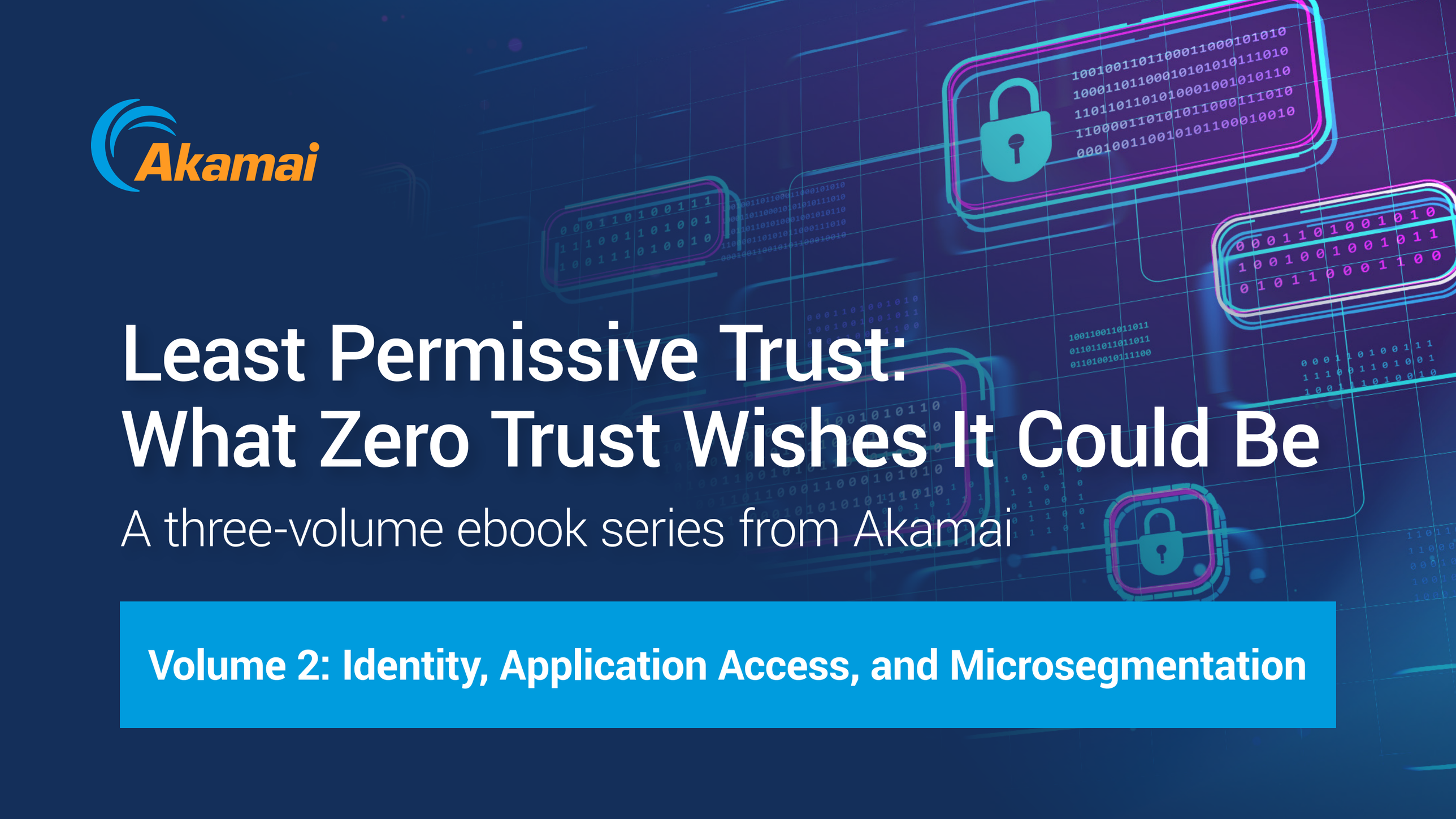


Least Permissive Trust: What Zero Trust Wishes It Could Be

A three-volume ebook series from Akamai

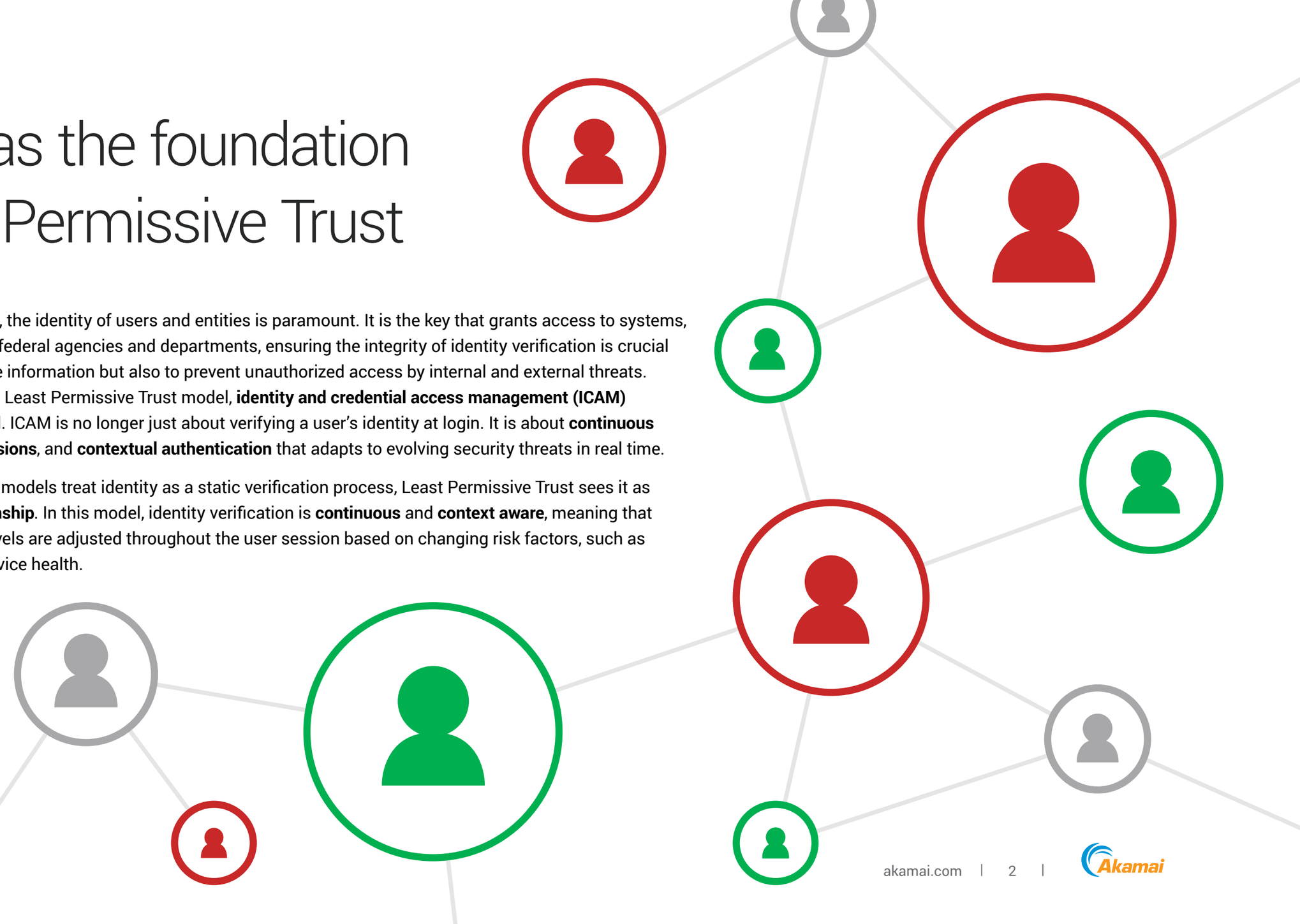
Volume 2: Identity, Application Access, and Microsegmentation

