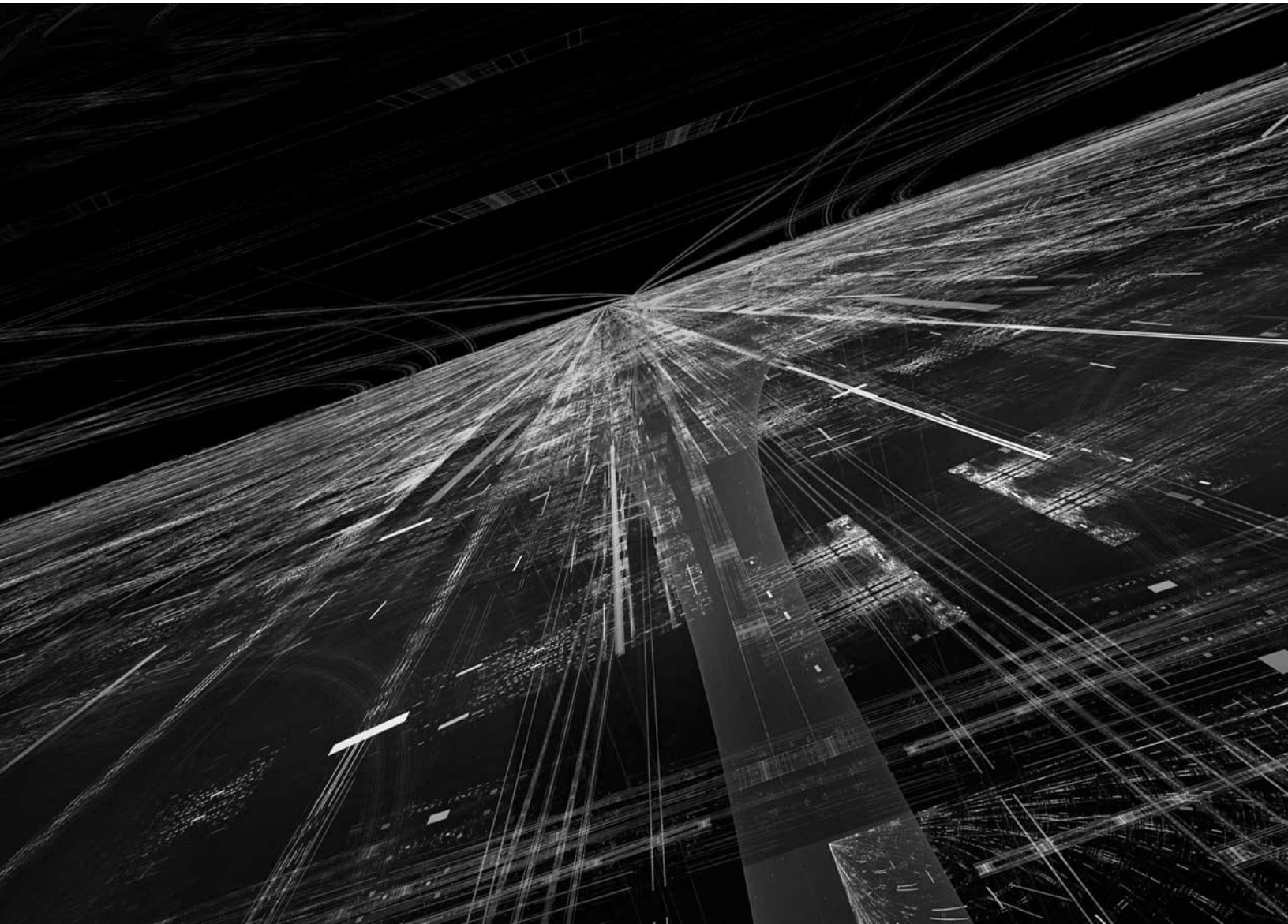
PARADIGM TECHNICA

Sponsored by: Teleport

Infrastructure Identity:

A New Paradigm for Trustworthy Computing in a Zero Trust World

Jack L. Poller, Principal Analyst
February 2025



Brace for Impact

Stolen credentials, phishing, and vulnerability exploitation are *still* the top three tactics attackers use to infiltrate organizations, according to the Verizon 2024 Data Breach Investigations Report.[1] Shockingly, both security incidents and confirmed breaches have doubled since last year. While zero-day exploits make the news, they're only behind 5% of breaches. The real threat? Identity attacks, which are now the go-to strategy for cybercriminals due to their simplicity and high success rate.

