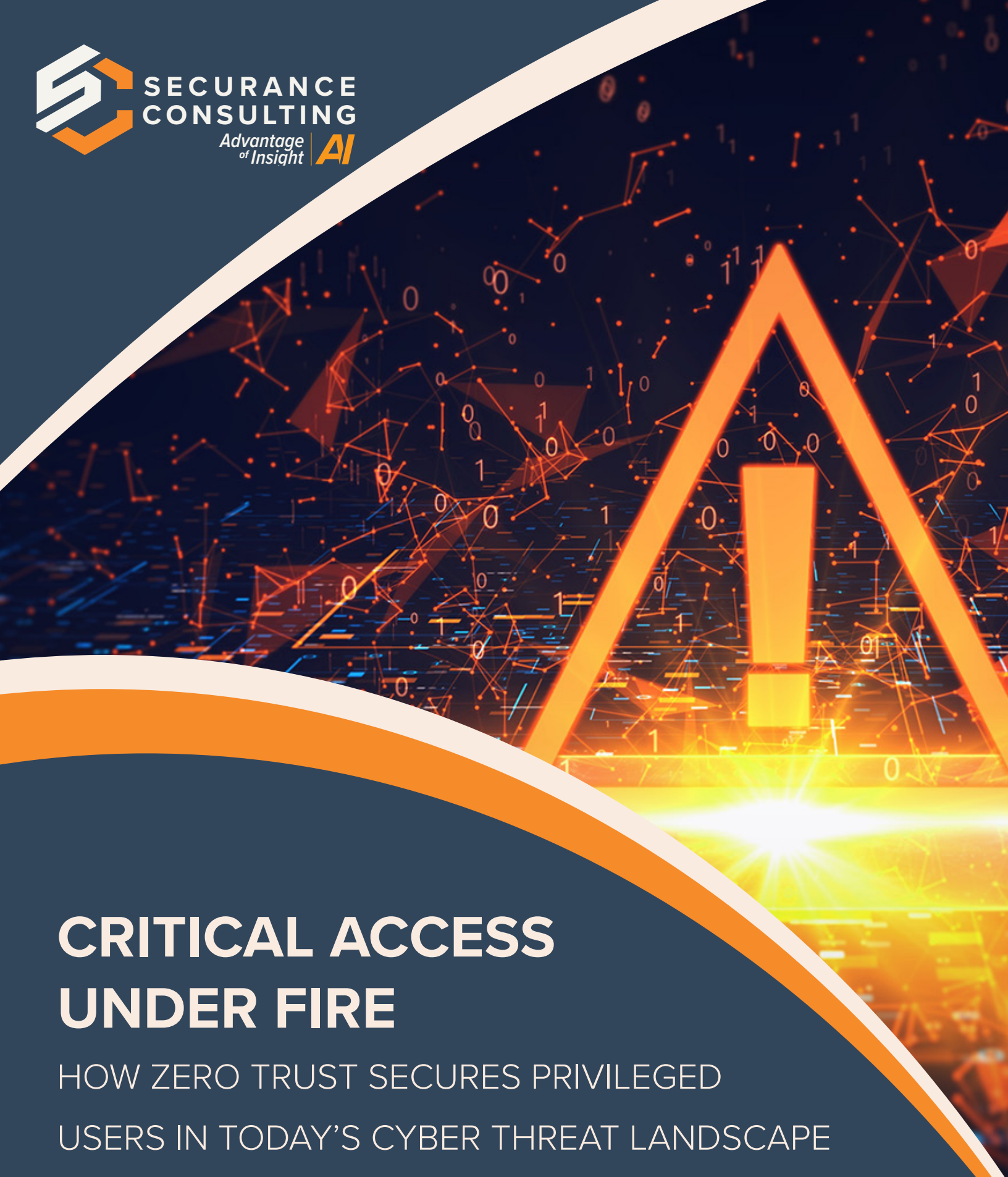
SECURANCE CONSULTING
Advantage of Insight | AI



CRITICAL ACCESS UNDER FIRE

HOW ZERO TRUST SECURES PRIVILEGED USERS IN TODAY'S CYBER THREAT LANDSCAPE

www.securanceconsulting.com

Privileged users—administrators, developers, cloud architects, and third-party vendors—have access to the systems that run your agency or business. If these accounts are compromised, attackers can bypass firewalls, disable security tools, steal sensitive data, and even destroy your infrastructure.

