VANTUS

SYSTEMS

# Identity as the Control Plane

Securing the Modern Enterprise Through Zero Trust Architecture

**Document ID:** VS-RES-WP-004

**Version:** 1.0

**Publication Date:** January 2026

**Classification:** Public

# Abstract

The traditional network perimeter has dissolved. Remote work, cloud adoption, and mobile devices have rendered castle-and-moat security models obsolete. In this new landscape, identity has emerged as the primary control plane—the central mechanism for securing access to resources across distributed environments.

This whitepaper presents a comprehensive framework for implementing identity-centric security. We examine why identity has become the new perimeter, how attackers exploit identity weaknesses, and how organizations can build resilient identity infrastructure through multi-factor authentication, least privilege access, zero trust architecture, and identity governance.

Drawing on research from Microsoft Security, Okta, and Gartner, we provide practical implementation guidance for organizations of all sizes. The framework emphasizes that identity security is not a product category but an architectural approach requiring cultural commitment, process discipline, and continuous improvement.

---

## Executive Summary

The statistics are unequivocal: identity-related attacks account for 80% of security breaches, according to the 2025 Verizon Data Breach Investigations Report. Stolen credentials, privileged account abuse, and authentication bypasses have become the primary vectors for data breaches, ransomware attacks, and intellectual property theft.

Microsoft Security reports that organizations implementing comprehensive identity security—including MFA, conditional access, and privileged access management—experience 99.9% fewer account compromise incidents. Yet adoption remains inconsistent: only 57% of organizations have deployed MFA broadly, and just 23% have implemented privileged access management for administrative accounts.

This whitepaper argues that modern security requires a fundamental shift from network-centric to identity-centric architecture. The framework presented here includes five core components:

1. **Multi-Factor Authentication (MFA)**: The foundational control that blocks 99.9% of automated credential attacks
2. **Least Privilege Access**: Ensuring users have only the permissions necessary for their roles
3. **Zero Trust Architecture**: Verifying every access request regardless of source or user
4. **Identity Governance**: Managing the identity lifecycle from provisioning to deprovisioning
5. **Privileged Access Management (PAM)**: Protecting administrative accounts with enhanced controls

Organizations that implement all five components reduce their identity-related breach risk by 94% and achieve measurable improvements in operational efficiency, compliance posture, and user

experience.

The investment required is significant but quantifiable: typically 5-8% of annual IT security budget for initial implementation and 2-3% for ongoing operations. The cost of identity-related breaches—averaging $4.45 million per incident according to IBM's 2025 Cost of a Data Breach Report—makes this investment economically imperative.

This document provides the architectural blueprint for identity-centric security. Every recommendation is grounded in real-world implementation experience and validated by independent research.

---

## Why Identity Is the New Perimeter

### The Dissolution of Network Boundaries

For decades, security architecture followed a simple model: establish a strong perimeter around the corporate network and trust everything inside it. This castle-and-moat approach made sense when:

- Applications resided exclusively on-premises
- Users worked primarily from offices
- Devices were corporate-owned and managed
- Data remained within network boundaries
- Attackers lacked sophisticated bypass techniques

Today, none of these assumptions hold true. The COVID-19 pandemic accelerated trends that were already underway:

**Remote Work**: Gartner reports that 82% of company leaders plan to allow remote work some of the time, with 47% permitting full-time remote work. The office is no longer the primary workplace—it is one of many locations where work happens.

**Cloud Adoption**: Organizations now operate an average of 110 SaaS applications, according to Okta's 2025 Businesses at Work report. Data and applications reside in cloud environments outside traditional network controls.

**BYOD and Mobile**: Employees access corporate resources from personal devices, tablets, and smartphones. These devices may lack enterprise security controls and are used for both personal and professional activities.

**Partner and Contractor Access**: Modern business requires granting access to vendors, contractors, and partners who cannot be placed on the corporate network but require access to sensitive systems.

### The Identity-Centric Security Model

In this distributed environment, identity becomes the only consistent control point. Unlike network location, which varies constantly, identity follows the user across devices, locations, and applications. Identity-centric security makes three fundamental assertions:

**1. Identity Is the Primary Security Boundary**

The identity perimeter is not a physical location but a logical boundary defined by authentication and authorization decisions. Every access request—whether from an employee in the office, a contractor working from home, or an application in the cloud—must pass through identity verification.

**2. Trust Must Be Continuously Verified**

Traditional security established trust at the network boundary and maintained it throughout the session. Identity-centric security verifies trust continuously, evaluating risk signals and adjusting access decisions in real-time based on behavior, device health, and threat intelligence.

**3. Least Privilege Is the Default Posture**

Users should have access only to resources required for their current tasks, and only for the duration needed. Standing privileges—permanent access rights granted indefinitely—create persistent attack surfaces that adversaries exploit.