Human factors play a pivotal role in cybersecurity breaches, accounting for 68% of incidents, with 49% specifically linked to compromised credentials. Among these, web application credentials are the most often exploited, comprising roughly half of all credential-related breaches. This is closely followed by breaches stemming from email phishing, desktop sharing, and VPN credential theft.[1]

The simplicity of social engineering, where attackers manipulate individuals into divulging confidential information, often proves more effective than technical hacks. According to the IBM X-Force Threat Intelligence Index 2024[2], 30% of all security incidents involved stolen credentials, marking a 71% increase from 2023. These breaches result in data theft (32%), extortion (24%), and further credential harvesting (23%).

Over 95% of breached assets are servers

2024 DBIR

Moreover, computing infrastructure remains a primary target, with over 95% of breached assets being servers, and the frequency of successful attacks is on an upward trend.[1] This starkly underscores that current cybersecurity access solutions are not meeting the needs of rapidly evolving infrastructure environments.

Ironically, while individual computers can be considered secure, the collective computing environments constructed from them are demonstrably vulnerable to breaches, revealing significant systemic weaknesses in our cybersecurity defenses.

Modern Infrastructure Challenges

Traditional IT, once a simple realm of servers and networks, has morphed into modern infrastructure, a sprawling, intricate web of distributed systems, cloud services, and interwoven platforms. Three challenges now loom large: the complexity and scale of systems that have transformed traditional architectures and management strategies; the rampant spread of

[1] Verizon 2024 Data Breach Investigations Report, https://verizon.com/dbir.
[2] IBM X-Force Threat Intelligence Index 2024, February 2024, https://www.ibm.com/reports/threat-intelligence.

vulnerabilities—especially around secrets—that threatens to derail security; and the relentless targeting of digital identities by attackers who recognize them as the keys to the kingdom.

Complexity and Scale

In the past, building a web application was straightforward, relying on one of the standard stacks such as LAMP, J2EE, or .NET. These examples of a 3-tier architecture typical of the times were relatively simple as well as relatively easy to secure with a corporate network perimeter. Management focused on a device-centric model, involving manual configuration and maintenance of each resource.

As applications have grown in size, speed, and sophistication, the infrastructure supporting them has become exponentially more complex, with:

- Systems comprising hundreds of layers and hundreds to thousands of individual entities.
- Distributed Systems to handle scale and reliability.
- Elastic computing environments that make static configurations obsolete and require security teams to have coding skills.
- Federated Access for seamless user authentication across different platforms.
- Multiple Databases to cater to diverse data needs and optimize performance.
- Artificial Intelligence to enhance decision-making and user interaction.

Modern infrastructure is different than IT—modern infrastructure emphasizes automation, resilience, and the ability to adapt to failures without significant downtime, ensuring robust, secure, and efficient operations in complex environments. Where IT environments typically comprise just a few servers, modern infrastructure encompasses vast fleets of diverse resources. This has driven a transformation in systems management, foregoing hands-on management of individual elements in favor of automated management of large, scalable, and diverse systems. This is commonly referred to as moving from managing “pets” to managing “cattle.”

Vulnerabilities and Secrets

Modern infrastructure’s enormous scale and complexity heightens the risk of human error and opens many avenues for attackers to exploit. As the number of managed resources increases, so does the likelihood of mistakes by team members, which can grow exponentially.

Each new technological layer added to stay competitive both enriches functionality and expands the attack surface, as each component can be a potential entry point for cyber-attacks.

One critical vulnerability in such scaled environments is the management of secrets. Every entity in the compute environment relies heavily on credentials like API keys, ssh keys, private keys, session tokens, and even browser cookies. These secrets are prime targets for theft, sale, accidental sharing, or loss, particularly due to human oversight. That is why the target of nearly every identity attack is a secret or a credential.

Attackers frequently aim to acquire these secrets through tactics like phishing and social engineering, exploiting the human element. With large-scale modern infrastructures, the volume of credentials and access points becomes overwhelming, making comprehensive security measures difficult to maintain. This not only amplifies the attack surface but also complicates the task of securing each potential entry point against unauthorized access.

As complexity and scale inevitably reach a certain moment, *the mere existence of a secret anywhere in a computing environment is considered a vulnerability*. Rotating or encrypting secrets only delays that moment.

Identities

Humans are susceptible to manipulation and errors, making social engineering a highly effective strategy. Attackers use techniques like phishing, smishing, vishing, credential stuffing, and attacks on multi-factor authentication (MFA) to compromise identities, granting them access to systems. Once inside, they can move laterally across the network to access sensitive data and further infiltrate systems.

The breadth of access, ease of compromise, and extremely high success rate are why identity compromise is a favorite tactic and continues to be the most frequent attack vector in successful breaches.