The zero trust model offers a modern, proactive approach to this escalating risk. With its foundational principle of **"never trust, always verify,"** zero trust transforms the way organizations manage access to critical resources. It enforces identity governance, least privilege, continuous monitoring, and strong authentication to ensure that no one can move through your environment unchecked.

In this white paper, we'll explore:


Why privileged accounts are the number-one target in most breaches


How zero trust helps shut down privilege escalation and lateral movement


Real-world breaches that highlight the risks—and the missed opportunities—associated with unchecked privileged access


Strategies to protect privileged accounts

> ***Every major breach in the last decade involved a compromised privileged account." - Cybersecurity & Infrastructure Security Agency (CISA)*** [1]

The Privileged Problem

Privileged accounts grant users elevated access to critical systems, sensitive configurations, high-value data, and cloud infrastructure. These aren't your standard user accounts; they're the keys to the kingdom. Think of domain administrators with control of entire networks, root accounts with unrestricted system privileges, service accounts that run automated processes, and DevOps roles with the ability to modify production environments.

Because of their power, privileged accounts are high-value targets for attackers and often weak points in an organization's security posture. Unfortunately, they're frequently:

Overprovisioned – Users are given broader access than they need, either in the name of convenience or due to unclear role requirements. This increases the blast radius if credentials are compromised.

Under-audited – These accounts often operate with little oversight. Without regular reviews and activity logging, it's difficult to detect misuse or confirm that actions are legitimate.

Persistent – Many privileged accounts are always active and rarely expire, which gives attackers a wide window of opportunity to establish backdoors.

Without strict governance, privileged accounts can turn into major security liabilities. That's why managing and securing them is a critical pillar of zero trust and identity-centric security strategies.

REAL-WORLD BREACHES

The Okta Support System Breach

In October 2023, identity management service provider Okta disclosed a security incident involving its support case management system. An attacker had gained unauthorized access using stolen credentials from a privileged service account. Once inside, the attacker was able to view sensitive HTTP session tokens uploaded by customers.[2]

Several identity and access control failures contributed to the breach:

Overprivileged Service Account: The compromised service account had elevated privileges without sufficient guardrails. It wasn't restricted by least privilege principles, and there were no controls to limit what it could see or do.

Lack of Visibility: There was no session recording or detailed audit trail of the account's actions, making it difficult to trace what was accessed and when.

Absence of Real-Time Monitoring: The breach wasn't immediately detected because there was no behavioral monitoring to flag unusual activity, such as a service account performing actions outside its typical usage patterns.

Uber's Internal Tools Breach

In September 2022, Uber experienced a significant security breach that began with the compromise of a privileged contractor account. The attacker initiated a targeted social engineering campaign, using malware or phishing to harvest the contractor's credentials.[3] To bypass multi-factor authentication (MFA), the attacker used an MFA fatigue tactic—repeatedly sending push notifications until the contractor unintentionally approved access.

With valid credentials and MFA approval, the attacker logged into Uber's virtual private network (VPN) and gained access to the internal corporate environment. From there, they:

- Exploited a PowerShell script on a shared network drive containing hardcoded administrator credentials, a major credential management failure.
- Used the admin credentials to access Uber's privileged access management (PAM) platform.
- Escalated privileges and moved laterally across several critical systems.

These breaches highlight why zero-trust architecture (ZTA) is critical for securing privileged access. Zero-trust controls could have significantly reduced the attacker's reach or prevented the breach altogether. For example, enforcing least privilege through role-based, time-limited access would have limited the attacker's ability to move laterally within the environment.

Requiring phishing-resistant MFA (such as FIDO2 or WebAuthn) could have blocked the initial login attempt. Eliminating standing administrator credentials and regularly rotating secrets would have made privilege escalation far more difficult. Additionally, implementing strong network segmentation between user systems, administrative tools, and production environments would have prevented unrestricted access to critical infrastructure.

