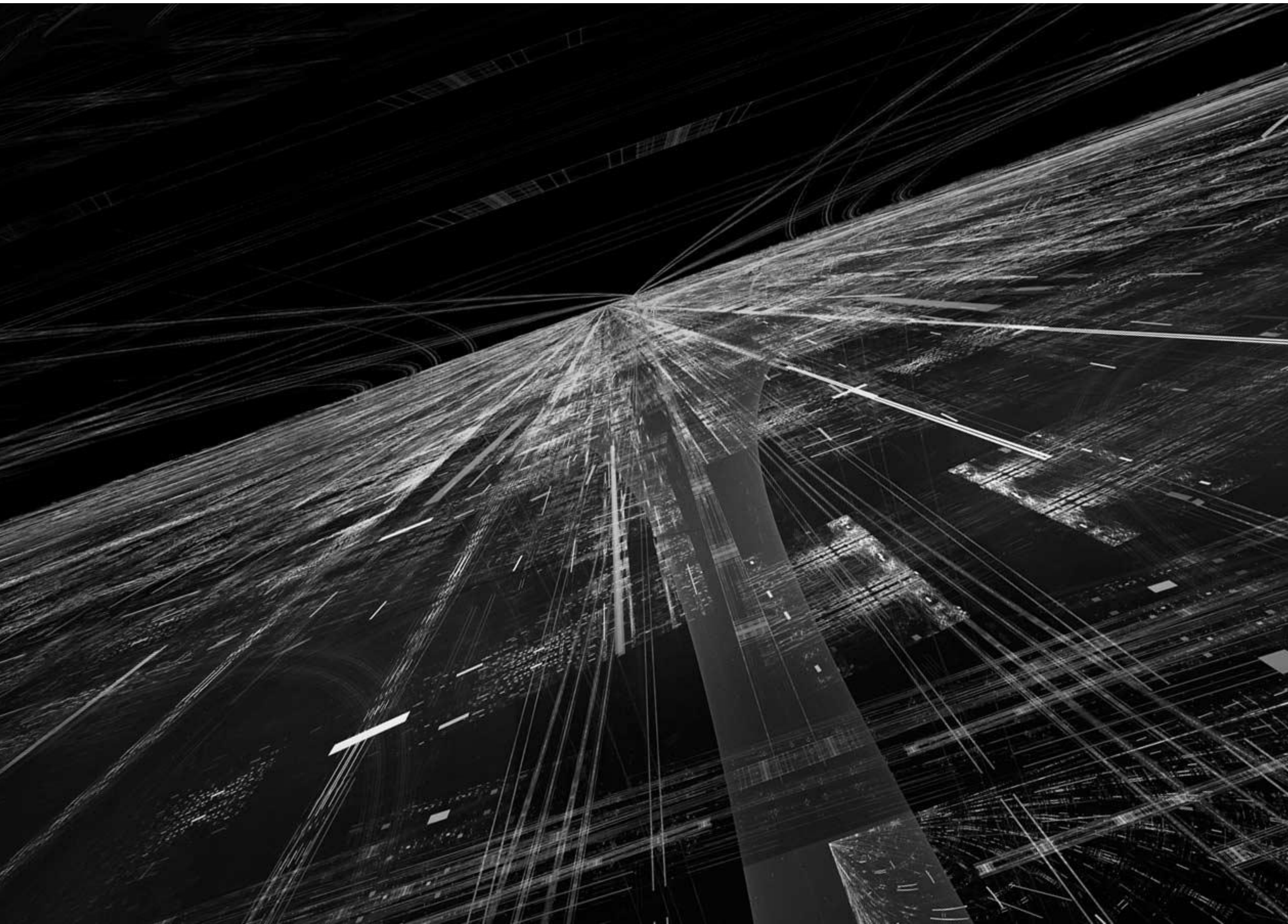
PARADIGM TECHNICA

Sponsored by: Teleport

Changing the Paradigm: Modernizing Secure Access to Infrastructure

Jack L. Poller, Principal Analyst

March 2024



The New Threat

According to the 2023 Data Breach Investigations Report, "the three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities." [1] While exotic and sophisticated zero-day attacks and vulnerability exploits garner significant press attention and thus are top of mind for CISOs and security teams, only approximately 5% of all breaches were the result of exploiting vulnerabilities in software.

