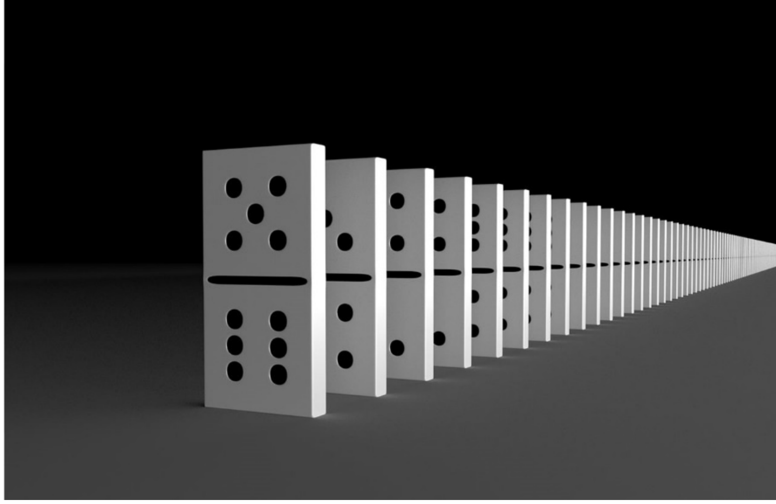


Maximum Resiliency

Eliminating the Cloud Domino Effect

Zero Downtime Access to Mission-Critical SaaS and LoB Apps with Decentralized Identity Assurance

At a Glance

Problem: The Cascading Failure Risk

Centralized 'Big Three' cloud provider Identity and Access Management (IAM) creates a Single Point of Failure (SPOF), causing a cascading "Domino Effect" that blocks access to reliant, mission-critical independent SaaS and LoB apps during cloud provider outages.

Solution: The Foundational Trust Shift

Trustus AAM provides a truly Decentralized Identity plane that operates completely independent of the Mainframe-on-Internet (MOI) provider, ensuring uninterrupted SaaS access and unphishable security.

Key Business Benefit: The Resiliency Benchmark

Maximum Access Resiliency and Zero Downtime for users, even during catastrophic public cloud authentication failures.

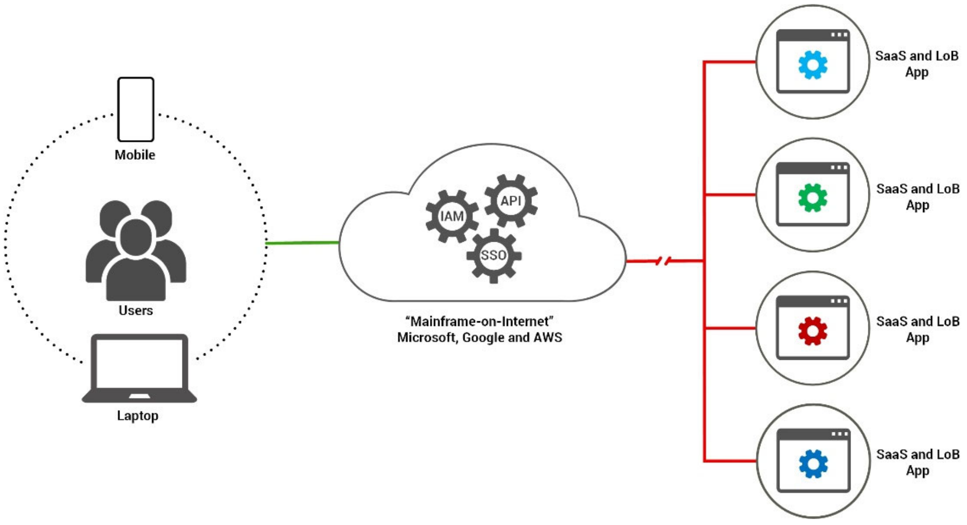
The Challenge: Forced Dependency and the Domino Effect

The modern enterprise is critically reliant on the **Mainframe-on-Internet (MOI)** architecture, primarily built on the "Big Three" (Microsoft, Google, and AWS). This architecture bundles identity and access controls into one mandatory, centralized gateway.

This consolidation creates one single, enormous vulnerability: The Domino Effect.

When a failure occurs within the MOI's central access component, all downstream SaaS and LoB apps are instantly cut off. This exposes a fatal flaw: why should a minor bug in a cloud provider's system block access to vital applications like Salesforce or Workday? This single point of failure demands an architectural reset.

The Cloud Domino Effect (SPOF)



The Trustus AAM Solution: Decentralized Identity

Trustus AAM is a **foundational re-architecture of access control** that inverts the traditional model, decisively ending the forced dependency and single point of failure of the MOI structure. It establishes a separate, **resilient identity plane** that functions entirely independently of the centralized cloud provider.