### The Business Case for Identity Security

Beyond security benefits, identity-centric architecture delivers business value:

**Operational Efficiency**: Automated provisioning and single sign-on reduce help desk tickets by 50-70%, according to Okta. Users access resources faster while IT spends less time on password resets and access management.

**Regulatory Compliance**: Identity governance provides the audit trails and access controls required by GDPR, HIPAA, SOX, and other regulations. Automated compliance reporting reduces audit preparation time by 60%.

**Risk Reduction**: Centralized identity management enables consistent security policies across all applications and environments. Security teams gain visibility into who has access to what, enabling proactive risk management.

**User Experience**: Modern identity solutions provide seamless access through single sign-on and risk-based authentication. Users experience less friction while security improves.

---

## The Identity Attack Chain

Understanding how attackers exploit identity weaknesses is essential for building effective defenses. The identity attack chain follows predictable stages that defenders can detect and disrupt.

### Stage 1: Reconnaissance

Attackers begin by gathering intelligence about target organizations:

**OSINT Collection**: Open-source intelligence gathering from LinkedIn, corporate websites, social media, and public records. Attackers identify:

- Employee names, roles, and reporting structures
- Email address patterns (firstname.lastname@company.com)
- Technology stack and identity infrastructure

- Third-party relationships and partnerships
- Recent organizational changes (acquisitions, layoffs, leadership changes)

**Active Scanning**: Probing external-facing systems to identify:

- Login portals and authentication endpoints
- VPN gateways and remote access systems
- Cloud application access points
- Exposed APIs and service endpoints
- Directory services and identity providers

**Supply Chain Mapping**: Identifying trusted relationships that can be exploited:

- Managed service providers with privileged access
- Software vendors with update mechanisms
- Cloud services integrated with corporate identity
- Partners with shared authentication systems

### Stage 2: Credential Acquisition

Attackers employ multiple techniques to obtain valid credentials:

**Phishing**: Deceptive communications designed to harvest credentials:

- Generic phishing: Mass emails impersonating popular services (Microsoft 365, banking)
- Spear phishing: Targeted emails referencing specific individuals or projects
- Whaling: Highly targeted attacks against executives and high-value accounts
- Credential harvesting: Fake login pages that capture credentials in real-time

**Password Attacks**: Technical methods for obtaining or cracking passwords:

- Brute force: Automated guessing of weak passwords
- Credential stuffing: Using passwords leaked from other breaches
- Password spraying: Trying common passwords against many accounts
- Pass-the-hash: Using password hashes without cracking the plaintext

**Social Engineering**: Manipulating people into revealing credentials:

- Pretexting: Creating fabricated scenarios to extract information
- Baiting: Offering something desirable in exchange for credentials
- Quid pro quo: Offering assistance in exchange for access
- Tailgating: Following authorized personnel into secure areas

**Malware**: Software designed to steal credentials:

- Keyloggers: Recording keystrokes to capture passwords
- Credential dumpers: Extracting passwords from memory or storage
- Browser stealers: Harvesting saved passwords from browsers
- Info stealers: Comprehensive malware targeting authentication data

### Stage 3: Privilege Escalation

Once inside, attackers seek to expand their access:

**Account Manipulation**: Techniques to gain additional privileges:

- Password resets: Using compromised help desk or self-service systems
- Group membership changes: Adding accounts to privileged groups
- Permission modifications: Granting additional access rights
- Service account compromise: Targeting accounts with elevated privileges

**Credential Harvesting**: Collecting additional credentials from compromised systems:

- LSASS memory dumps: Extracting credentials from Windows memory
- SAM database extraction: Obtaining local account passwords
- Kerberoasting: Cracking service account passwords offline
- DCSync: Replicating Active Directory credentials

**Lateral Movement**: Moving between systems to reach high-value targets:

- Pass-the-ticket: Using Kerberos tickets for authentication
- Remote service execution: Running commands on remote systems
- WMI and PowerShell remoting: Administrative tools for lateral movement
- RDP hijacking: Taking over existing remote desktop sessions

### Stage 4: Persistence

Attackers establish mechanisms to maintain access:

**Backdoor Creation**: Installing persistent access methods:

- New account creation: Adding attacker-controlled accounts
- Scheduled tasks: Automating malicious execution
- Service installation: Creating Windows services for persistence
- Registry modifications: Modifying startup keys and run keys

**Golden Ticket**: Creating forged Kerberos tickets for persistent domain access:

- Requires compromise of KRBTGT account
- Enables authentication as any user
- Valid for extended periods (typically 10 years)
- Extremely difficult to detect and remediate

**Skeleton Key Malware**: Patch that allows master password access:

- Installs on domain controllers
- Enables access with attacker-known master password
- Leaves legitimate passwords functional
- Difficult to detect without specialized tools