Due to the considerable cost of mounting a successful malware-based attack and industry's increased investment in software supply chain security, attackers have adapted their strategy. Identity attacks have become much more common: 74% of all breaches include the human element, with 49% of breaches involving credentials, and approximately 15% used phishing.[2] Why is this happening? Because manipulating humans to share confidential information such as MFA codes, stealing credentials, and impersonating identities is easier than finding and exploiting software vulnerabilities.

According to the IBM X-Force Threat Intelligence Index 2024, 30% of all incidents used stolen credentials, a 71% year over year increase. The impact of these attacks can be devastating, with 32% of attacks resulting in data theft (up from 19% in 2022), 24% resulting in extortion, up from 21% in 2022, and 23% resulting in credential harvesting, up from 11% in 2022.[3]

Computing infrastructure continues to be the prime target of attacks as almost 85% of all data breaches involve servers.[4] Meanwhile, the infrastructure itself has been rapidly evolving and the existing cybersecurity solutions to manage access have not kept pace with the change.

The Impact of the Exploding Complexity of Modern Infrastructure

85% OF ALL DATA BREACHES INVOLVED SERVERS

2023 DBIR

The security best practices followed by most IT teams evolved around the static allocation of resources typical of traditional on-premises or co-located data centers. In what we call "***traditional IT***," management of the infrastructure often relies on a device-centric approach where each compute, storage, and networking resource is individually, independently, and manually configured and maintained. Security is enforced on the network level, hence the popularization of the term "NetSec," often relying on the corporate perimeter.

Manual management combined with perennial lack of skilled IT personnel (64% of organizations say IT candidates lack the necessary skills or experience and another 56% cite an overall shortage of candidates[5]) leads IT teams adopt new technology in phases over extended timeframes. Thus, many organizations miss obtaining immediate and short-term value and new technology is often perceived as being a poor return on investment.

Modern cloud infrastructure is vastly different than traditional IT. In what we call "***modern infrastructure***," storage, compute, and networking resources are automatically created and deployed

[1] 2023 Data Breach Investigations Report (DBIR), October 2023.
[2] Ibid.
[3] IBM X-Force Threat Intelligence Index 2024, February 2024.
[4] 2023 Data Breach Investigations Report (DBIR), October 2023.
[5] MIT Technology Review: New approaches to the tech talent shortage, September 2023.

with code (infrastructure as code). Whereas in traditional IT compute, storage, and networks are manually pre-provisioned, in modern infrastructure, these resources are automatically and dynamically provisioned on the fly at the same time as applications get deployed. Automation is used to scale resources as needed and many resources are ephemeral: servers can be created, used, and destroyed in a matter of minutes to accommodate changes in the business.

In modern infrastructure, there is no longer an operational difference between hardware and software: it is all code.

Deployment of new technology in modern infrastructure is also vastly different than traditional IT. Instead of phased, sequential deployment, Agile methodology is preferred with continuous deployment, where every change that passes automated testing is automatically deployed into production. Thus, changes to the infrastructure occur frequently, often on a daily basis.

The manual job of managing traditional IT by system administrators has evolved into DevOps engineers building and automatically deploying the new technology that drives modern infrastructure. DevOps engineers using Agile methodology emphasize automation and delivering incremental value to customers through frequent iterations and tight feedback loops.

DevOps teams are always applying new technology in the quest to accelerate time to value. As a result, the complexity of computing environments has exploded. Modern infrastructure technology stacks often consist of hundreds of technology layers, each exposing potential attack vectors.

The ephemeral nature of resources, the use of multiple cloud solutions, and the constant change inherent in modern infrastructure invalidates the concept of a static network perimeter. Additionally, the explosion of technology layers leads to fragmentation of user identities because not all computing resources are HTTP-based, and therefore do not integrate natively with identity platforms and SSO.