How Trustus AAM Ensures Uninterrupted Access

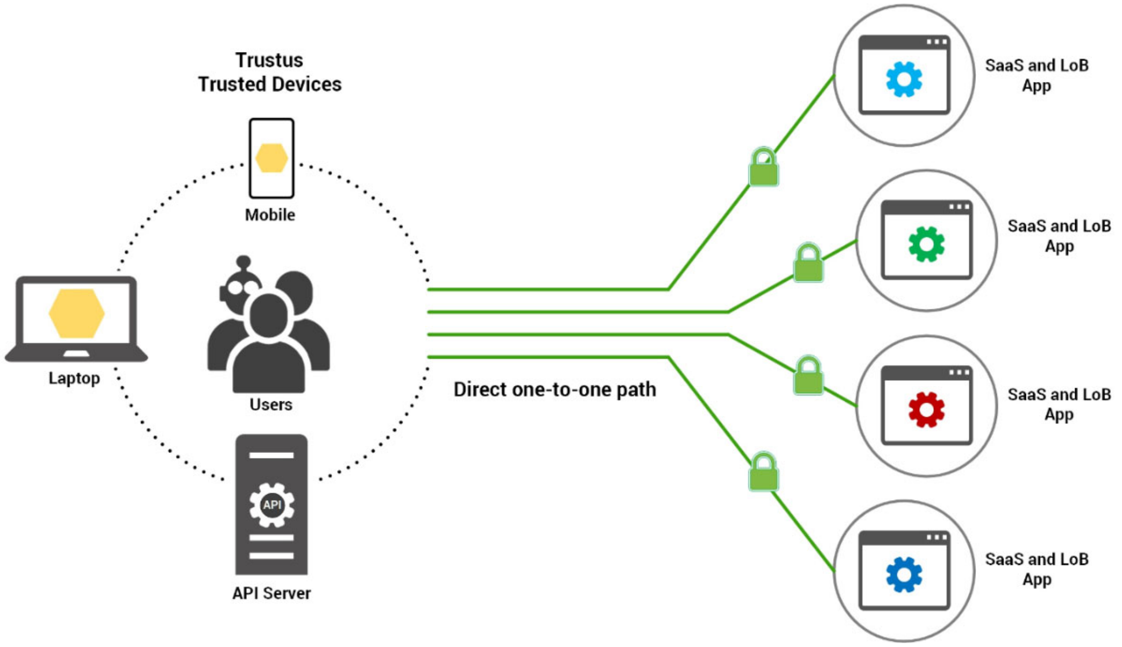
- **Architectural Independence:** Trustus AAM operates in a separate, autonomous domain, and does not rely on the MOI whatsoever to grant secure access, detaching your identity system from the MOI's central access component.
- **Direct (Decentralized) Path:** We establish a unique, highly-encrypted, direct path from the trusted user's device straight to each SaaS and LoB application, bypassing the MOI's authentication layer.
- **Maximum Operational Continuity:** This independent access architecture delivers maximum operational continuity, ensuring your users maintain seamless access and productivity, even during catastrophic public cloud authentication failures.

Key Benefits: Resiliency, Security, and Speed

Trustus AAM Feature	Business Value	Differentiator
Decentralized Access Plane	**Eliminates the Domino Effect.** Users maintain access to applications even during major cloud authentication outages.	**Complete Maximum Uptime** (access) and business continuity regardless of cloud provider status.
Native Application Fidelity	**Pure, Unhindered Functionality.** Preserves the application's native features, ensuring users never experience feature loss or compromised performance due to API proxy mediation.	**Full Native App Experience** with no functional degradation or loss of feature granularity.

Trustus AAM Feature	Business Value	Differentiator
Certificate-Based Authentication (CBA)	**Unphishable Security.** The user's certificate is the secure, cryptographically-secured identity, eliminating token theft and phishing vulnerability.	Superior **Identity Assurance** that exceeds MOI's token-based authentication.
One-Click, Direct Path	**Seamless User Experience.** Access is established instantly and directly, ensuring an unhindered user workflow without logon prompts or redirects.	**Fastest, most resilient** access path in the industry.

Foundational Trust: The Sovereign Access Architecture



Conclusion: Own Your Resilience

The modern enterprise can no longer afford to outsource its critical access controls to a centralized architecture that exposes it to the **Domino Effect**. Recent large-scale outages are not anomalies; they are proof that the Mainframe-on-Internet (MOI) model is fundamentally fragile.

Trustus AAM represents the necessary **Foundational Trust Shift** in this digital era. It replaces systemic dependency with **Architectural Independence**, token vulnerability with **Unphishable Security**, and shared failure with **Complete Maximum Uptime**.

By deploying Trustus AAM, you are not simply buying a new product; you are reclaiming **Sovereign** control over your security posture and ensuring **uninterrupted business continuity** regardless of the cloud provider's status. It is time to implement the new standard—**The Resilience Benchmark**—and architecturally eliminate access failure forever.

Next Steps

It's time to choose access that is independent, resilient, and unphishable.

Contact your Trustus representative today to schedule a technical demonstration.

- **Visit:** https://trustussecurity.com/maximum-resiliency/
- **Email:** Sales@TrustusSecurity.com
- **Connect:** https://www.linkedin.com/company/trustussecurity/

Important Information This solution brief has been prepared by Trustus Technologies Group (Trustus) for general informational purposes only and does not constitute professional advice. All software technologies and content described herein are the exclusive proprietary intellectual property (IP) of Trustus. While Trustus strives for accuracy, we accept no liability for any loss or damage arising from reliance on its contents. Readers are cautioned not to use this information as their own, nor to engineer or reverse-engineer the IP without express written permission. Readers are encouraged to seek expert consultation for specific needs.