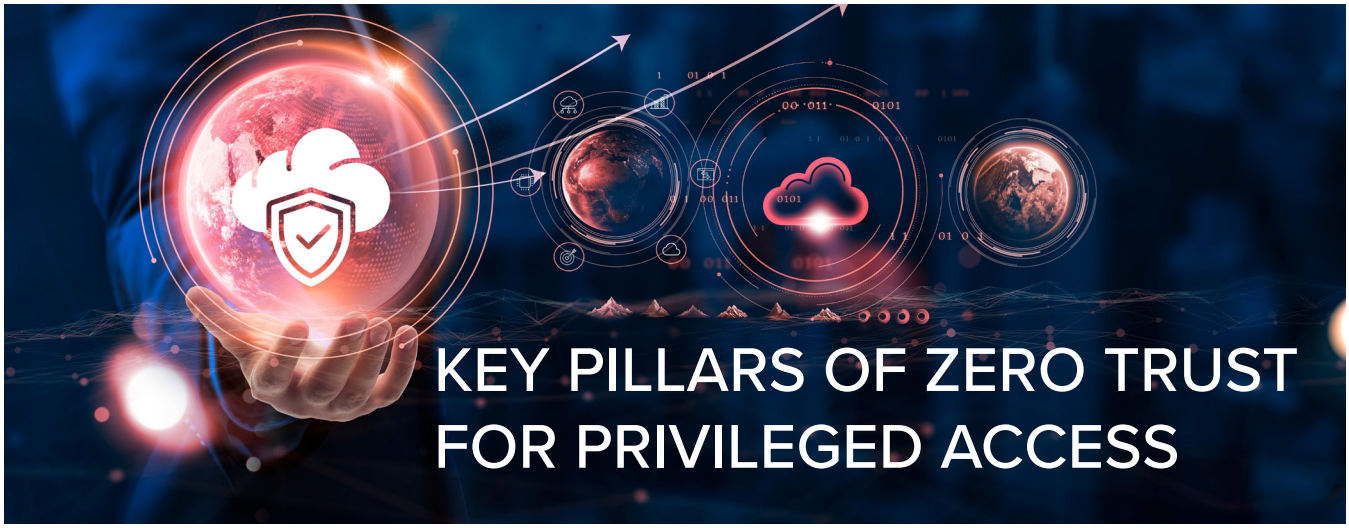
Zero trust is not a one-time solution or a single product. It's a strategic, ongoing approach to cybersecurity. This is especially important when managing privileged users, who pose the greatest risk if compromised. Zero trust requires continuous identity verification, granular access controls, real-time monitoring, and automated enforcement. As these incidents show, failing to implement these measures can leave organizations vulnerable to significant operational, financial, and reputational harm from a single compromised account.

Zero Trust: A Security Framework Built for Privileged Access

At its core, zero trust is a security philosophy that flips the traditional model on its head. Instead of trusting users and devices just because they're "inside the network," zero trust assumes no user, device, or workload is inherently trustworthy, even if it's behind the firewall. Every access request must be explicitly verified, and contextually validated.

This approach is especially critical when it comes to privileged access. A single privileged account can reconfigure an environment, exfiltrate data, or disrupt operations. For attackers, compromising a privileged account is a golden ticket. For defenders, it's where zero trust must be airtight.

Identity verification in a zero trust model is about more than just who is accessing a resource—it's also about how, where, and when access occurs. Context-aware policies evaluate risk in real time, adjusting authentication requirements based on behavioral anomalies, device posture, or geolocation. This dynamic, adaptive approach closes critical gaps that static credential systems leave wide open.



Every access attempt must begin with strong identity assurance. In a zero trust framework, verifying identity goes far beyond requiring a username and password. It involves confirming the legitimacy of the user, device, location, and context behind the request. This layered approach ensures that only the right people, using trusted devices under the right conditions, can access sensitive systems and data.