The traditional approach to security for traditional IT is no longer effective for modern infrastructure where the network perimeter is no longer relevant, nothing is static, everything is ephemeral and defined by code, and the explosion of complexity leads to many technology layers each featuring its own remote access protocol.

Today, IT teams focus on two tasks: securing access to web apps used by the workforce and securing traditional IT. Meanwhile, the task of meeting new requirements to secure modern infrastructure is often taken by DevOps engineering teams.

Securing Access to Web Applications

The primary difference between securing access to web applications and infrastructure is in the underlying protocols and tools. Web applications are always consumed in a browser or on a smartphone where popular standards such as OAuth and SAML are available to enable password- and passwordless-based authentication. This de facto standardization on web applications and authentication protocols is helpful because it enables IT teams to establish a set of principles to secure access. These principles are:

- **Consolidation of user identities.** Instead of using the identity store built into each application, IT teams should consolidate user identities into a unified Identity Platform (IDP) and implement single sign-on (SSO). This dramatically lowers the operational overhead of provisioning and deprovisioning access at scale.

- **Adopt strong authentication.** All identities, regardless of privilege, must use phishing-resistant authentication – strong MFA, preferably coupled with biometrics on a trusted client device equipped with a trusted platform module (TPM) to minimize the probability of credential compromise.

- **Adopt identity governance and administration (IGA)** to implement **the principle of least privilege**. Ensure that each identity is given only the privileges necessary to do the job, no more and no less. Obtain visibility into weak access patterns (such as accounts with disabled MFA) and implement robust analytics and reporting for easier enforcement of compliance standards.

Securing Access to Traditional IT

While the principles to secure access to web applications are well known and understood, applying these principles to traditional IT has proven to be challenging due to some inherent differences. One difficulty is that computing resources use a variety of communication protocols and are not always consumed in a browser. This means that some of the principles, such as using standard authentication protocols, SSO, or strong authentication may be hard or impossible to implement.

Another difficulty is consolidating identities and access policies. Every server has a list of user accounts that exist in a silo and may not be able to be synchronized with an IDP.

Traditional IT historically has been designed to rely on the network perimeter for security, and strong encryption and authentication is not the default.

To address these challenges, IT teams looking to secure access to traditional IT should consider these additional principles:

- **Transition to the zero trust security model**. The perimeter security model implicitly trusts anyone inside the perimeter. The zero trust security model removes this implicit trust concept and relies on strong authentication for security. Every client must be authenticated, and every connection must be encrypted end-to-end.

- **Deploy privileged access management (PAM).** IT teams managing traditional IT rely on privileged accounts on statically configured servers. While having these accounts in an identity silo in each server is unavoidable, a PAM solution that controls access to these privileged accounts is invaluable. PAM systems can provide complete visibility and control access to the privileged accounts, enabling IT teams to enforce the principle of least privilege.

- **Adopt the principle of defense in depth.** Employ multiple layers of security measures to protect the organization's assets, ensuring that if one defense fails, others will continue to provide protection. Specifically, IT teams should invest in identity threat detection/response (ITDR) and security information and event management (SIEM). These cybersecurity and identity observability solutions enable the detection of unwanted or anomalous behavior. Using ITDR and SIEM systems can help IT teams to analyze access patterns, security events, and network traffic to identify and lock compromised identities and terminate all relevant active sessions.

Securing Access to Modern Infrastructure

The solutions designed for securing traditional IT are often insufficient for modern infrastructure that is elastic, ephemeral, and defined by code.

Infrastructure as code introduces new attack vectors. The infrastructure provisioning code, the deployment pipeline that executes the code, and the DevOps engineers who build and maintain the infrastructure-as-code pipeline all become a new class of de-facto privileged accounts with access to execute any action on any resource.

In modern infrastructure, there is a much greater variety of computing resources to protect: physical servers, virtual servers, cloud provider accounts, containers, Kubernetes, CI/CD pipelines, DevOps dashboards, and dozens of specialized databases. IoT, mobile platforms, and generative AI drive even greater complexity. Every resource has its own remote access protocol, its own need for encryption, and its own identities with credentials, policies, and need for auditing. Every resource requires domain-specific expertise to secure and manage, placing a significant operational burden on IT teams.