A secret anywhere in the environment is a vulnerability

To counter identity threats and attacks, IT-focused solutions implement various security measures including Identity and Access Management (IAM), Identity Governance and Administration (IGA), Multi-Factor Authentication (MFA), and Identity Security Posture Management (ISPM).

However, these traditional controls face significant challenges when applied to modern infrastructure:

- **Scalability**: Traditional security controls were designed for environments with static, individually manageable resources (pets). They struggle to adapt to the scale and dynamic nature of modern infrastructures, where resources are numerous and constantly changing (cattle).
- **Identity Scope**: Security solutions often assume identities are solely human. Yet, in computing, identities also encompass hardware and software, which require their own identities, management, and access control.
- **Identity Silos**: with sprawling, heterogeneous systems, user access management is fragmented creating security gaps and operational inefficiencies.
- **AI-driven Attacks**: Artificial intelligence has reduced costs and increased the sophistication of identity attacks. AI can enhance the believability of social engineering,

speed up reconnaissance, conduct multiple parallel attacks, and adapt quickly to defensive changes.

- **Agentic AI**: Autonomous AI agents, capable of planning, reasoning, and executing tasks, introduce new security vulnerabilities. These agents, which blend characteristics of both software and humans, are prone to both malware and identity theft. Like humans, they require authentication and authorization, and their activities need to be auditable and distinguishable from the human operators.

A New Paradigm: Infrastructure Identity

Building a trustworthy infrastructure now demands a security architecture that incorporates all types of identities—hardware, software, human, and AI—in concert when deciding access rights. The security architecture must address the challenges of the modern infrastructure, ensuring:

- The architecture covers the entirety of the infrastructure, eliminating silos.
- Access decisions are swift, efficient, and made at scale.
- The architecture Integration into modern automated management methodologies.
- The architecture eliminates the inherent risks of secrets.

Inspired by the hyperscaler's adaptation of their security architecture to the evolving challenges of modern IT infrastructures—complexity, scale, automation, and the persistent targeting of identities by attackers—a novel security framework has emerged: **Infrastructure Identity**.

Infrastructure Identity introduces a comprehensive and unified identity model that encompasses:

- **Unified Identity Across All Entities**: This paradigm extends identities to cover all aspects of an infrastructure, including humans, hardware (servers, IoT devices), software (applications, services), and even AI agents.
- **Cryptographic Identities**: Instead of traditional username-password combinations, each component is given a cryptographic identity, eliminating the reliance on shared secrets and static credentials.
- **Zero-Trust Networking+**: Infrastructure Identity extends the zero-trust model, where no user is inherently trusted, and all users must be verified before being granted access, to incorporate all identities—humans and non-humans alike. Every identity and every access request are validated.
- **Short-Lived Privileges**: Moving away from long-term or permanent access rights, Infrastructure Identity employs ephemeral, just-in-time access, ensuring that access is granted only for the duration necessary to perform a specific task, reducing the window of opportunity for attackers to exploit credentials.

- **Dynamic Access Control**: Security controls are adaptive, responding to the context of the request, the identity of the requester, and the nature of the resource being accessed, minimizing exposure by tailoring privileges to the exact needs at the moment.

By implementing these principles, Infrastructure Identity addresses several critical pain points:

- **Mitigating Scale and Complexity**: Infrastructure Identity scales with the infrastructure, handling the dynamic nature of modern IT environments where resources are automatically managed and constantly changing.
- **Reducing Attack Surface**: By eliminating static credentials and employing cryptographic methods, Infrastructure Identity significantly lowers the risk of credential theft or reuse.
- **Enhancing Security Posture**: The zero-trust approach ensures that every action is scrutinized, reducing the likelihood of unauthorized access or lateral movement within the network.
- **Improving Compliance and Auditability**: With every identity and action being tracked and controlled, organizations can more easily comply with regulations and audit security practices.
- **Supporting Engineering and Development**: This Infrastructure Identity model integrates seamlessly with engineering practices by embedding security into the development and operational processes from the start, ensuring that infrastructure security is not an afterthought but a continuous aspect of the lifecycle.

Infrastructure Identity is a significant shift towards a more secure, resilient, and manageable approach to IT infrastructure, adapting to the modern infrastructure's demands for security at scale.

Implementing Infrastructure Identity: A Blueprint for Trustworthy Computing

The Infrastructure Identity Architecture redefines security by creating a trustworthy computing environment through a layered approach. This architecture is designed to manage the complexities of modern IT infrastructures, ensuring that every entity—whether human, machine, AI, or software—operates within a secure, auditable framework.