Key elements include:

1. **Phishing-resistant MFA:** Traditional MFA methods like SMS or app-based codes are increasingly vulnerable. Instead, zero trust demands phishing-resistant options, such as FIDO2 security keys, smartcards, or certificate-based authentication, which offer stronger protection against credential theft.
2. **Digital Certificates for Device Trust:** Authenticating the device is just as important as authenticating the user. Digital certificates ensure that only known, managed, and compliant devices can access critical resources, helping prevent unauthorized device access.
3. **Biometrics or Passwordless Authentication:** Static credentials like passwords are a common target for attackers. Implementing biometric logins, facial recognition, or passwordless technologies, such as Windows Hello or hardware tokens, strengthens identity assurance while improving the user experience.
4. **Least-Privilege Access:** Zero trust enforces access that is limited, temporary, and purpose-driven. The principle of least privilege ensures users only get the minimum level of access required for their role and only when needed. Implementing controls such as role-based access controls (RBAC), attribute-based access controls (ABAC), and just-in-time (JIT) access helps prevent privilege misuse and contain insider threats or lateral movement.
5. **Session Monitoring and Recording:** With privileged access comes a need for oversight. Session monitoring tools track and record user activity in real time—capturing keystrokes, commands, and screen actions. This visibility enables organizations to detect anomalies, investigate incidents, and meet compliance requirements. It ensures accountability, especially for high-risk access scenarios, and supports post-event forensics.

6. **Microsegmentation:** Microsegmentation limits the blast radius of attacks by isolating workloads, systems, and user groups into discrete network segments. Each segment enforces its own access rules, reducing opportunities for lateral movement. This approach is essential in hybrid and multi-cloud environments, where traditional perimeter defenses fall short. It allows organizations to enforce least-privilege access at the network level.

7. **Behavioral Analytics:** Static rules aren't enough. Zero trust uses behavioral analytics to detect unusual or risky activity based on learned behavior patterns. User and entity behavior analytics (UEBA) establish baselines and flag deviations such as access from new locations or unusual times. Behavioral insights enable real-time threat detection and can trigger step-up authentication or automated response, turning reactive security into proactive defense.

8. **Smarter, Stronger MFA Enforcement:** Zero trust requires adaptive MFA that responds to risk context, including unfamiliar devices and geolocations. It also counters MFA fatigue attacks through number matching, biometric confirmation, and rate limiting. Strong MFA isn't optional. It's a foundational layer that must be resilient, universal, and intelligent.

Implementation Tips:

1. **Start with Privileged Access**

   Rolling out a zero-trust architecture across an entire enterprise can feel daunting. But you don't need to do it all at once to make an immediate impact. The best place to start, both strategically and practically, is with your privileged users.

   Privileged accounts have the keys to your most critical systems, sensitive data, and infrastructure. If compromised, these accounts can enable attackers to cause maximum damage with minimal effort. That's why securing privileged access delivers fast, high-impact results and sets a strong foundation for a broader zero trust journey.

   Key risks include:

   - **Overprivileged Roles:**
     Whether in the cloud, on-premises, or hybrid environments, users and services are frequently granted more access than needed "just to get the job done." This violates the principle of least privilege and increases the risk of misuse, whether intentional or accidental.

   - **Lack of Visibility and Governance:**
     Organizations often struggle to track and manage who has access to what across their entire IT ecosystem, including cloud platforms, legacy systems, and third-party SaaS tools. Without centralized governance and regular access reviews, overprovisioned accounts can go undetected, creating fertile ground for insider threats and unauthorized access.

   - **Exploitable Misconfigurations:**
     From misconfigured cloud storage buckets and open ports to outdated access control lists in on-prem systems, technical missteps are common. When paired with excessive permissions, these misconfigurations create high-risk vulnerabilities that attackers are quick to exploit.

- **Privileged Access via Federated Identities:**
  Many organizations rely on identity providers like Azure AD, Okta, or Ping Identity to manage access across systems through federation. If federation is improperly secured, such as through misconfigured trust relationships or weak authentication, it can become a direct pathway for attackers to reach sensitive resources.