In Volume 1 of this ebook series, the concept of **Least Permissive Trust** was introduced as an evolutionary extension of the Cybersecurity and Infrastructure Security Agency's (CISA's) **Zero Trust Architecture**. In Volume 2, we continue this strategy discussion to include the important concepts of identity management, application access, and microsegmentation for federal agencies and departments, including the Department of Defense (DoD).

Identity as the foundation of Least Permissive Trust

In any security architecture, the identity of users and entities is paramount. It is the key that grants access to systems, applications, and data. For federal agencies and departments, ensuring the integrity of identity verification is crucial not only to protect sensitive information but also to prevent unauthorized access by internal and external threats. As agencies move toward a Least Permissive Trust model, **identity and credential access management (ICAM)** becomes even more critical. ICAM is no longer just about verifying a user's identity at login. It is about **continuous validation**, **dynamic permissions**, and **contextual authentication** that adapts to evolving security threats in real time.

While traditional Zero Trust models treat identity as a static verification process, Least Permissive Trust sees it as a **dynamic**, **ongoing relationship**. In this model, identity verification is **continuous** and **context aware**, meaning that permissions and access levels are adjusted throughout the user session based on changing risk factors, such as behavioral anomalies or device health.



ICAM in traditional Zero Trust models

Under the traditional Zero Trust framework, identity management ensures that each user or entity is authenticated before access is granted. This typically involves multi-factor authentication (MFA), where users must provide multiple forms of verification (e.g., a password and a security token) before they can log in to a system. However, while MFA strengthens initial authentication, it often fails to account for **contextual risks** that may arise during the session itself. Once a user is authenticated, they are often given broad, persistent access to systems and data without any further scrutiny.

This approach creates several challenges:

Overprovisioning of access

Users are often granted access to resources they do not need, increasing the risk of data leaks or malicious activity.

Stale credentials

Users may retain access to sensitive systems even after their roles change, leading to unnecessary exposure.

Static trust models

Once a user is authenticated, trust is often assumed for the duration of the session, even if the user's behavior or device health deteriorates over time.

These challenges are particularly concerning in federal environments, where the stakes are high and the consequences of unauthorized access can be severe. Traditional identity management strategies need to evolve toward more **adaptive**, **dynamic models** that continuously assess trust throughout the session.

The dynamic nature of identity in Least Permissive Trust

Least Permissive Trust builds on the “never trust, always verify” principle by **minimizing trust at every step of the user’s journey**. Access decisions are not made just once at login but are continuously reassessed based on multiple factors, as illustrated in Figure 1.

ICAM becomes the **linchpin of Least Permissive Trust**. It is the system through which dynamic access controls are enforced, ensuring that users only receive the **minimum level of access necessary** to perform their tasks at any given moment.

Fig. 1: With Least Permissive Trust, access decisions are continuously reassessed

Akamai's ICAM solutions for dynamic identity management

Akamai's ICAM solutions are designed to provide the **continuous, adaptive identity management** that is essential for implementing Least Permissive Trust. Akamai's approach goes beyond static identity verification, offering real-time, risk-based identity management that adjusts permissions based on contextual data.

1 Phishing-resistant MFA

Akamai's ICAM solutions enhance MFA, a staple of Zero Trust, to **phishing-resistant MFA**. This form of MFA ensures that even if an attacker compromises one authentication factor (e.g., a password), they cannot easily bypass additional layers of security. Akamai supports **FIDO2-compliant MFA**, which uses **public key cryptography** to secure the authentication process.

Phishing-resistant MFA is continuously applied. For example, if a user successfully logs in but then displays suspicious behavior (such as logging in from an unfamiliar device or network), Akamai's system can trigger additional authentication challenges before granting continued access to sensitive applications or data.

2 Context-based access controls

Akamai's ICAM solutions integrate **contextual authentication**, meaning that identity verification is based not just on who the user is but also on **where they are**, **what device they are using**, and **how they are behaving**. This ensures that access is granted in the most restrictive manner possible.

For example, a user accessing systems from a secure, managed device within the office might be granted more privileges than the same user accessing the system from a personal device over a public network. These contextual controls are dynamically enforced throughout the session, continuously adjusting access levels based on real-time risk assessments.

3 Role-based vs. risk-based access

Traditional identity management models often rely on **role-based access control**, where users are granted permissions based on their role. While this model provides a solid foundation for access management, it can lead to **overprovisioning**, where users have more access than they need because of their broad role definitions.

Akamai's ICAM solutions introduce **risk-based access control** as an enhancement to traditional role-based models. In this approach, access is not only defined by the user's role but also adjusted dynamically based on **real-time risk factors**. This ensures that users only receive the permissions they need, when they need them, and that these permissions are revoked or reduced when the system detects heightened risks.

For example, a systems administrator may have broad access to manage infrastructure, but if the system detects that the administrator is logging in from an unusual location or using a suspicious device, access can be revalidated in real time.

4 Just-in-time and just-enough access

A key feature of Akamai's ICAM solutions is the ability to implement **just-in-time (JIT)** and **just-enough access (JEA)** policies that ensure users are only granted access to resources for the exact duration they need and only to the specific resources required to complete their tasks. For example, an employee needing access to a specific application for a temporary project would only receive access for the time required to complete the task. Once finished, the permissions are automatically revoked, reducing the risk of unauthorized access or privilege escalation.