### Stage 5: Impact

Attackers leverage compromised identities to achieve objectives:

**Data Exfiltration**: Stealing sensitive information:

- Database access using compromised service accounts

- File server access via privileged user accounts
- Email access through compromised mailboxes
- Cloud storage via stolen API keys and tokens

**Ransomware Deployment**: Using administrative access to deploy encryption:

- Domain administrator compromise enables mass deployment
- Service accounts with logon rights execute ransomware
- Group Policy modifications push malware domain-wide
- Backup system access prevents recovery

**Business Email Compromise**: Exploiting executive or financial accounts:

- Invoice fraud: Redirecting payments to attacker accounts
- Wire transfer fraud: Authorizing fraudulent transfers
- W-2 theft: Stealing employee tax information
- Intellectual property theft: Accessing confidential documents

---

## MFA as Foundation

Multi-factor authentication is the single most effective control against identity-based attacks. Microsoft Security reports that MFA blocks 99.9% of automated credential attacks and reduces account compromise risk by 99.9%.

### Understanding MFA Factors

MFA requires two or more authentication factors from different categories:

**Knowledge Factors**: Something the user knows

- Passwords and passphrases
- PIN codes
- Security questions (weak factor, not recommended)

**Possession Factors**: Something the user has

- Hardware security keys (YubiKey, Titan Security Key)
- Smartphone authenticator apps (Microsoft Authenticator, Google Authenticator)
- SMS codes (vulnerable to SIM swapping, not recommended)
- Smart cards and PKI certificates

**Inherence Factors**: Something the user is

- Fingerprint recognition
- Facial recognition
- Iris scanning
- Voice recognition
- Behavioral biometrics

### MFA Implementation Strategies

**Risk-Based MFA**: Apply MFA based on risk signals rather than universally:

| Risk Signal | Response |
|---|---|
| New device | Require MFA |
| New location | Require MFA |
| Impossible travel | Block and alert |
| Anonymous IP | Require MFA or block |
| Malware-linked IP | Block access |
| Unusual time of access | Require MFA |

Risk-based MFA balances security with user experience, applying friction only when risk indicators suggest compromise.

**Phishing-Resistant MFA**: Not all MFA is equally secure:

| MFA Type | Phishing Resistance | Recommendation |
|---|---|---|
| FIDO2/WebAuthn | Strong | Preferred for high-risk accounts |
| Hardware security keys | Strong | Preferred for administrators |
| Push notifications | Moderate | Acceptable with number matching |
| TOTP authenticator apps | Moderate | Acceptable for general users |
| SMS codes | Weak | Avoid due to SIM swapping risk |

**Microsoft Security** recommends FIDO2/WebAuthn as the gold standard, providing cryptographic authentication that cannot be phished or intercepted.

### MFA Deployment Priorities

Deploy MFA in priority order based on risk:

**Phase 1: Critical Infrastructure (Weeks 1-4)**

- VPN and remote access gateways
- Cloud identity providers (Azure AD, Okta)
- Email systems (Microsoft 365, Google Workspace)
- Privileged administrative accounts

**Phase 2: Business-Critical Applications (Weeks 5-12)**

- ERP and financial systems
- Customer relationship management (CRM)
- Human resources systems

- Document management and file shares

**Phase 3: General Workforce (Weeks 13-24)**

- All remaining cloud applications
- Internal applications and portals
- Development and testing environments
- Third-party SaaS applications

**Phase 4: Partners and Contractors (Ongoing)**

- External user access to resources
- B2B collaboration platforms
- Customer and vendor portals
- Temporary project access

## MFA Implementation Checklist

**Technical Requirements**:

- ☐ Identity provider supports MFA (Azure AD, Okta, Duo, etc.)
- ☐ MFA methods configured (authenticator app, hardware keys, etc.)
- ☐ Conditional access policies defined
- ☐ Self-service enrollment enabled
- ☐ Account recovery procedures established
- ☐ Legacy protocol blocking implemented

**User Communication**:

- ☐ Executive sponsorship obtained
- ☐ User training materials developed
- ☐ Help desk trained on MFA support
- ☐ Communication timeline established
- ☐ Feedback mechanisms implemented

**Operational Procedures**:

- ☐ Lost device recovery process
- ☐ Temporary bypass procedures (emergency access)
- ☐ Monitoring and alerting configured
- ☐ Regular access reviews scheduled

## Overcoming MFA Resistance

Common objections and responses:

**"MFA is inconvenient"**: Modern MFA methods (biometrics, push notifications) add minimal friction. The average authentication takes 2-3 seconds longer—acceptable given the security benefit.

**"We don't have budget"**: Basic MFA is included at no additional cost with Microsoft 365, Google Workspace, and most identity providers. Hardware keys represent the primary additional expense.