The explosion of resources leads to an explosion of credentials distributed among multiple identity silos and multiple policy silos, expanding the attack surface and increasing organizational risk.

While infrastructure-as-code automation lowers operational overhead, it requires identities for machine-to-machine access. And the machines themselves represent yet another challenge and another attack vector as the organization must define identities and access policies for both humans and machines. Moreover, in the quest for ever-greater efficiency, DevOps engineers are splitting cloud-native applications into smaller micro-services, each requiring its own identity to implement the principle of least privilege. All of this leads to ever-increasing fragmentation of identities and policies.

Social Engineering and Identity Attacks

The rise of complexity, the resulting fragmentation of identities, and the engineering talent shortage contribute to the identity attacks that are the root cause of increasingly frequent data breaches.

The typical identity attack follows a pattern of leveraging identification and authentication failures followed by lateral movement. Identification and authentication failures can occur through:

- Phishing, smishing, or vishing, where the attacker uses disguised email, texts, voicemail, or AI-based voice impersonation and social engineering to deceive someone into revealing their password or MFA factors.
- Credential stuffing, where the attacker tries to authenticate using a list of valid usernames and passwords from other applications or organizations.
- Default, weak, or well-known usernames and passwords such as “Password1” or “admin/admin”.
- Weak or ineffective forgotten-password or credential recovery processes.
- Ineffective or missing MFA.

Once the attacker gains access, they attempt to move laterally across the environment. Instead of directly attacking a single target, attackers navigate through the various interconnected systems, using the compromised credentials to gain access to different resources. This enables the attacker to access sensitive data or systems that might otherwise be protected.

All the techniques used to gain access through identification and authentication failures are forms of social engineering: the manipulation and exploitation of human psychology and behavior. Knowing this, many organizations attempt to counter these social engineering techniques through security awareness training.

However, humans are easily distracted and forgetful, and training must continuously be reinforced. And as the organization scales and the complexity of the infrastructure continues to increase, the number of identities and identity silos increase, providing ever more opportunities for social engineering attacks.

While training can reduce the probability of a successful attack, it can't reduce the probability of success to zero. Yet, the existing methodology for protecting modern infrastructure continues to rely on good human behavior to recognize and ignore social engineering attacks.

A New Paradigm to Modernize Secure Access to Infrastructure

Modern infrastructure environments are predicated on being highly scalable. Thus, they require scalable approaches to security: as more resources are added, as more technology layers are introduced, and as more engineers join the team, the probability of social engineering, human manipulation, or human error leading to credential theft must not increase.

Integrating security as early as possible into the design, development, and deployment of modern infrastructure enables teams to design security into the environment rather than bolt-on security as an afterthought. This means transferring the responsibility for security of modern infrastructure from traditional IT teams to DevOps teams as these teams are responsible for the design and architecture and therefore have the required expertise to understand how to secure the environment. This "shifting left" of security enables early identification and remediation of vulnerabilities, reducing costs and improving security.

Shifting security left and ensuring the scalability of security is just a partial solution. What is needed is a new paradigm to modernize secure access to infrastructure – one that eliminates the human element from the access path. Since the ultimate goal of social engineering attacks is to obtain valid credentials by manipulating humans into exposing shared secrets, removing all forms of shared secrets removes the human element and in turn drastically reduces risk of compromise.

Organizations applying this new paradigm – removing shared secrets and the possibility of social engineering – need to apply a set of principles pertaining to the characteristics of identity in modern infrastructure. These principles are:

- **Consolidate all identities**. All identities – people as well as non-human systems such as servers, laptops, bots, databases, microservices, etc. – need to be consolidated into an inventory that is a single source of truth. Because modern infrastructure is dynamic and resources are ephemeral, the inventory must automatically self-update rather than rely on manual maintenance. This ensures that the live inventory is always accurate and scales with the environment.
- **Enforce strong authentication with cryptographic identity**. Deploy strong authentication by making phishing-resistant passwordless authentication mandatory. While traditionally, strong authentication applies to human users, it's imperative that organizations also authenticate every system and resource in the infrastructure to be able to grant the appropriate privileges. This also prevents attackers from deploying their own rogue malicious systems.