5 Federal identity assurance and authentication standards compliance

Akamai's ICAM solutions are specifically designed to meet the **rigorous identity and authentication requirements** of federal agencies, aligning with NIST Special Publication 800-63 standards for identity assurance levels (IALs) and authenticator assurance levels (AALs).

- **IAL3/AAL3 support:** Akamai's platform fully supports the highest levels of identity proofing and authentication assurance required for access to highly sensitive government systems and classified information. This ensures federal agencies can implement Least Permissive Trust while maintaining strict compliance with federal standards.
- **Seamless CAC/PIV integration:** Akamai provides native support for common access card (CAC) and personal identity verification (PIV) credentials, the cornerstone of federal identity management. Unlike traditional implementations that simply verify the presence of a certificate, Akamai's approach:
  - Continuously validates certificate status against certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) responders
  - Implements certificate path validation to ensure the trust chain remains intact throughout the session
  - Correlates certificate information with other contextual signals to prevent credential misuse
  - Supports derived credentials for mobile device authentication while maintaining the same assurance levels
- **Adaptive authentication orchestration:** Akamai's platform dynamically adjusts authentication requirements based on risk signals and resource sensitivity. For example, when accessing routine applications, a user with a valid CAC/PIV credential might proceed without additional challenges. However, when accessing more sensitive resources or when risk indicators are present, the system can automatically escalate to require additional verification such as biometric confirmation or out-of-band approval.
- **Credential binding and nonrepudiation:** Akamai's solutions create cryptographic bindings between authenticated sessions, device certificates, and CAC/PIV credentials, establishing clear audit trails that support nonrepudiation requirements for highly regulated federal operations. This ensures that all actions taken within the system can be irrefutably tied to the authenticated identity.

Preventing privilege escalation with Least Permissive Trust

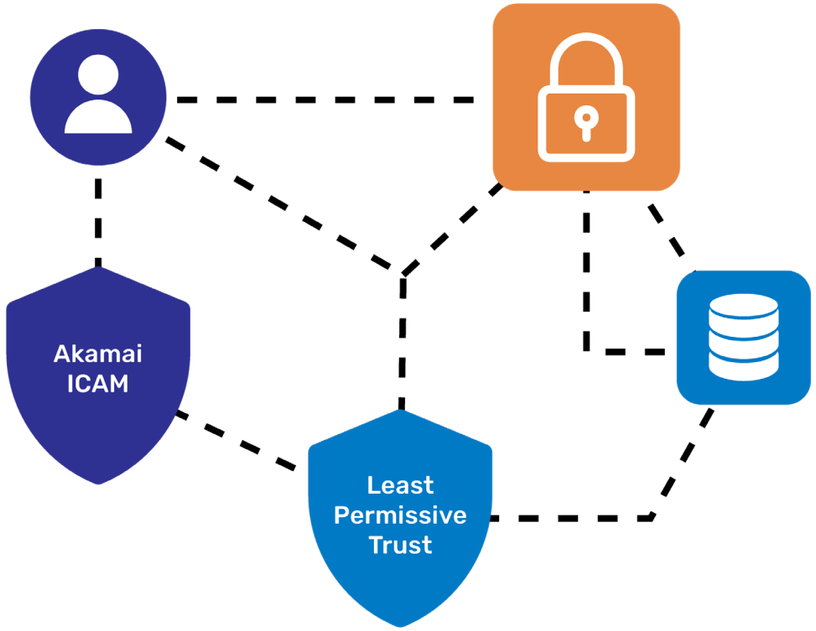
Privilege escalation remains one of the most significant threats in modern cybersecurity. Attackers often exploit overprovisioned user accounts or vulnerabilities in identity systems to gain unauthorized access to critical systems. Least Permissive Trust, as enabled by Akamai's ICAM solutions, is designed to prevent these types of attacks by ensuring permissions are kept to a minimum. Akamai's approach includes:

- **Continuous monitoring for anomalous behavior:** Akamai's solutions continuously monitor user activity, looking for signs of privilege escalation or suspicious behavior. If an anomaly is detected, the system can automatically downgrade the user's access permissions or trigger a reauthentication process.
- **Granular access controls:** Instead of granting broad access based on a user's role, Akamai's system applies granular controls that limit access to the specific resources a user needs, minimizing the risk of privilege escalation.

Integrating ICAM with other Zero Trust pillars

One of the strengths of Akamai's ICAM solutions is the ability to integrate seamlessly with other Zero Trust pillars, such as **network security**, **application access**, and **data protection**. By linking identity management with other security layers, Akamai enables a holistic Least Permissive Trust model where all components work together to minimize risk. For example:

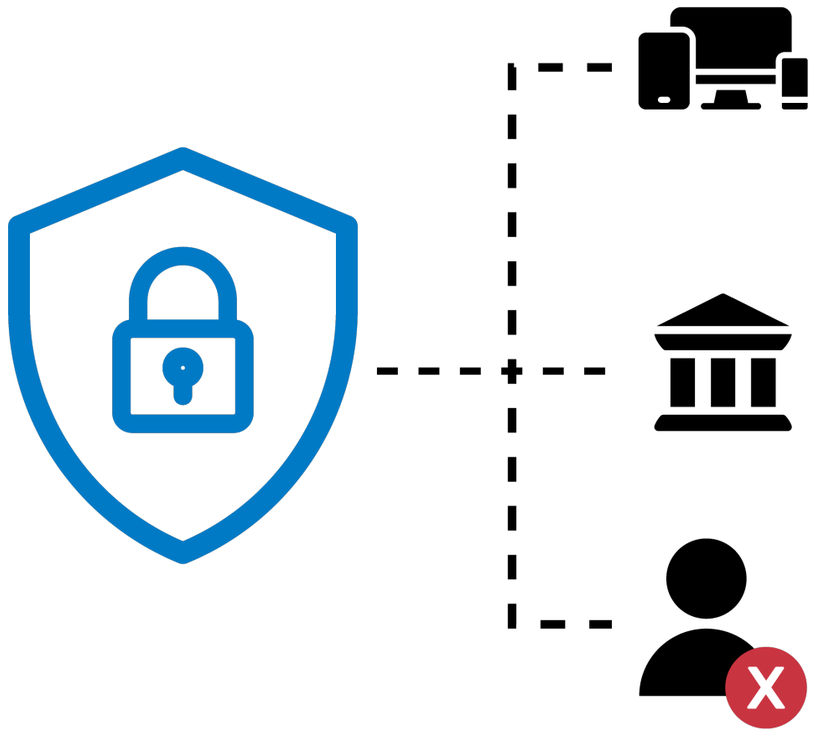
- **Network security:** Akamai's ICAM solutions work in conjunction with network segmentation and monitoring tools to ensure that even if a user is authenticated, their network traffic is continuously monitored for signs of compromise. If suspicious activity is detected, the user's access can be immediately limited or revoked.
- **Application access:** Akamai **Enterprise Application Access** integrates with ICAM to dynamically adjust user permissions within applications based on their identity, device health, and behavioral context.