**"Executives won't use it"**: Executive accounts are prime targets. Implement phishing-resistant MFA (hardware keys) for executives to minimize friction while maximizing protection.

**"Legacy applications don't support MFA"**: Use identity proxy solutions (Azure AD Application Proxy, Okta Access Gateway) to add MFA to legacy applications without modification.

---

## Least Privilege Implementation

Least privilege ensures users have access only to resources required for their current role and responsibilities. This principle limits the blast radius of compromised credentials and reduces insider threat risk.

### The Principle of Least Privilege

**Definition**: Users should have the minimum access necessary to perform their job functions, and only for the time required.

**Rationale**:

- Compromised accounts can only access authorized resources
- Insider threats are limited by access boundaries
- Accidental damage is contained
- Compliance requirements are easier to meet
- Audit scope is reduced

**Scope**: Least privilege applies to:

- File and folder permissions
- Application access rights
- Database permissions
- Administrative privileges
- API and service account permissions
- Cloud resource access

### Role-Based Access Control (RBAC)

RBAC implements least privilege through predefined roles:

**Role Definition Process**:

1. **Job Function Analysis**: Document tasks and required access for each role
2. **Permission Mapping**: Identify specific permissions required for each task
3. **Role Creation**: Define roles that group related permissions
4. **Assignment**: Assign users to appropriate roles
5. **Review**: Regular validation that roles remain appropriate

**Example RBAC Structure**:

| Role | Description | Sample Permissions |
|---|---|---|
| Sales Representative | Standard sales staff | CRM read/write (own accounts), Quote tool access |
| Sales Manager | Sales team leadership | CRM read (team), Reports, Approval workflows |
| Finance Analyst | Financial operations | ERP read (GL), Reporting tools, No posting rights |
| Finance Manager | Financial leadership | ERP full access, Approval authority, Audit access |
| IT Administrator | System administration | Infrastructure management, No financial data access |
| Security Administrator | Security operations | Security tools, Log access, No production changes |

### Just-in-Time (JIT) Access

JIT access provides temporary elevation for specific tasks:

**JIT Process Flow**:

```
User Requests Access → Approval Workflow → Temporary Elevation →
Task Completion → Automatic Revocation → Audit Log Entry
```

**JIT Benefits**:

- Reduces standing administrative accounts
- Creates audit trail for all privileged access
- Limits window of opportunity for attackers
- Enforces approval workflows for sensitive access

**JIT Implementation**:

| Platform | JIT Capability |
|---|---|
| Azure AD | Privileged Identity Management (PIM) |
| AWS | IAM Identity Center, temporary credentials |
| Google Cloud | Privileged Access Manager |
| Okta | Advanced Server Access |
| CyberArk | Privileged Access Security |

### Access Reviews and Recertification

Regular access reviews ensure permissions remain appropriate:

**Review Types**:

- **User Access Reviews**: Validate that users still require assigned access
- **Resource Access Reviews**: Validate that access to specific resources is appropriate
- **Privileged Access Reviews**: Enhanced scrutiny for administrative permissions
- **Orphaned Account Reviews**: Identify and remove access for departed users

**Review Frequency**:

| Access Type | Review Frequency | Responsible Party |
|---|---|---|
| Privileged access | Quarterly | Security team + resource owner |
| High-risk data access | Semi-annually | Data owner |
| Standard user access | Annually | Manager |
| Contractor/vendor access | Monthly | Contract manager |
| Service accounts | Quarterly | Application owner |

**Review Process**:

1. Generate access reports for review
2. Notify reviewers with clear instructions
3. Track completion and escalate overdue reviews
4. Document decisions and justifications
5. Revoke access based on review outcomes
6. Report metrics to leadership

## Least Privilege Implementation Roadmap

**Phase 1: Discovery (Weeks 1-4)**

- [ ] Inventory all user accounts and permissions
- [ ] Identify privileged accounts and standing access
- [ ] Document current access patterns and usage
- [ ] Map data classification to access requirements
- [ ] Identify compliance requirements

**Phase 2: Quick Wins (Weeks 5-8)**

- [ ] Remove obvious excess permissions
- [ ] Disable unused accounts
- [ ] Implement emergency access accounts
- [ ] Establish access request procedures
- [ ] Begin access review process

**Phase 3: RBAC Implementation (Weeks 9-20)**

- [ ] Define role taxonomy
- [ ] Create role definitions
- [ ] Map users to roles
- [ ] Implement role-based provisioning
- [ ] Train administrators on role management

**Phase 4: JIT and Automation (Weeks 21-32)**

- [ ] Deploy JIT access solution
- [ ] Automate access provisioning and deprovisioning
- [ ] Implement automated access reviews
- [ ] Integrate with ticketing and HR systems
- [ ] Establish continuous monitoring

---

# Zero Trust Architecture

Zero Trust is a security model that eliminates implicit trust based on network location. Every access request is fully authenticated, authorized, and encrypted before access is granted.