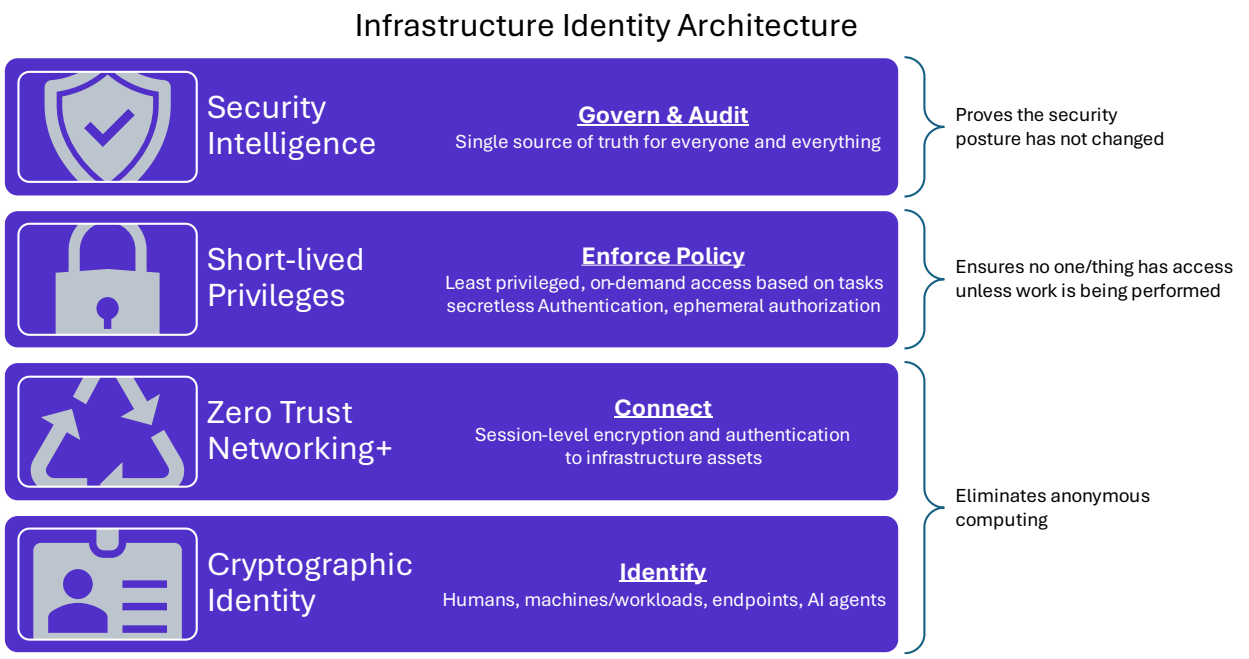


Figure 1: Infrastructure Identity Architecture

Here's how this architecture revolutionizes infrastructure security:

- **Cryptographic Identity:** This architecture is anchored in a strong security foundation based on cryptographic identities—secure, tamper-proof digital identities that use cryptographic methods to verify and authenticate individuals or entities accurately. Automation uses these identities to streamline and scale identity management across all resources. Additionally, trusted platform modules (TPMs), hardware security modules (HSMs), and other hardware-based solutions strengthen the attestation process. By reducing human error and mitigating social engineering risks, this approach enhances security, ensures efficiency, and enables seamless identity management across the entire infrastructure.

- **Zero Trust Networking+:** This layer extends zero trust security beyond human interactions to all infrastructure communications. Every service, container, database, and user interaction are encrypted, authenticated, and authorized on a per-transaction basis. By making identity the linchpin of security, this approach removes the outdated concept of a secure perimeter, enforcing continuous verification over implicit trust, thus creating an environment where security is inherently built into every connection.

- **Short-lived Privileges**: This critical layer introduces a dynamic access control system where permissions are granted only for the time needed to complete a specific task. Once the task concludes, access rights are automatically terminated. This “just-in-time” access model applies to all identities, ensuring that both human users and automated systems operate under the strictest principle of least privilege, significantly reducing the potential attack surface by ensuring no unnecessary access persists.

- **Security Intelligence**: Serving as the central hub for security operations, this layer aggregates all security-related data into one authoritative source. It allows for real-time threat detection, consistent security policy enforcement, and simplified compliance. Through continuous analysis, it shifts security from reactive to proactive, finding vulnerabilities before they can be exploited. This intelligence not only aids in immediate threat mitigation but also supports strategic security decisions by providing a holistic view of the security posture.

The Infrastructure Identity Architecture ensures that access is granted only for active tasks, enhancing security as the organization grows. By integrating cryptographic identities with a fortified zero-trust model, this architecture eliminates anonymity in computing, making every action accountable and auditable. This transparency is essential for enforcing security policies and maintaining a robust security posture, directly supporting the implementation of short-lived privileges for a truly secure, scalable, and trustworthy infrastructure.