Enabling Least Permissive Trust with Enterprise Application Access

As federal organizations increasingly rely on remote workforces and cloud-based applications, securing access to applications has become one of the most critical components of their cybersecurity strategy. Traditionally, securing access meant relying on virtual private networks (VPNs) and perimeter-based defenses to keep unauthorized users out. Today, this approach is insufficient. With employees accessing applications from various locations, devices, and networks, it's essential to adopt a Least Permissive Trust model for application access.

Access to applications should be restricted to the **absolute minimum necessary** at all times, with permissions being dynamically adjusted based on real-time risk assessments. **Enterprise Application Access** plays a pivotal role in enabling Least Permissive Trust, offering a Zero Trust solution that goes beyond traditional perimeter security by continuously verifying users and devices, ensuring minimal exposure of sensitive applications, and dynamically adjusting access permissions based on context and behavior.



From VPNs to Zero Trust access

For decades, VPNs were the primary method for providing employees with secure remote access. However, VPNs have several inherent limitations:

Broad access

VPNs often grant access to entire networks, unnecessarily exposing applications to users who only need access to a few systems.

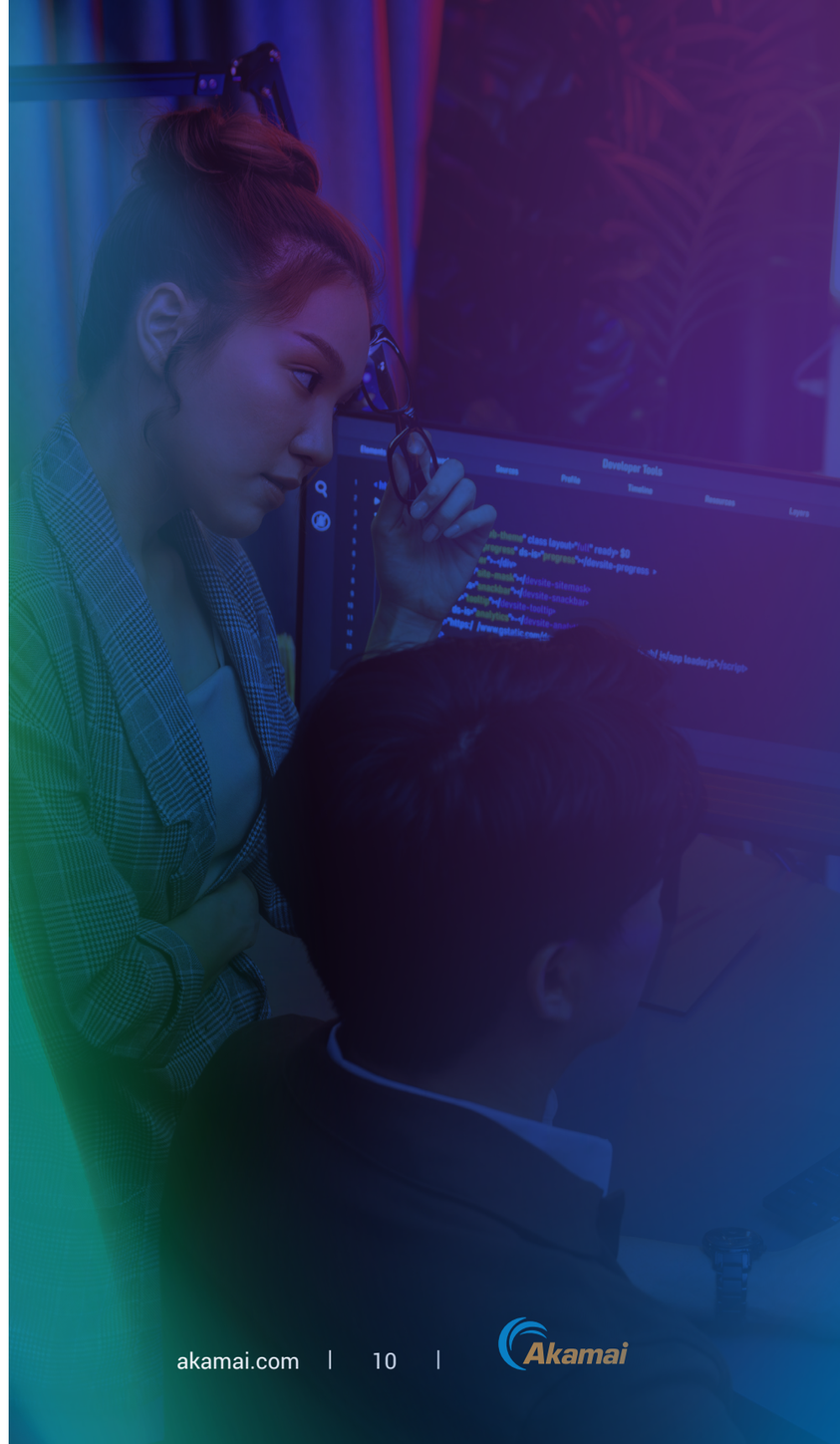
Lack of granular control

VPNs lack the ability to dynamically control access at the application level based on real-time data such as user behavior or device health.

Overreliance on perimeter defenses

VPNs operate on the assumption that if a user can authenticate and access the network, they can be trusted. However, in a Zero Trust world, every access attempt must be validated continuously, regardless of the user's location.

Zero Trust Network Access (ZTNA) addresses these limitations by shifting the focus from perimeter-based security to **application-specific access**. With ZTNA, access is granted on a **per-application basis**, and permissions are continuously monitored and adjusted to ensure that users only interact with the specific applications they need, when they need them. However, even ZTNA must evolve to implement Least Permissive Trust.



The role of Enterprise Application Access

Enterprise Application Access is a cloud native ZTNA solution designed to provide **secure**, **least permissive access** to internal applications, whether they are hosted on-premises or in the cloud. Enterprise Application Access ensures that users can access only the specific applications they need while continuously validating their identity, device, and behavioral context. Unlike traditional access solutions, Enterprise Application Access does not expose applications to the public internet, significantly reducing the attack surface and preventing unauthorized users from even seeing that the applications exist.