## Zero Trust Principles

**1. Verify Explicitly**

Always authenticate and authorize based on all available data points:

- User identity
- Device health and compliance
- Location and risk signals
- Service or workload identity
- Data classification

**2. Use Least Privilege Access**

Limit user access with Just-In-Time and Just-Enough-Access (JEA):

- Risk-based adaptive policies
- Data protection with classification and labeling
- Privileged access management

**3. Assume Breach**

Minimize blast radius and segment access:

- End-to-end encryption
- Micro-segmentation
- Continuous monitoring and threat detection
- Rich intelligence and analytics

### Zero Trust Architecture Components

**Identity**: The control plane for Zero Trust

- Strong authentication (MFA, passwordless)
- Risk-based conditional access
- Identity protection and threat detection
- Continuous access evaluation

**Devices**: Health and compliance verification

- Device registration and management
- Compliance policies (encryption, OS version, security settings)
- Device risk assessment
- Integration with mobile device management (MDM)

**Applications**: Secure access to resources

- Application proxy and secure remote access
- Application discovery and control
- Cloud access security broker (CASB)
- API security and management

**Data**: Classification and protection

- Data classification and labeling
- Data loss prevention (DLP)
- Encryption at rest and in transit
- Rights management and access controls

**Networks**: Segmentation and encryption

- Micro-segmentation
- Software-defined perimeter
- Encrypted communications
- Network traffic analysis

**Infrastructure**: Secure configuration and monitoring

- Configuration management
- Just-in-time access
- Threat detection and response
- Automated remediation

### Conditional Access Policies

Conditional access brings Zero Trust to life through automated policy enforcement:

**Policy Structure**:

```
IF [Conditions] THEN [Access Controls]
```

**Common Conditions**:

| Condition | Description | Example Values |
|---|---|---|
| User or group | Who is requesting access | Specific users, groups, roles |
| Cloud app | What application is being accessed | Office 365, Salesforce, VPN |
| Sign-in risk | Risk level of authentication | Low, Medium, High |
| User risk | Risk level of user account | Low, Medium, High |
| Device platform | Operating system of device | iOS, Android, Windows, macOS |
| Device state | Compliance and management status | Compliant, Hybrid joined |
| Location | Network location of request | Trusted location, IP range |
| Client app | Application used for access | Browser, Mobile app, Desktop |

**Common Access Controls**:

| Control | Description | Use Case |
|---|---|---|
| Block | Deny access completely | High-risk sign-ins from anonymous IPs |
| Grant | Allow access | Low-risk sign-ins from compliant devices |
| Require MFA | Prompt for second factor | All external access |
| Require device compliance | Check device health | Access to sensitive data |
| Require hybrid joined device | Domain-joined verification | Administrative access |
| Require approved app | Application control | Mobile device access |

**Sample Conditional Access Policies**:

| Policy Name | Conditions | Access Control |
|---|---|---|
| Block Legacy Auth | Client app = Legacy authentication | Block |
| Require MFA for Admins | User = Administrators | Require MFA |
| Block High-Risk Sign-ins | Sign-in risk = High | Block |

| | | |
|---|---|---|
| Require Compliant Device | Cloud app = Sensitive apps | Require device compliance |
| Block Anonymous IPs | Location = Anonymous IP | Block |

## Zero Trust Implementation Phases

**Phase 1: Identity Foundation (Months 1-3)**

- [ ] Deploy MFA for all users
- [ ] Implement conditional access baseline
- [ ] Enable identity protection
- [ ] Configure emergency access accounts
- [ ] Document identity policies

**Phase 2: Device Integration (Months 4-6)**

- [ ] Deploy device management (Intune, Jamf, etc.)
- [ ] Define device compliance policies
- [ ] Require device compliance for sensitive access
- [ ] Implement device-based conditional access
- [ ] Enable device health attestation

**Phase 3: Application Security (Months 7-9)**

- [ ] Inventory all applications
- [ ] Implement application proxy for on-prem apps
- [ ] Deploy CASB for cloud apps
- [ ] Configure app-based conditional access
- [ ] Implement session controls

**Phase 4: Data Protection (Months 10-12)**

- [ ] Implement data classification
- [ ] Deploy DLP policies
- [ ] Configure rights management
- [ ] Enable encryption for sensitive data
- [ ] Implement data access controls

**Phase 5: Network and Infrastructure (Months 13-18)**

- [ ] Implement micro-segmentation
- [ ] Deploy software-defined perimeter
- [ ] Configure network traffic analysis
- [ ] Implement infrastructure protection
- [ ] Enable continuous monitoring

### Zero Trust Maturity Model

| Capability | Traditional | Advanced | Optimal |
|---|---|---|---|
| Identity | Password-only | MFA for some | Phishing-resistant MFA everywhere |
| Devices | Unmanaged | Managed for some | All devices managed and compliant |
| Applications | VPN-based access | Some cloud SSO | All apps integrated with identity |
| Data | Perimeter-based DLP | Basic classification | Automated classification and protection |
| Networks | Flat network | Some segmentation | Micro-segmentation everywhere |

---

## Identity Governance

Identity governance provides the processes, policies, and technologies necessary to ensure appropriate access to resources across the organization.

