WHITESWAN
IDENTITY SECURITY

MFA Bypass Defense & Lateral Movement Protection

Eliminating Post-Authentication Blind Spots

The Problem

MFA Stops at the Front Door

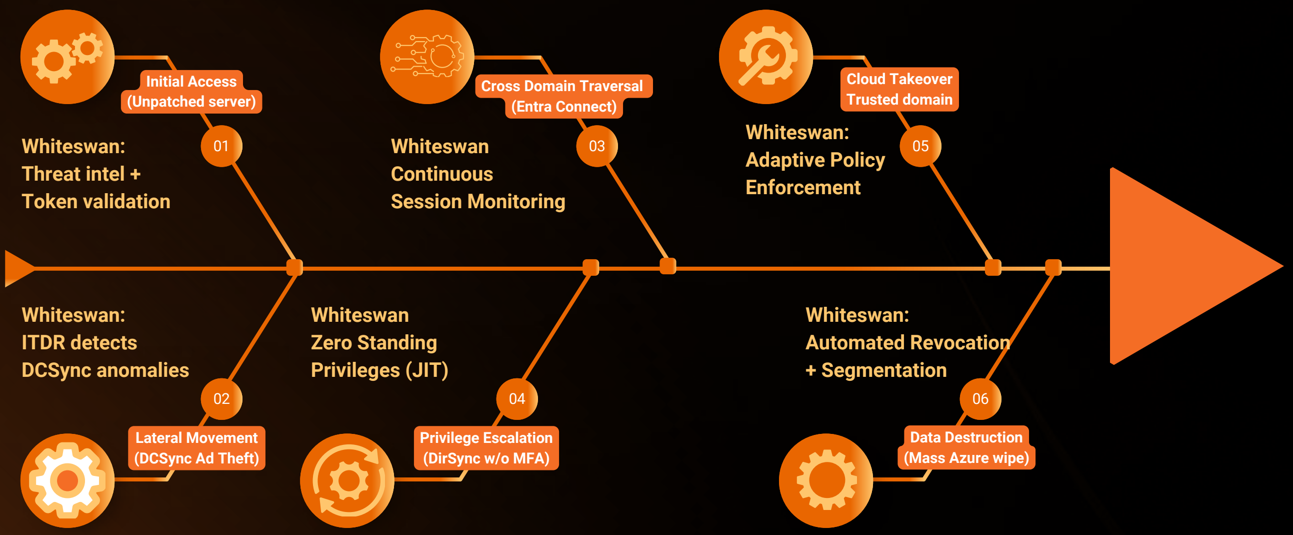
87% of cyberattacks in 2024 involved session hijacking after valid MFA logins

while 70% leveraged lateral movement once inside. Traditional MFA protects the front door but leaves hallways and side-doors exposed—session tokens, legacy systems, service accounts, and trust relationships.

Business Impact

Average breach cost $4.88M, 6-month recovery times. Move budget from "more MFA prompts" to post-authentication controls that shrink blast radius and eliminate persistence.

Storm-0501 Kill Chain Example (Aug 2025)


Initial Access (Unpatched server)
01
Whiteswan: Threat intel + Token validation
Cross Domain Traversal (Entra Connect)
03
Whiteswan Continuous Session Monitoring
Cloud Takeover Trusted domain
05
Whiteswan: Adaptive Policy Enforcement
Whiteswan: ITDR detects DCSync anomalies
02
Lateral Movement (DCSync Ad Theft)
Whiteswan Zero Standing Privileges (JIT)
04
Privilege Escalation (DirSync w/o MFA)
Whiteswan: Automated Revocation + Segmentation
06
Data Destruction (Mass Azure wipe)

Why Whiteswan?

Whiteswan secures the post-MFA environment with **identity-first Zero Trust** controls that defend where attackers actually move

1 Session Hijacking Prevention

Anchor sessions to TPM/passkey-protected devices, making stolen tokens useless

2 Identity-First Zero Trust

Continuous authentication across sessions, not just login prompts

3 Blast Radius Containment

Zero Standing Privileges shrink the space attackers can move, eliminating lateral pathways

4 Trust Path Protection

Monitor and harden hybrid relationships (AD ↔ Entra ↔ SaaS) preventing cross-environment pivots

5 Service & Machine Identity Governance

Secure non-human accounts that create invisible backdoors

Core Capabilities

Comprehensive Lateral Movement Detection

- Session anchoring to TPM/passkey-protected devices preventing token theft
- Behavioral baselines identifying compromised accounts before damage occurs
- Active Directory attack surface hardening – Prevent DCSync, Golden/Silver Ticket attacks, and privilege escalations
- Service account governance with ownership assignment and automated rotation
- Trust path monitoring (NTLM/Kerberos) with policy enforcement preventing protocol abuse
- Hybrid environment mapping revealing and securing cross-domain attack pathways

Zero Trust Access Control - Lateral Movement Prevention

- Just-in-Time privilege elevation with time-boxed access
- Identity-based network segmentation per application and resource
- Continuous session validation replacing point-in-time authentication
- Automated threat response for token revocation and forced re-authentication
- Cross-platform coverage including legacy Windows Server 2003-2012

Business Outcomes

Metric	Improvement
Threat Detection	*Hours to detect and stop threats (vs. industry average 287 days)*
Lateral Movement	*Containment of successful breach attempts within initial access point*
Authentication Friction	*Reduced prompts for legitimate users through risk-based policies*
Recovery Time	*Faster incident response through automated session termination*
Compliance	*Comprehensive audit trails for SOC2/HIPAA/GDPR requirements*

Industry Implementation Priorities

Manufacturing

IT/OT bridge security, production system access control

Healthcare

Legacy medical device protection, EHR system segmentation, vendor access control

Government

Continuous verification for classified access, advanced threat detection

Financial Services

Hybrid cloud trust boundary management, regulatory compliance automation

Technical Requirements

Supported Environments

Windows 7-11, Server 2003-2022 | Linux (RHEL, Ubuntu, CentOS) | macOS | Active Directory, Entra ID, Okta | AWS, Azure, GCP, hybrid

Deployment Model

Agentless API integration | <100ms authentication decisions | 99.9% SLA | Linear scaling 1K-100K+ identities

30-Day Implementation

Week 1	Identity discovery and risk baseline
Week 2	Passwordless authentication pilot with risk-based policies
Week 3	Just-in-Time privileges for critical roles
Week 4	Threat detection activation with automated response

Outcome

Reduced lateral movement, faster threat containment, decreased authentication friction, higher stakeholder confidence.

WHITESWAN
IDENTITY SECURITY

Whiteswan delivers an identity-first defense against MFA bypass and lateral movement.

Ready to Defend Beyond MFA?

Whiteswan closes the post-MFA security gap — stopping attackers where they move laterally, not just where they initially authenticate.

- **Free Security Assessment:** Identify MFA coverage gaps and lateral movement risks
- **30-Day Pilot Program:** Deploy core capabilities in your most critical environment
- **ROI Analysis:** Calculate savings from reduced breach risk and faster incident response

Learn More: www.whiteswansecurity.com
Contact: vmamidi@whiteswansecurity.com

Whiteswan Identity Security - Comprehensive post-authentication protection for hybrid enterprise environments