Key features include:

Application-specific access

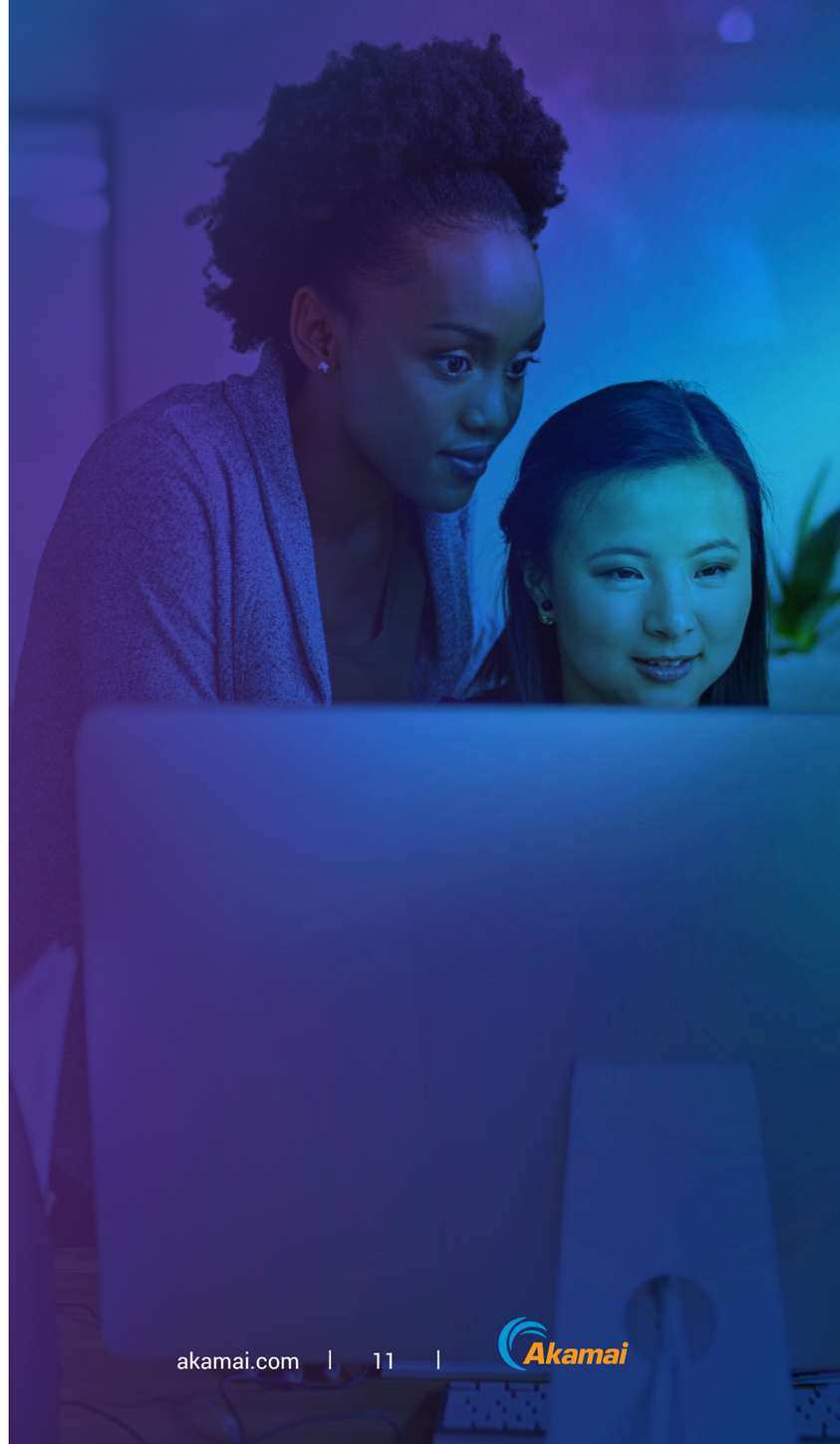
Users are granted access only to the specific applications they need, and access is monitored and adjusted continuously based on risk.

No network exposure

Applications are not exposed to the public internet. Enterprise Application Access uses a reverse proxy architecture to create a secure tunnel between the user and the application, without exposing IP addresses or endpoints to potential attackers.

Continuous risk-based access control

Enterprise Application Access integrates with Akamai's identity management solutions to continuously assess user behavior, device health, and contextual factors. Access permissions are dynamically adjusted based on this real-time risk assessment, ensuring that users maintain only the minimum level of access required.



Achieving Least Permissive Trust with Enterprise Application Access

Enterprise Application Access enables Least Permissive Trust by integrating several key capabilities that ensure minimal permissions and dynamic adjustments.

1 Dynamic access based on user behavior and context

In a Least Permissive Trust model, access to applications is not static. Instead, it adjusts continuously based on the user's **behavior**, **location**, **and device health**. For example:

- **User behavior:** If a user exhibits unusual behavior — such as accessing the application from an unfamiliar location or attempting actions outside of their normal behavior patterns — Enterprise Application Access can immediately restrict or revoke access until further verification is completed.
- **Device health:** Enterprise Application Access can assess the health of the device attempting to access an application. If the device is determined to be compromised (e.g., running outdated or vulnerable software), the user's access to the application can be limited or denied.

By continuously assessing and validating these factors, Enterprise Application Access ensures that users are granted access only when conditions are deemed secure. This is particularly crucial in federal environments, where users may handle classified or sensitive information.

2 Per-application granular permissions

With Least Permissive Trust, users should only have **access to the exact resources they need** at any given time. With Enterprise Application Access, this is enforced through **per-application access controls**. Unlike traditional VPNs or broad network access controls, Enterprise Application Access ensures that users can only access specific applications, not the underlying infrastructure or other systems on the network.

For example, a contractor working on a specific project for a federal agency may be granted access to a single application, with permissions dynamically limited based on the project's needs. Other applications and systems, even within the same network, remain completely inaccessible. This granular control prevents unauthorized lateral movement within the network, significantly reducing the potential attack surface.

3 Zero Trust protection against lateral movement

A critical feature of Least Permissive Trust is its ability to **prevent lateral movement** within a network. Attackers often exploit broad access permissions to move laterally within a compromised network, gaining access to sensitive systems and data over time. Enterprise Application Access addresses this threat by ensuring that users can only access the specific applications to which they've been assigned, without gaining visibility or access to other systems.

Enterprise Application Access uses a **reverse proxy architecture** where users cannot connect directly to applications — they can only connect through the secure proxy, which acts as an intermediary. While Enterprise Application Access helps mitigate the risk of lateral movement by validating each access request against dynamic policies, it is important to note that additional measures, such as microsegmentation, are necessary to fully control and limit lateral movement within the network.