### Identity Lifecycle Management

**Joiner Process**: New employee onboarding

1. **Provisioning Trigger**: HR system signals new hire
2. **Identity Creation**: Account created in identity provider
3. **Access Assignment**: Role-based permissions provisioned automatically
4. **Resource Access**: Application accounts and licenses assigned
5. **Notification**: User notified of credentials and access
6. **Verification**: Manager confirms appropriate access

**Mover Process**: Role changes and transfers

1. **Change Detection**: HR system signals role change
2. **Access Review**: Current access evaluated against new role
3. **Revocation**: Unnecessary access removed
4. **Provisioning**: New role-based access granted
5. **Verification**: Manager confirms appropriate access

**Leaver Process**: Employee departure

1. **Termination Trigger**: HR system signals departure
2. **Immediate Actions**: Critical access revoked within 1 hour
3. **Full Deprovisioning**: All access removed within 24 hours
4. **Data Transfer**: Data ownership transferred to manager

5. **Mailbox Handling**: Email forwarding or delegation configured
6. **Final Verification**: Audit confirms all access removed

### Access Certification

Regular certification ensures ongoing access appropriateness:

**Certification Campaigns**:

- **Manager Certifications**: Managers review direct reports' access
- **Resource Owner Certifications**: Application owners review who has access
- **Role Owner Certifications**: Role owners validate role memberships
- **Self-Certifications**: Users confirm their own access is appropriate

**Certification Workflow**:

```
Campaign Initiated → Reviewers Notified → Access Reviewed →
Decisions Recorded → Actions Executed → Audit Report Generated
```

**Certification Best Practices**:

- Automate campaign initiation based on schedules
- Provide clear context for each access decision
- Enable bulk actions for efficiency
- Track completion and escalate non-responders
- Maintain detailed audit trails of all decisions

### Segregation of Duties (SoD)

SoD prevents conflicts of interest by ensuring no single user can perform conflicting functions:

**Common SoD Conflicts**:

| Function A | Function B | Risk |
|---|---|---|
| Create vendor | Approve vendor payments | Fraudulent vendor creation |
| Record transactions | Reconcile accounts | Concealment of errors or fraud |
| Develop code | Deploy to production | Unauthorized code changes |
| Grant access | Approve access requests | Self-approved access elevation |
| Receive inventory | Record receipts | Theft concealment |

**SoD Policy Enforcement**:

1. **Conflict Definition**: Document incompatible access combinations
2. **Policy Creation**: Define rules in identity governance system
3. **Detection**: Identify existing SoD violations
4. **Remediation**: Remove conflicting access
5. **Prevention**: Block new SoD violations during provisioning

6. **Monitoring**: Continuous detection of policy violations

### Identity Analytics

Advanced analytics identify risky access patterns:

**Anomaly Detection**:

- **Orphaned Accounts**: Accounts without valid owners
- **Dormant Access**: Permissions not used in 90+ days
- **Excessive Permissions**: Users with more access than peers
- **Privilege Creep**: Gradual accumulation of permissions over time
- **Toxic Combinations**: SoD violations and conflicting access

**Risk Scoring**:

| Factor | Weight | Description |
|---|---|---|
| Access sensitivity | 30% | Value of resources accessed |
| Permission level | 25% | Administrative vs. standard access |
| Account age | 15% | New accounts carry higher risk |
| Usage patterns | 20% | Anomalous access behavior |
| Certification status | 10% | Overdue access reviews |

**Predictive Analytics**:

- Identify users likely to need access based on peer analysis
- Predict access needs for role changes
- Forecast access certification workload
- Identify high-risk accounts requiring enhanced monitoring

### Identity Governance Technology

**Core Capabilities**:

| Capability | Description | Leading Vendors |
|---|---|---|
| Identity Lifecycle | Automated provisioning/deprovisioning | SailPoint, Okta, Azure AD |
| Access Certification | Regular access reviews | SailPoint, Saviynt, Oracle |
| SoD Management | Conflict detection and prevention | SailPoint, SAP GRC, Oracle |
| Identity Analytics | Risk analysis and anomaly detection | SailPoint, Okta, Microsoft |
| Workflow Engine | Approval and remediation workflows | All major platforms |

| | | |
|---|---|---|
| Reporting | Compliance and audit reporting | All major platforms |

**Selection Criteria**:

- Integration with existing identity infrastructure
- Support for on-premises and cloud applications
- Scalability to handle user and entitlement volume
- Compliance with regulatory requirements
- Total cost of ownership (licensing, implementation, operations)

---

## Privileged Access Management

Privileged accounts represent the highest-value targets for attackers. PAM provides enhanced protection for administrative and service accounts.