Benefits of an Infrastructure Identity Platform

Deploying an Infrastructure Identity Platform based on this architecture yields substantial advantages for both engineering and security teams, focusing on speed, security, and resilience:

- **Accelerating Infrastructure Operations at Scale:** The Infrastructure Identity Architecture revolutionizes access and security management in large-scale environments. By dissolving anonymity and identity silos and adopting zero-trust ephemeral access, organizations can overhaul their access management strategies. This leads to the obsolescence of traditional VPNs and bastion hosts, while unifying privileged access management and simplifying compliance. As a result, engineering teams can shift their focus from managing complex security environments to delivering business value, enhancing productivity, and maintaining resilience as infrastructure scales.

- **Boosting Engineering Productivity:** The unification of identities across the board eliminates fragmented access points, streamlining both onboarding and access to critical infrastructure. This coherence in access management significantly improves engineering workflows, accelerating application development, automating infrastructure, managing resource fleets more efficiently, and implementing policies through code. By reducing operational complexities, the architecture not only saves engineering time but also accelerates project delivery and time-to-market.

- **Enhancing Security via Risk Identification and Mitigation:** With a central security intelligence layer, the platform provides a singular, authoritative view of security data, enabling proactive identification and blocking of unauthorized or “shadow” access. By eliminating static credentials and applying authorization based on specific tasks, it mitigates risks from human errors and sophisticated identity attacks. This architecture ensures compliance, reduces the attack surface, and fortifies the organization's security posture against threats, making security an integral part of operational efficiency.

- **Building Resilience by Transforming Security Models:** The Infrastructure Identity Architecture shifts away from static credentials and persistent privileges to a dynamic security model based on the principles of least privilege and zero trust. This transformation creates a "security invariant" where access is only granted during active tasks. During steady-state operation with no work to be done, no access is available, inherently reducing risk. By unifying all identity types into one model, it eradicates anonymity and puts security management into the hands of engineering, where it can be most effectively managed. This shift not only minimizes human error but also supports automated operations at scale, enhancing the organization's ability to detect, prevent, and respond to security threats, thereby significantly boosting overall resilience.

Why This Matters

In an era where cyber threats are more frequent and more sophisticated, the integrity of computing infrastructure stands as a critical linchpin in organizational security. The challenges of identity attacks, infrastructure complexity, and scalability issues underscore the urgent need for a paradigm shift in how we manage identity and access within vast, complex infrastructure environments:

- **Trustworthy Computing is a Necessity**: Identity attacks, using stolen credentials and human error, have become the most effective vectors for breaching organizational defenses. The traditional reliance on static credentials and standing privileges fails in this dynamic threat landscape, making a robust, trustworthy computing infrastructure an imperative.
- **Scalability Issues with Static Credentials**: Systems designed around static credentials and broad, persistent access rights are ill-equipped to handle the scale and agility required by modern infrastructures. The complexity of today's systems, with distributed resources and diverse identity types (human, machine, AI), demands a security model that can adapt and scale dynamically.
- **Unified Identity and Access Management:** The necessity for agility and resilience in infrastructure management drives the need for a unified approach to identity and access. This involves extending identity concepts to all entities, including non-human ones like servers, applications, and AI agents, ensuring that access is granted based on need, context, and the principle of least privilege.

The introduction of Infrastructure Identity as a new paradigm underscores the shift towards a security model where every entity, from hardware to AI, is authenticated and authorized based on real-time needs. This approach mitigates risks associated with scale and complexity, enhances security through zero-trust principles, and aligns with engineering and development processes to ensure security is integrated throughout the development lifecycle. By adopting these strategies, organizations can protect their assets more effectively while maintaining compliance, reducing operational overhead, and significantly improving their cybersecurity posture in an era where identity is the prime target.

Sponsored by: Teleport

Teleport is the Infrastructure Identity Company, modernizing identity, access, and policy for infrastructure, improving engineering velocity and infrastructure resiliency against human factors and compromise. The Teleport Infrastructure Identity Platform implements trusted computing at scale, with unified cryptographic identities for humans, machines and workloads, endpoints, infrastructure assets, and AI agents. Our identity-everywhere approach vertically integrates access management, zero trust networking, identity governance, and identity security into a single platform, eliminating overhead and operational silos. Headquartered in Oakland, CA, Teleport operates globally, with industry-leading customers such as Nasdaq, Moody's, Adobe, and Elastic. For more information, visit www.goteleport.com or follow @goteleport.