4 Integration with ICAM

Enterprise Application Access seamlessly integrates with identity management systems, such as Akamai's ICAM solutions, to ensure that authentication is not a one-time event but an ongoing process. Users are continuously authenticated based on their identity, behavior, and device health throughout their entire session. For example, if a user's risk profile changes mid-session — such as if they attempt to access an application from an unauthorized network — Enterprise Application Access can dynamically adjust or revoke access until further authentication is completed. This ensures that permissions are continuously aligned with the real-time security posture of the user and device.

Improving security and user experience simultaneously

One of the primary concerns for federal agencies is balancing **security** with **usability**. While Least Permissive Trust enforces stricter access controls, Enterprise Application Access is designed to maintain a positive user experience by streamlining access and reducing friction:

- **Simplified access:** Users access applications through a single portal, eliminating the need for VPNs, multiple credentials, or complicated network setups.
- **Single sign-on (SSO):** This allows users to authenticate once and gain access to all authorized applications without repeated logins. This simplifies the user experience while maintaining strict access control policies.
- **Cloud-based scalability:** Enterprise Application Access is fully cloud native, meaning it can scale to accommodate the demands of large federal agencies and DoD operations without the need for additional on-premises infrastructure.

By improving both security and user experience, Enterprise Application Access provides federal agencies with a solution that supports their mission-critical operations without compromising on safety or efficiency.

CASE STUDY

Enterprise Application Access implementation in a federal environment

Enterprise Application Access has been successfully deployed in several federal environments, including an agency responsible for managing highly sensitive data across distributed teams. Before adopting Enterprise Application Access, the agency relied on traditional VPNs, which created several challenges:

- **Broad access:** VPNs granted users access to the entire network, exposing applications unnecessarily and increasing the risk of unauthorized access.
- **Complex user experience:** The process of logging into multiple systems through the VPN was cumbersome and created friction for users, leading to frustration and reduced productivity.
- **Limited monitoring:** VPNs provided limited visibility into user behavior once access was granted, making it difficult to identify potential insider threats or compromised devices.

By implementing Enterprise Application Access, the agency was able to:

- **Reduce the attack surface:** Users were granted access only to the applications they needed, and no other network resources were exposed.
- **Enhance user experience:** The SSO and cloud native access portal streamlined the login process, improving user satisfaction while maintaining strong security controls.
- **Increase visibility:** Enterprise Application Access's continuous monitoring capabilities allowed the agency to track user behavior in real time, identifying potential threats and adjusting access dynamically to mitigate risks.

This deployment demonstrated the power of Enterprise Application Access to improve security and enhance operational efficiency, enabling the agency to meet its mission-critical objectives without compromising on safety.

Microsegmentation with Akamai Guardicore Segmentation to secure federal networks

In today's complex cybersecurity landscape, network security remains one of the most critical aspects of protecting sensitive federal data, applications, and systems. Traditional approaches to network security, which focused heavily on perimeter defenses such as firewalls and VPNs, are no longer sufficient. Once attackers breach the perimeter, they often have free rein to move laterally across the network, accessing sensitive resources without significant barriers.

As cyberattacks become more sophisticated, it is essential to **limit the damage** attackers can cause, even if they succeed in breaching one part of the network. This is where **microsegmentation** comes into play. Microsegmentation, as an evolution of network security, offers **fine-grained access control** within the network itself, ensuring that permissions are restricted to the absolute minimum necessary at any given moment and that lateral movement by attackers is curtailed.

Akamai **Guardicore Segmentation** enables microsegmentation in a way that aligns with **Least Permissive Trust**, dynamically adjusting permissions and segmenting network traffic at the most granular level possible.

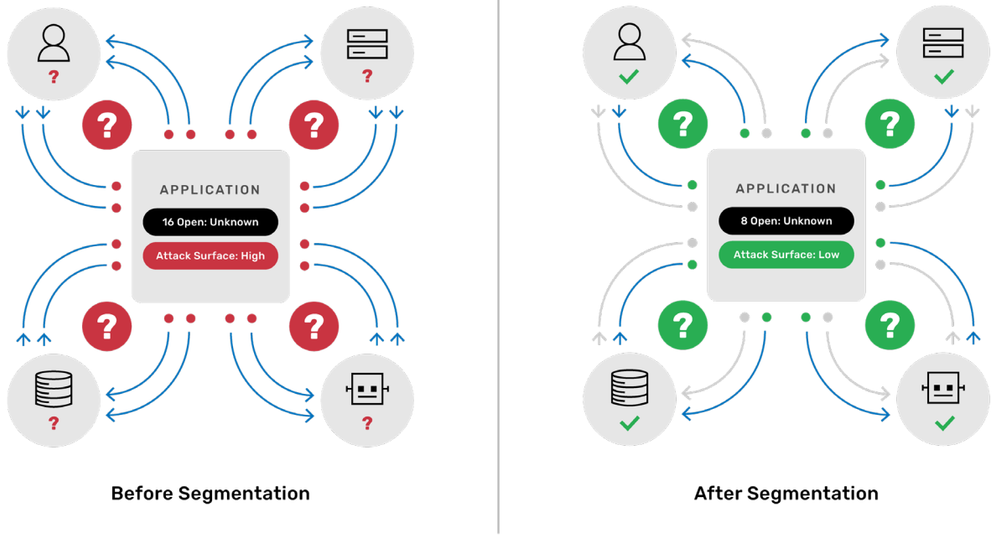
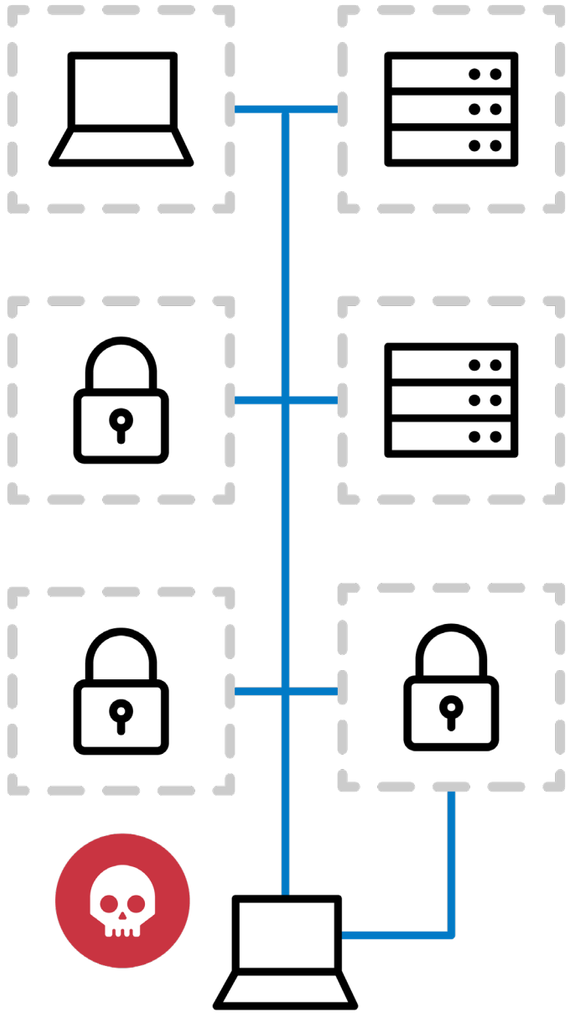