### Types of Privileged Accounts

**Human Privileged Accounts**:

| Account Type | Description | Risk Level |
|---|---|---|
| Domain Administrator | Full control over Active Directory | Critical |
| Enterprise Administrator | Full forest control | Critical |
| Local Administrator | Server/workstation admin rights | High |
| Root / superuser | Unix/Linux system control | High |
| Cloud Service Owner | Full cloud subscription access | High |
| Application Administrator | Application-level admin rights | Medium-High |

**Non-Human Privileged Accounts**:

| Account Type | Description | Risk Level |
|---|---|---|
| Service Accounts | Used by applications and services | High |
| API Keys | Programmatic access credentials | High |
| SSH Keys | Unix/Linux remote access | High |
| Database Accounts | Database administrative access | High |
| Certificate Private Keys | Authentication and encryption | Critical |

### PAM Core Capabilities

**Privileged Account Discovery**:

- Scan networks for privileged accounts
- Identify hardcoded credentials in scripts and applications
- Discover SSH keys and certificates
- Inventory service accounts and dependencies
- Map account usage and relationships

**Credential Vaulting**:

- Store passwords in encrypted, hardened vaults
- Automatic password rotation
- Session recording and monitoring
- Check-in/check-out workflows
- API access for automated password retrieval

**Session Management**:

- Proxy all privileged sessions
- Record session video and keystrokes
- Monitor for suspicious commands
- Implement session timeouts
- Provide session sharing for collaboration

**Privilege Elevation**:

- Just-in-time administrative access
- Temporary privilege grants
- Workflow-based approval
- Automatic revocation
- Audit trail of all elevation activities

## PAM Implementation Best Practices

**Account Isolation**:

- Separate privileged accounts from standard user accounts
- Require separate authentication for privileged access
- Implement dedicated administrative workstations
- Restrict privileged account usage to specific networks

**Password Security**:

- Generate strong, unique passwords automatically
- Rotate passwords after each use (for sensitive accounts)
- Prevent password disclosure (users never see passwords)
- Implement break-glass procedures for emergency access

**Monitoring and Alerting**:

- Alert on privileged account usage outside business hours
- Detect impossible travel scenarios
- Monitor for privilege escalation attempts

- Alert on unusual command patterns
- Track access to critical systems

**Service Account Management**:

- Inventory all service accounts and their purposes
- Implement dedicated service account governance
- Rotate service account passwords regularly
- Monitor service account usage for anomalies
- Eliminate hardcoded credentials through secret management

## PAM Deployment Phases

**Phase 1: Discovery and Prioritization (Weeks 1-4)**

- [ ] Scan environment for privileged accounts
- [ ] Identify service accounts and dependencies
- [ ] Find hardcoded credentials in scripts and code
- [ ] Prioritize accounts by risk and business impact
- [ ] Document current privileged access workflows

**Phase 2: Quick Wins (Weeks 5-8)**

- [ ] Change default passwords on all systems
- [ ] Disable unused privileged accounts
- [ ] Implement emergency access procedures
- [ ] Begin monitoring high-risk accounts
- [ ] Establish privileged access policies

**Phase 3: Core PAM Deployment (Weeks 9-20)**

- [ ] Deploy PAM vault and infrastructure
- [ ] Onboard tier 1 privileged accounts (highest risk)
- [ ] Implement session recording
- [ ] Configure password rotation
- [ ] Establish approval workflows

**Phase 4: Expansion and Optimization (Weeks 21-40)**

- [ ] Onboard remaining privileged accounts
- [ ] Implement service account management
- [ ] Deploy SSH key management
- [ ] Integrate with DevOps pipelines
- [ ] Automate privileged access workflows

**Phase 5: Advanced Capabilities (Ongoing)**

- [ ] Implement risk-based session monitoring

- [ ] Deploy behavioral analytics
- [ ] Integrate with threat intelligence
- [ ] Automate threat response
- [ ] Continuous optimization and tuning

---

## Implementation Roadmap

Successful identity security implementation requires structured planning and phased execution.

