operations is essential for implementing Least Permissive Trust. Federal agencies should focus on fostering **cross-pillar collaboration** between their identity, network, application, and data security teams. This includes:

- **Establishing shared goals and metrics:** Ensure that all teams are working toward the same objective — minimizing risk through dynamic, least-permissive access controls.
- **Streamlining communication and workflows:** Security events detected in one pillar (e.g., a compromised identity) should trigger actions in other pillars (e.g., revoking application access or isolating network segments).

This level of integration ensures that security policies are **enforced consistently across the entire organization**, reducing the risk of miscommunication or gaps in policy enforcement.

6 Ensure compliance with federal regulations

As federal agencies implement Least Permissive Trust, they must ensure that their security strategy aligns with federal regulations, such as those outlined in **Executive Order 14028** and **NIST Special Publication 800-207**. Akamai's solutions are designed to help agencies achieve compliance with these mandates while also enabling real-time policy enforcement and dynamic access controls. For example:

- **Akamai's ICAM solutions** help agencies comply with identity and access management requirements by ensuring that all users are authenticated and authorized using phishing-resistant multi-factor authentication (MFA) and context-based access controls.
- **Akamai Guardicore Segmentation** ensures that network segmentation policies align with federal standards for controlling lateral movement and protecting sensitive data.

By aligning their security strategy with federal mandates, agencies can ensure that they are meeting compliance requirements while also reducing their overall security risk.

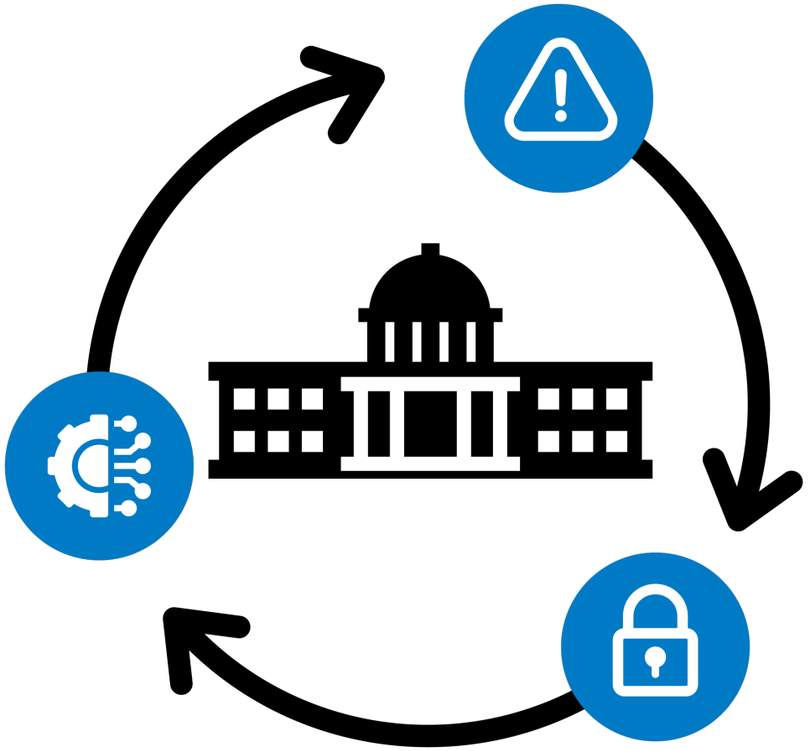
Long-term strategies for resilience and flexibility

Implementing Least Permissive Trust is not a one-time event but an ongoing process that requires continuous improvement and adaptation. Federal agencies should adopt long-term strategies to ensure that their security architecture remains resilient and flexible in the face of evolving cyberthreats.

1 Continuous monitoring and threat intelligence

Federal agencies must adopt a proactive approach to cybersecurity by implementing **continuous monitoring** and integrating **threat intelligence** into their security operations. Akamai's solutions provide real-time analytics and threat detection capabilities that allow agencies to stay ahead of emerging threats and adapt their security posture accordingly. For example:

- **Enterprise Application Access** continuously monitors user interactions with applications, ensuring that any suspicious behavior triggers immediate actions, such as reauthentication or access revocation.
- **Akamai Guardicore Segmentation** provides ongoing network monitoring and segmentation enforcement, ensuring that suspicious traffic is automatically blocked or isolated before it can cause significant harm.