Fig. 2: Before and after segmentation

The role of microsegmentation in Zero Trust

In traditional security models, networks are often divided into broad segments using **network-based firewalls**. While this provides a level of security, it lacks the granularity required to fully protect modern, distributed environments. Network-based segmentation typically results in **overprovisioning**, where users and applications have access to more resources than necessary. This creates opportunities for lateral movement — when attackers compromise one part of the network, they can move across to more sensitive areas with little resistance.

Microsegmentation addresses this challenge by introducing **fine-grained control over east-west traffic** (i.e., traffic within the network). In a microsegmented environment, each application, workload, or even service is isolated from others, and access is restricted based on specific policies. This ensures that users, devices, and applications can only communicate with the resources they are explicitly authorized to access. By implementing **identity-based**, **application-aware segmentation**, microsegmentation limits the potential damage from cyberattacks, reduces the attack surface, and enforces the principle of **Least Permissive Trust**.



How Akamai Guardicore Segmentation enables microsegmentation

Akamai **Guardicore Segmentation** is a leading microsegmentation solution designed to help organizations, especially federal agencies and the DoD, achieve Least Permissive Trust by securing traffic within their networks. It offers a **software-defined approach** to segmentation, making it highly adaptable to both on-premises and cloud environments.

1 Granular segmentation of workloads and applications

Unlike traditional network segmentation, which segments traffic at a network level, Akamai Guardicore Segmentation operates more granularly at the **application and workload levels**. This means that access control policies are applied to specific applications, services, or processes, rather than broad network segments.

For example, a federal agency using Akamai Guardicore Segmentation could segment its network so that an HR application can only communicate with the HR database and no other systems on the network. Even if an attacker gains access to the application, they will be unable to move laterally to other systems or access data outside the HR environment. This **ringfencing** of applications prevents attacks from spreading and isolates threats within individual segments.

2 Identity-based microsegmentation

Akamai Guardicore Segmentation supports **identity-based segmentation**, meaning that segmentation decisions are made not just based on IP addresses or network locations but also based on **user and device identity**. This aligns with the principles of Least Permissive Trust by ensuring that **only trusted users and devices** can interact with specific resources.

For example, a federal agency might have multiple internal services that are accessible to employees, contractors, and third-party partners. With Akamai Guardicore Segmentation, access can be restricted based on each user's role, ensuring that contractors and third-party partners can only access the resources they need while government employees have broader permissions. This reduces the risk of **unauthorized access** and ensures that permissions are granted dynamically based on **real-time identity verification**.

3 Dynamic policy enforcement

Akamai Guardicore Segmentation allows for **dynamic policy enforcement**, where access control policies are automatically adjusted based on real-time factors such as **user behavior**, **device health**, **and network activity**. This real-time adaptability ensures that access permissions are kept to the minimum necessary at all times.

For instance, if Akamai Guardicore Segmentation detects suspicious activity, such as an unusual volume of data transfers between two segmented systems, it can automatically enforce tighter restrictions, block traffic, or trigger alerts for security teams. This dynamic enforcement ensures that security policies are not static but are continuously adapting to emerging threats.

4 Zero Trust segmentation for hybrid and multicloud environments

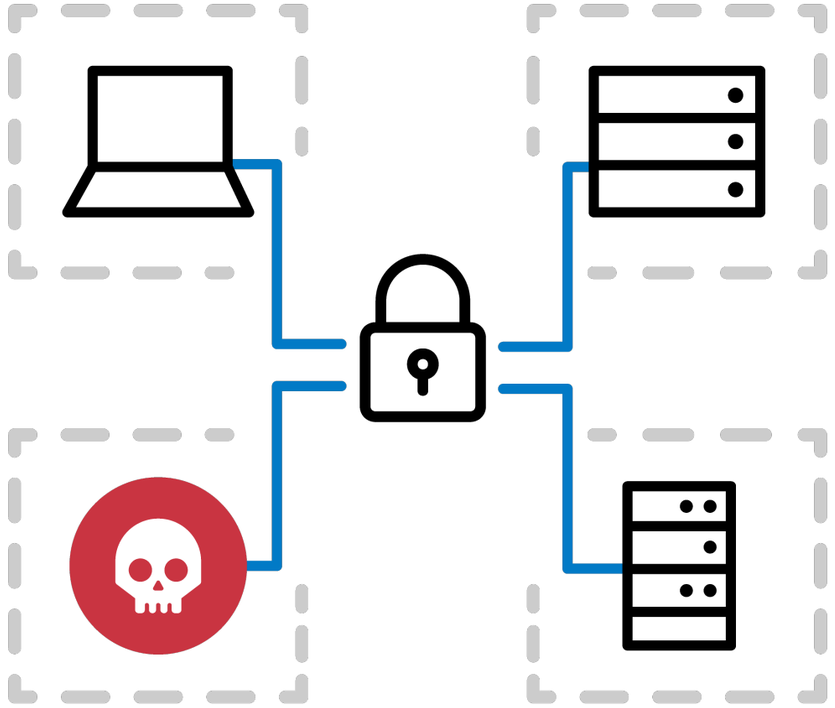
As federal agencies increasingly adopt **multicloud and hybrid environments**, ensuring consistent security across these environments becomes more challenging. Akamai Guardicore Segmentation is designed to provide **cross-environment segmentation**, ensuring that security policies are applied consistently, whether workloads are running on-premises, in the cloud, or in hybrid deployments.

This is particularly important for federal agencies, which may operate in a mix of legacy systems, private clouds, and public cloud environments. Akamai Guardicore Segmentation allows agencies to implement microsegmentation across all environments, ensuring that **east-west traffic** between cloud workloads is as tightly controlled as on-premises traffic. Least Permissive Trust principles are applied across the entire infrastructure, no matter where data or applications reside.