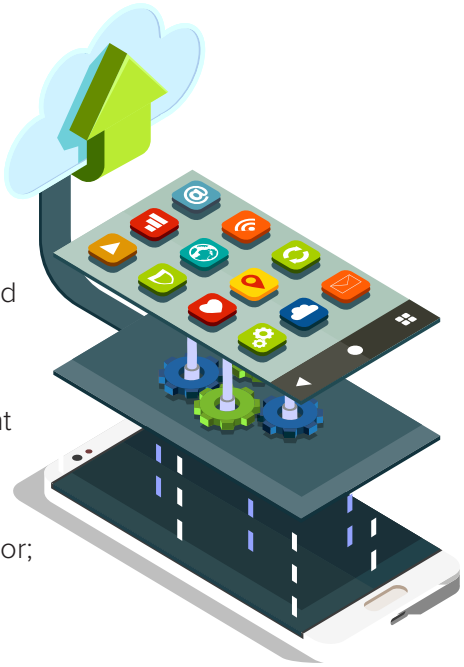
2. Mitigate Risk

Without strict controls, users and systems often end up with more access than they need, which makes it easier for attackers to exploit misconfigurations, misuse accounts, or steal credentials. The following best practices help reduce these risks and ensure stronger, more secure access management across your cloud and on-premises systems.

- Implement least privilege policies and regularly audit permissions.
- Enforce MFA for both cloud consoles and command-line interface (CLI) access. CLI access gives admins direct control over systems, making it critical to secure with strong authentication.
- Use cloud-native security tools, like the AWS IAM Access Analyzer, Azure Privileged Identity Management, and GCP IAM Recommender, to detect misconfigurations and overprivileged accounts.
- Apply JIT access for administrative roles and monitor privileged sessions.
- Adopt a zero trust approach to cloud access and treat every request as untrusted until it has been verified.

As IT environments grow more complex and interconnected, privileged access must be tightly managed. Without proper oversight, a single misstep can expose entire systems to compromise.

3. Secure Vendor Access



One of the biggest mistakes organizations make is granting always-on administrative rights to users or third parties. In zero trust, access should be time-bound, JIT, and fully auditable.

Third-party vendors, such as IT consultants, contractors, managed service providers (MSPs), and software integrators, often require temporary, elevated access to internal systems. They may be brought in for upgrades, troubleshooting, deployments, or specialized tasks. But while they can be essential to business operations, these external users also pose a significant security risk if their access isn't tightly controlled.

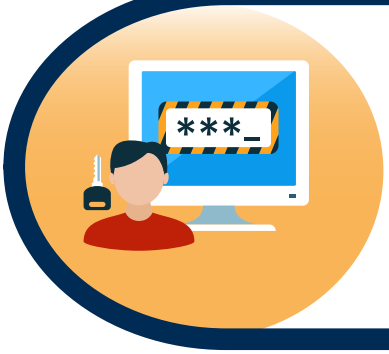
In many high-profile breaches, attackers didn't break in through the front door; they piggybacked through poorly managed vendor accounts.

One of the most infamous examples of third-party risk occurred when hackers compromised Target's point-of-sale (POS) systems and stole data on 40 million credit and debit cards, along with personal information for another 70 million customers.[4]

How Weak Vendor Access Controls Led to a Major Data

1. Initial Compromise: Attackers obtained login details used by Target's HVAC contractor.

Insider Risk: Third-party access became an entry point.



2. Over-Permissioned Access: The vendor account had more access than necessary to perform HVAC functions, including access to Target's billing platform.

Risk Amplified: Minimal restrictions led to maximal exposure.

3. Poor Network Segmentation: Vendor access was not segmented from critical infrastructure.

Consequence: Payment systems were vulnerable to compromise.

4. Breach Execution: Attackers reached point-of-sale terminals.

Outcome: A massive data breach affected millions of customers.

The breach not only damaged Target's reputation, but it also resulted in hundreds of millions in fines, legal costs, and remediation expenses.

The scale and cost of the Target breach underscore a hard truth: Traditional perimeter-based defenses are no longer enough. Once attackers gained access, there were few internal controls to stop them. This is exactly the kind of scenario that zero trust is designed to prevent.