2 Embrace emerging technologies

As cyberthreats continue to evolve, federal agencies should embrace **emerging technologies**, such as **artificial intelligence (AI)** and **machine learning (ML)**, to enhance their cybersecurity capabilities. These technologies can be integrated into Akamai's solutions to improve threat detection, automate responses to suspicious activity, and enhance the overall effectiveness of Least Permissive Trust. For example:

- AI-driven behavioral analytics can be used to detect subtle anomalies in user behavior or network traffic, allowing security teams to respond more quickly to potential threats.
- ML algorithms can help automate the process of adjusting access permissions based on real-time risk assessments, reducing the burden on security teams and improving the overall speed and accuracy of policy enforcement.

3 Foster a security-first culture

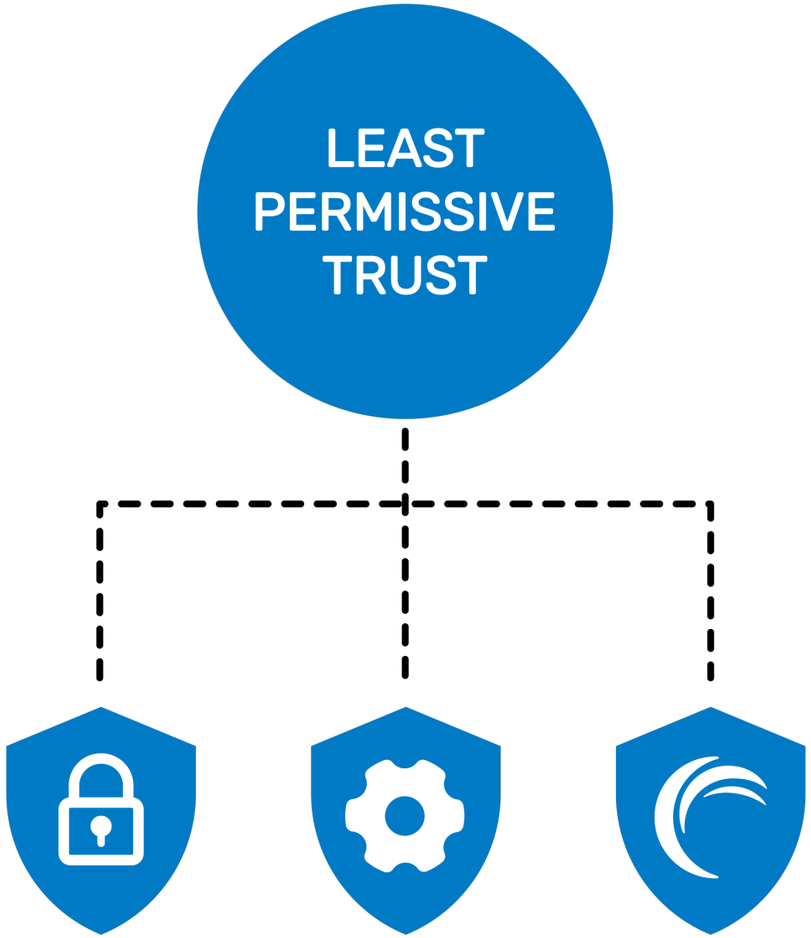
Finally, federal agencies must work to foster a **security-first culture** throughout their organizations. This includes providing regular training for employees on the importance of cybersecurity, promoting the adoption of least-permissive practices, and ensuring that all employees understand their role in protecting the organization from cyberthreats.

Strong leadership and clear communication are essential for overcoming resistance to change and ensuring that all teams are aligned in their efforts to implement Least Permissive Trust.

Achieving cybersecurity through Least Permissive Trust

The implementation of Least Permissive Trust is not just a cybersecurity initiative — it is a strategic shift in how federal agencies and the DoD approach securing their most sensitive systems and data. By adopting a dynamic, integrated approach that continuously adjusts access permissions based on real-time risk assessments, federal agencies can achieve greater resilience, reduce their attack surface, and ensure that their security architecture evolves alongside emerging threats.

Akamai's **ICAM solutions**, **Enterprise Application Access**, and **Akamai Guardicore Segmentation** provide the tools necessary to implement Least Permissive Trust across all pillars, from identity management and application security to network segmentation and data protection. By following this roadmap, federal agencies can meet the mandates of Executive Order 14028 while building a more agile, flexible, and secure infrastructure that will support mission-critical operations for years to come.



What's next?

The journey toward Least Permissive Trust may be challenging, but it is essential for safeguarding national security, protecting sensitive data, and ensuring that federal systems remain resilient in the face of increasingly sophisticated cyberthreats. To learn more about how Akamai can help your organization implement a Least Permissive Trust strategy, contact an Akamai expert today.