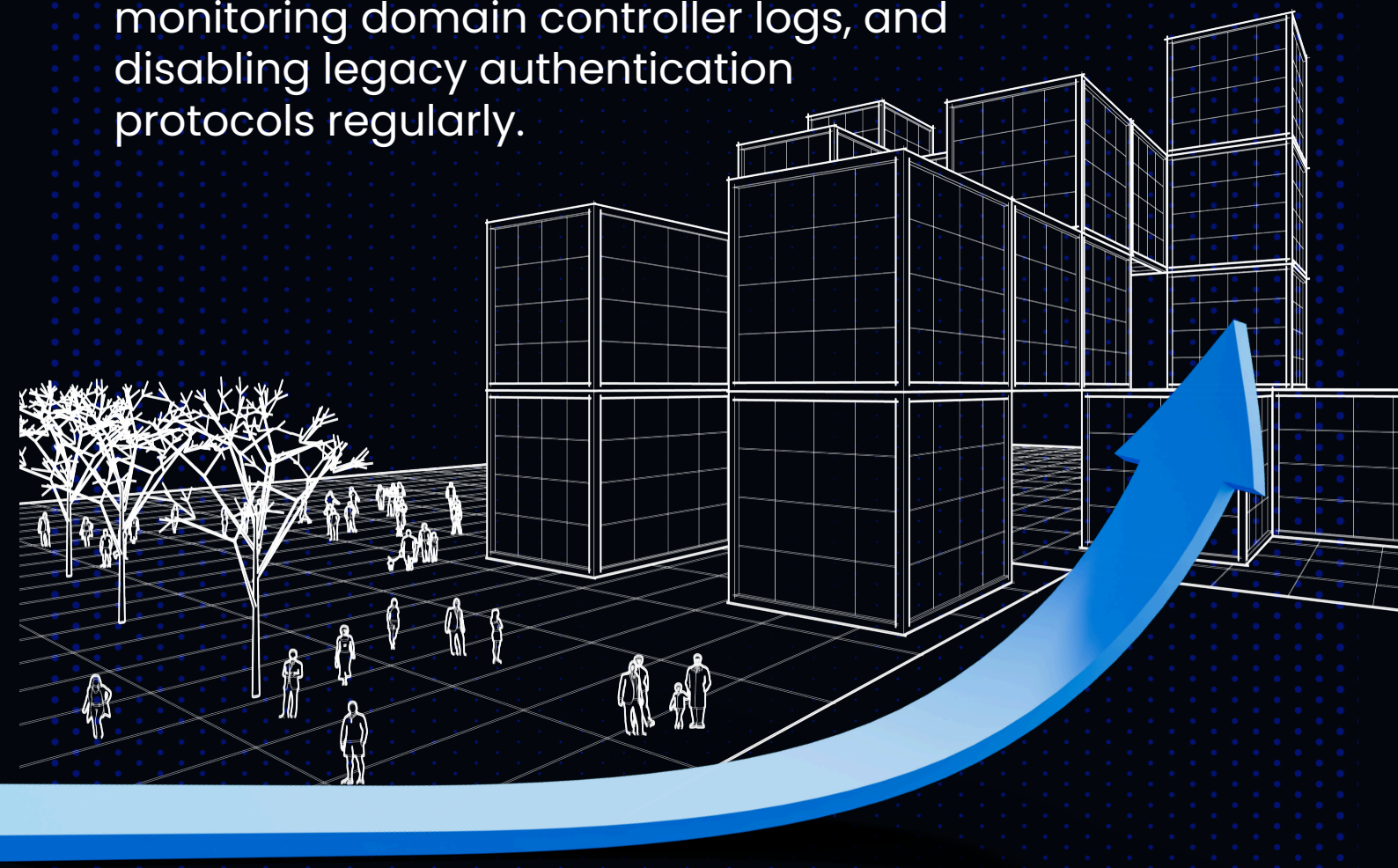
ACTONIX

ACTONIX FOR ACTIVE DIRECTORY

Strengthen Active Directory by enforcing least privilege, rotating service account credentials, monitoring domain controller logs, and disabling legacy authentication protocols regularly.



Highlights

- Advanced AD Security Assessment (MITRE ATT&CK® Mapped)
- Core AD Management & Automation
- Real-Time Change Auditing & Forensic Visibility

ACTONIX

Advanced AD Security Assessment (MITRE ATT&CK® Mapped)

Transform your audit logs into actionable threat intelligence with a security layer specifically designed to thwart sophisticated identity-based attacks.

150+ Security-Focused Reports: A deep library of reports categorized by risk level, targeting vulnerabilities in protocols, configurations, and user behaviors.

MITRE ATT&CK® Framework Mapping: Every security report and alert is mapped to specific MITRE techniques (e.g., T1558 - Steal or Forge Kerberos Tickets, T1484 - Domain Policy Modification). This allows security teams to visualize their defensive coverage against known adversary tactics.

Threat Detection Indicators: Identify early signs of reconnaissance and lateral movement, such as DCSync attacks, Golden Ticket creation, and Kerberoasting attempts.

Vulnerability Heatmaps: Visualize "hot spots" in your AD environment where misconfigurations (like unconstrained delegation or circular nested groups) create the highest risk.

ACTONIX

Core AD Management & Automation

Unified Dashboard: Manage users, groups, and OUs without toggling between multiple legacy MMC consoles.

Automated Lifecycle Management: Rule-based onboarding and offboarding that ensures users have the right access from day one and zero access upon departure.

Bulk Administration: Execute mass password resets, attribute updates, or group membership changes in seconds.

SSPR & Account Unlock: A self-service portal that empowers users while maintaining strict security verification via Multi-Factor Authentication (MFA).

Real-Time Change Auditing & Forensic Visibility

Continuous Monitoring: Track every change to AD objects and Group Policy with the essential Who, What, When, and Where context.

Before/After Values: Instant visual comparison of attribute changes to identify exactly what was modified.

Logon Intelligence: Complete visibility into successful and failed logins, including source IP, workstation name, and authentication protocol (NTLM vs. Kerberos).

ACTONIX

State Analysis & Rapid Recovery

Configuration Snapshots: Regularly capture the "state" of your AD, including GPOs and permissions, to establish a secure baseline.

Drift Analysis: Compare current settings against any historical snapshot to detect unauthorized "shadow" changes.

Object & Attribute Rollback: Undo accidental deletions or unauthorized changes instantly, ensuring 99.9% uptime for identity services.

Compliance & Strategic Reporting

Regulatory Alignment: Automated reporting templates for GDPR, HIPAA, PCI-DSS, SOX, and DPDP Act (Digital Personal Data Protection).

Executive Dashboards: High-level security posture overviews for CISOs and IT Directors, alongside granular technical logs for SysAdmins.

Automated Distribution: Schedule reports to be delivered to compliance officers, auditors, or security teams on a recurring basis.