A zero trust approach treats third-party users just like any other untrusted entity. It requires rigorous validation and tight control over every access request. Here's how it strengthens vendor access management:

- **JIT Access**
  Instead of persistent accounts, vendors receive access only when needed and only for a limited time, reducing the window of risk.
- **Least Privilege Enforcement**
  Third parties are granted the minimum level of access required to perform their tasks—nothing more. This limits lateral movement if credentials are compromised.
- **Strong Authentication and Verification**
  Vendors must pass MFA and may be required to authenticate through identity federation or secure portals.
- **Session Monitoring and Audit Trails**
  All vendor activity should be logged and, where appropriate, recorded in real time. This ensures visibility into what's being accessed and by whom.
- **Network Segmentation and Isolation**
  Even if vendors have access, they should be restricted to specific zones or resources, preventing them from accessing sensitive systems like production environments or payment platforms.

Vendors can be an extension of your team or a weak link in your security chain. Without strict governance, a single third-party account can become the entry point for a major breach. Zero trust ensures that vendor access is measured, monitored, and minimal, helping organizations protect their most sensitive assets.

4. Protect Cloud Environments

Zero-trust is also critical in today's cloud-first environments, where workloads, users, and data are no longer confined to corporate networks. With continuous authentication, microsegmentation, and context-aware policies, zero trust protects cloud resources from lateral movement and unauthorized access, no matter where users or systems are located.

As organizations shift more workloads to the cloud, platforms like AWS, Microsoft Azure, and GCP have become foundational to enterprise IT. These environments depend on identity and access management to regulate access to critical resources. Privileged roles can create, modify, or delete resources; access sensitive data; manage security settings; and even disable logging and monitoring. When these permissions are overly broad, misconfigured, or unmonitored, they significantly expand the attack surface and increase the risk of compromise.

QUICK WINS TO ACCELERATE YOUR ZERO TRUST ADOPTION

1. **Inventory All Privileged Accounts**
   You can't secure what you don't know. Begin by identifying all privileged users, service accounts, domain admins, and application credentials across your environment, including cloud services. Pay attention to legacy accounts and shadow IT.

2. **Enforce MFA for All Admins**
   Make phishing-resistant MFA non-negotiable for anyone with elevated privileges. This alone can prevent the majority of credential-based attacks.

3. **Rotate and Vault Credentials**
   Use a PAM solution to store, rotate, and manage privileged credentials. Eliminate hard-coded passwords and shared admin accounts that attackers love to exploit.

4. **Limit Persistent Access**
   Apply JIT access so that privileged rights are granted only when needed and revoked immediately afterward. This minimizes the attack surface and reduces standing risk.

5. **Monitor All Sessions with PAM Tools**
   Record and monitor all privileged sessions in real-time. Look for unusual behavior and ensure every action can be audited. Session monitoring is your frontline defense for detecting misuse or compromise.

6. **Auto-Expire Unused Accounts**
   Stale accounts are a major liability. Automate the expiration and cleanup of dormant privileged accounts to reduce exposure and enforce least privilege.

> ***The overarching zero trust concept of 'never trust, always verify' is about controlling access—and privileged access is the riskiest type of access. - Delinea*** [5]

By focusing on privileged access first, you're tackling the highest-risk, highest-value targets and building momentum to implement a zero-trust architecture across all users, devices, networks, and workloads.

FINAL THOUGHTS: A STRATEGIC IMPERATIVE

Privileged accounts are under constant attack, and for good reason. These accounts offer cybercriminals direct access to your most sensitive systems, data, and infrastructure. With a single set of compromised credentials, an attacker can disable defenses, move laterally, exfiltrate critical data, or disrupt operations.

Without the guardrails of zero trust access controls, privileged accounts become ticking time bombs quietly waiting to be exploited. When you implement zero trust principles, such as continuous verification, least privilege enforcement, and real-time monitoring around privileged access, you protect not only accounts and passwords, but also your organization's operations and its future.

Call to Action

Ready to secure your privileged accounts with zero trust? We can help assess your current state and build a roadmap tailored to your infrastructure. Schedule a free access review today and start protecting what matters most.

ABOUT SECURANCE

Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://securis.com/news/privileged-access-management/
2. https://sec.okta.com/articles/harfiles/
3. https://www.upguard.com/blog/what-caused-the-uber-data-breach
4. https://redriver.com/security/target-data-breach
5. https://delinea.com/blog/zero-trust?utm_source=chatgpt.com

Critical Access Under Fire

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com