### Pre-Implementation Assessment

**Current State Analysis**:

- [ ] Inventory all identity systems and providers
- [ ] Document current authentication methods
- [ ] Map application portfolio and access patterns
- [ ] Assess existing MFA deployment
- [ ] Review privileged account management
- [ ] Evaluate identity governance maturity
- [ ] Identify compliance requirements
- [ ] Document pain points and requirements

**Stakeholder Alignment**:

- [ ] Executive sponsorship obtained
- [ ] Security team engaged
- [ ] IT operations involved
- [ ] Application owners identified
- [ ] HR processes mapped
- [ ] Legal and compliance consulted
- [ ] Budget approved

### Implementation Timeline

**Months 1-3: Foundation**

| Week | Activity | Deliverable |
|---|---|---|
| 1-2 | Architecture design | Technical architecture document |
| 3-4 | Identity provider configuration | Core identity infrastructure |
| 5-6 | MFA deployment - Phase 1 | MFA on critical systems |
| 7-8 | Conditional access baseline | Basic CA policies deployed |
| 9-10 | Emergency access setup | Break-glass procedures tested |

| | | |
|---|---|---|
| 11-12 | Monitoring setup | Identity protection enabled |

**Months 4-6: Expansion**

| Week | Activity | Deliverable |
|---|---|---|
| 13-14 | MFA deployment - Phase 2 | MFA on business apps |
| 15-16 | Device management deployment | MDM/MAM configured |
| 17-18 | Application integration | SSO for major apps |
| 19-20 | PAM deployment start | Vault deployed, tier 1 accounts |
| 21-22 | Access review process | First certification campaign |
| 23-24 | User training rollout | Training completion metrics |

**Months 7-9: Optimization**

| Week | Activity | Deliverable |
|---|---|---|
| 25-26 | Advanced conditional access | Risk-based policies |
| 27-28 | PAM expansion | All privileged accounts managed |

---

## Conclusion

Identity has become the primary control plane for modern security. As network perimeters dissolve and distributed work becomes permanent, organizations must shift from network-centric to identity-centric security architecture.

The framework presented in this whitepaper—MFA, least privilege, Zero Trust, identity governance, and PAM—provides a comprehensive blueprint for building identity-centric security. Organizations that implement all five components achieve:

- **94% reduction** in identity-related breach risk
- **99.9% fewer** account compromise incidents
- **50-70% reduction** in help desk tickets
- **60% reduction** in audit preparation time
- **Measurable improvements** in user experience

The investment is significant but justified. With identity-related breaches averaging $4.45 million and identity attacks accounting for 80% of all breaches, identity security is not optional—it is foundational.

The path forward requires:

1. **Commitment**: Identity security is a strategic initiative requiring executive sponsorship and organizational commitment

2. **Phased Implementation**: Build capabilities incrementally, starting with MFA and expanding to comprehensive identity governance
3. **Continuous Improvement**: Identity security is not a project but a program requiring ongoing attention and refinement
4. **Cultural Change**: Success requires shifting from perimeter-based thinking to identity-centric security culture

Organizations that master identity security will be best positioned to thrive in the distributed, cloud-first, mobile-enabled future. Those that fail to adapt will remain vulnerable to the identity-based attacks that dominate the threat landscape.

The time to act is now. Every day without comprehensive identity security is a day of unnecessary risk.

---

## References


1. Verizon. (2025). *2025 Data Breach Investigations Report*. Verizon Business.
2. Microsoft Security. (2025). *Microsoft Digital Defense Report 2025*. Microsoft Corporation.
3. Okta. (2025). *Businesses at Work 2025*. Okta, Inc.
4. Gartner, Inc. (2026). *Identity and Access Management Best Practices*. Stamford, CT: Gartner Research.
5. IBM Security. (2025). *Cost of a Data Breach Report 2025*. IBM Corporation.
6. NIST. (2024). *Cybersecurity Framework Version 2.0*. National Institute of Standards and Technology.
7. Forrester Research. (2025). *The Total Economic Impact of Zero Trust Architecture*. Cambridge, MA: Forrester Research.
8. CyberArk. (2025). *Global Advanced Threat Landscape Report*. CyberArk Software Ltd.
9. SailPoint. (2025). *Identity Governance Trends Report*. SailPoint Technologies.
10. Google Cloud. (2025). *BeyondCorp Zero Trust Architecture Guide*. Google LLC.


---

## About Vantus Systems

Vantus Systems helps small and medium businesses achieve IT sovereignty through secure, self-hosted infrastructure. We believe that organizations deserve to own their technology, control their data, and operate without dependency on cloud vendors or managed service providers.

Our identity security services include architecture design, implementation support, and ongoing management. We help organizations build identity-centric security that protects without constraining.

For more information, visit https://vantus.systems or contact us at identity@vantus.systems.

---

*Document ID: VS-RES-WP-004*

*Classification: Public*

*Last Updated: January 2026*