Preventing lateral movement in government networks

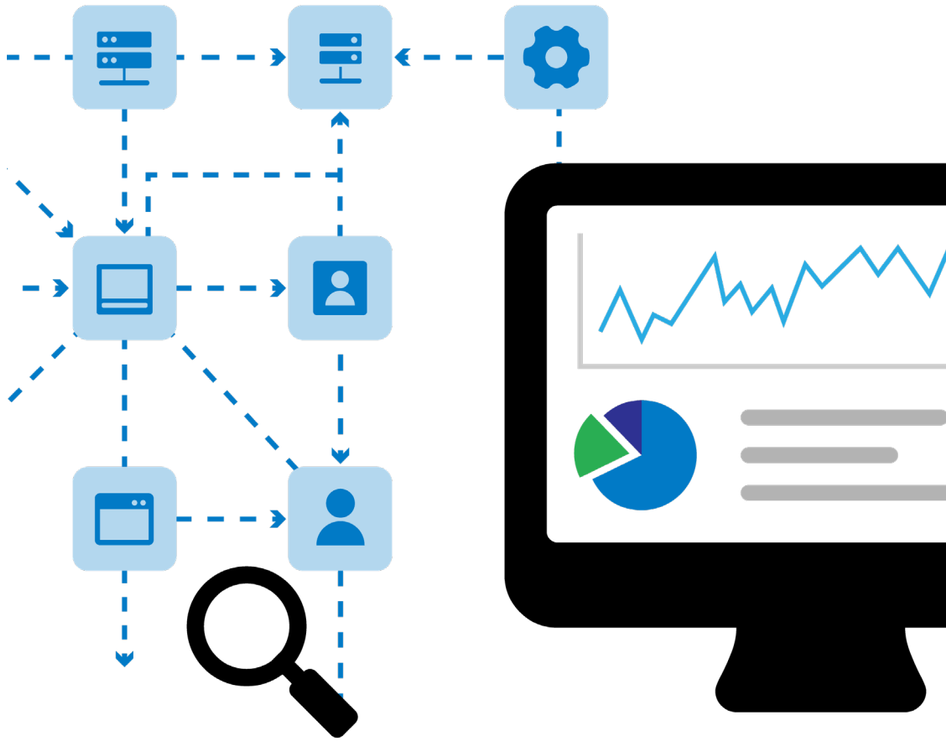
Lateral movement is one of the most common tactics attackers use once they breach a network. By moving laterally from one system to another, attackers can escalate privileges, access sensitive data, and exfiltrate valuable information. When classified information and national security are at stake, preventing lateral movement is essential. Akamai Guardicore Segmentation's microsegmentation capabilities make lateral movement **extremely difficult** for attackers:

- **Isolated segments:** Each segment within the network is isolated, meaning that even if an attacker compromises one part of the network, they cannot move freely to other segments.
- **Strict access controls:** Access between segments is restricted to **explicitly authorized traffic**. Even legitimate users can only access the specific resources they are authorized for, reducing the potential for lateral movement through overprovisioned access rights.
- **Real-time monitoring and alerts:** Akamai Guardicore Segmentation continuously monitors traffic between segments and can detect attempts at lateral movement in real time. When an attack is detected, the system can block traffic, isolate the compromised segment, and alert security teams for further investigation.



Visibility and analytics

A critical aspect of any segmentation strategy is **visibility** — understanding what traffic is flowing between workloads, applications, and users. Akamai Guardicore Segmentation provides **deep visibility** into the network, offering detailed analytics on traffic patterns, user behavior, and security events. This visibility is key to implementing and maintaining Least Permissive Trust policies.



1 Visualizing traffic flows

Akamai Guardicore Segmentation's **visualization capabilities** allow federal agencies to see traffic flows between different segments in real time. This provides security teams with a comprehensive view of how applications and users are interacting with one another, making it easier to identify potential vulnerabilities or misconfigurations.

For example, if security teams notice unexpected traffic between a low-security segment and a high-security application, they can quickly investigate and adjust access policies to prevent unauthorized access. This **real-time visibility** is crucial for maintaining the integrity of segmented environments and ensuring that least permissive access is enforced at all times.

2 Behavioral analytics for anomaly detection

Akamai Guardicore Segmentation uses **behavioral analytics** to detect anomalies within the network. By analyzing patterns of communication between applications, workloads, and users, it can identify unusual activity that may indicate a security breach or insider threat. For example, if Akamai Guardicore Segmentation detects that a normally isolated application is suddenly communicating with multiple external systems, this could be a sign of an attack. The system can then alert security teams and automatically adjust segmentation policies to contain the threat. This **proactive detection** helps agencies stay ahead of attackers.

Integration with other security layers

Akamai Guardicore Segmentation integrates seamlessly with other security technologies to provide a comprehensive Least Permissive Trust solution:

- **ICAM:** It can integrate with identity management systems to enforce segmentation policies based on user identity and role. This ensures that segmentation policies are dynamically adjusted based on real-time identity verification, adding an additional layer of security.
- **Enterprise Application Access:** Akamai Guardicore Segmentation works alongside Enterprise Application Access to control access to applications. While Enterprise Application Access ensures that users can only access authorized applications, Akamai Guardicore Segmentation ensures that traffic between those applications is segmented and tightly controlled.
- **Threat intelligence:** It integrates with threat intelligence platforms to stay updated on emerging threats. This enables the system to dynamically adjust segmentation policies in response to new attack vectors or vulnerabilities.

CASE STUDY

Akamai Guardicore Segmentation in a federal environment

One federal agency implemented Akamai Guardicore Segmentation's microsegmentation to protect internal systems from lateral movement attacks. Before this implementation, the agency relied on traditional network-based segmentation, which provided limited granularity and allowed for broad access between different network segments. This would create a significant risk of lateral movement if any part of the network were compromised. With Akamai Guardicore Segmentation, the agency was able to:

- **Implement granular segmentation:** By segmenting workloads at the application level, the agency reduced the risk of lateral movement and ensured that each application could only communicate with the resources it needed.
- **Improve visibility:** Akamai Guardicore Segmentation's visualization tools provided the agency with deep insight into its internal traffic, allowing security teams to identify and mitigate potential threats in real time.
- **Enhance security:** By integrating Akamai Guardicore Segmentation with its existing identity management and access control systems, the agency was able to enforce Least Permissive Trust across its network, ensuring that access was continuously monitored and dynamically adjusted based on real-time risk assessments.

This case demonstrates the power of Akamai Guardicore Segmentation to improve network security, reduce the risk of lateral movement, and ensure that permissions are kept to the minimum necessary at all times.

What's next?

To learn more about how Least Permissive Trust can enhance the security of federal systems, read Volume 3 of this ebook series: **Cross-Pillar Capabilities and Implementation Guidelines**.

Contact Akamai today to learn more about our comprehensive security solutions.