But how do you implement passwordless authentication for non-human systems? By assigning a unique identity to every system or resource. This identity must be able to be cryptographically authenticated using public key infrastructure (PKI) with hardware security modules (HSMs) and TPMs. This can be challenging to manually implement in dynamic, ephemeral environments such as Kubernetes, where systems are automatically instantiated as needed. Thus, automating the processes is a necessity. Adopting cryptographic identity is the key to making infrastructure security immune to human errors and human behavior.

- **On-demand least privilege access.** In traditional IT, users are granted a set of static privileges and can use those privileges at any time. Thus, attackers who successfully take over an account have access to those privileges at any time. Removing these "standing privileges" removes this risk vector.

  Instead of standing privileges, organizations need to provide on-demand access, where the privilege to accomplish a task is provided only when there is a task to complete. By providing a unified access mechanism that is a front-end to all the disparate infrastructure access protocols, organizations can grant access based on tasks. This enables granting the minimal required privileges to complete the task and ensures that access is deprovisioned immediately after the task is completed. On-demand least-privileged access needs to be applied to both human and non-human machine and service accounts.

- **Zero Trust**. Remove implicit trust from the network by transitioning from perimeter security to zero trust security. This prevents an attacker from moving laterally; they're stopped at a single compromised resource, reducing the blast radius.

  The goal of zero trust is that every resource can be safely exposed to public access, removing the distinction between the corporate network and public networks and obviating the need for firewalls and VPNs.

  To achieve zero trust, organizations need to either remove insecure access protocols or to provide a secure wrapper (tunnel) around those protocols. Additionally, zero trust access for modern infrastructure should provide unified access that incorporates a single control point for authentication and authorization. This provides visibility, auditing, and enforcement of policies and compliance with regulations. It is imperative that the unified access system can associate the actual human user with each action, even for shared identities.

Why This Matters

Organizations today face a plethora of cyberattacks, and while ransomware and zero-day exploits of vulnerabilities get the majority of publicity and attention, identity-related attacks are the most common and widespread. Worse yet, in 2023 attacks targeting infrastructure increased by 75% year over year.[6]

Why are attackers targeting infrastructure? For two reasons:

1. It's easy! Without phishing resistant authentication, it's easy for attackers to compromise credentials and purchasing stolen credentials is commonplace.

[6] Crowdstrike 2024 Global Threat Report, February 2024.

2. In modern infrastructure, every access is a privileged access. Gaining access to a DevOps credential gives the attacker carte blanche access to the entire infrastructure and all the sensitive and critical corporate data.

Modern DevOps infrastructure is complex, dynamic, and ephemeral. What works for traditional IT – perimeter security with VPNs, shared secrets, vaults, PAM, IGA, and many other security controls – doesn't work for modern infrastructure.

If your organization has adopted modern cloud infrastructure and DevOps, and wants to reduce its risks, you should consider a new cybersecurity paradigm. Your infrastructure security needs a unified access solution that can enforce strong authentication and authorization that provides on-demand least privilege access based on a foundation of cryptographic identity and zero trust.

Sponsored by: Teleport

Today's computing environments have too much complexity, too many network boundaries, and too little trust. Complexity slows engineers down and leads to human errors. Complex systems can't be secured despite the red tape of bureaucracy. Teleport makes trusted computing simple. Teleport modernizes infrastructure access, improving efficiency of engineering teams, fortifying infrastructure against bad actors or error, and simplifying compliance and audit reporting. With Teleport Access Platform, organizations improve their resiliency to identity-based attacks, while giving engineers freedom to move and freedom to build a better future. For more information, visit www.goteleport.com.

This Paradigm Technica White Paper was commissioned by Teleport and is distributed under license. All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources Paradigm Technica considers to be reliable but is not warranted by Paradigm Technica. This publication may contain opinions of Paradigm Technica., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent Paradigm Technica.'s assumptions and expectations considering currently available information. Paradigm Technica. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.