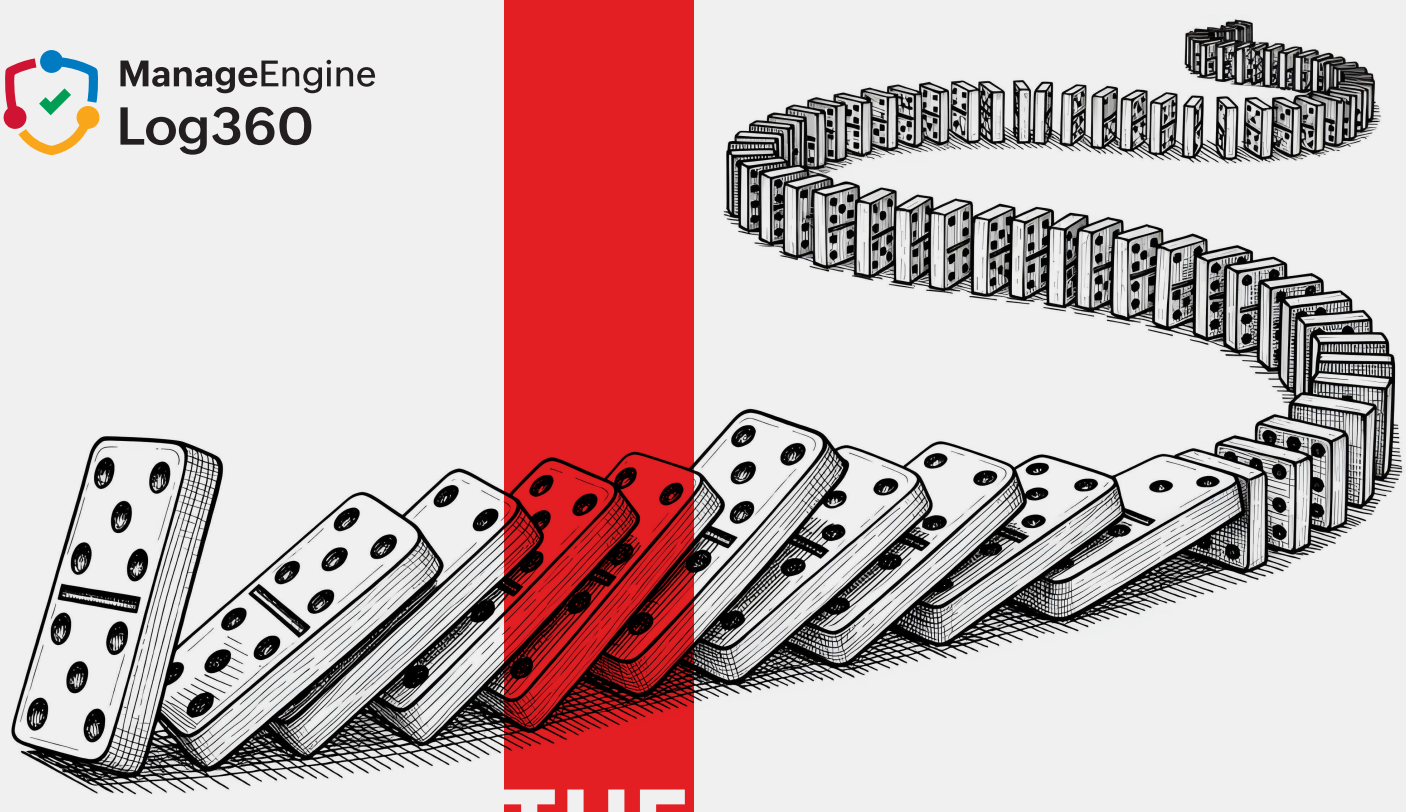
ManageEngine
Log360



THE DOMINO EFFECT:

How small changes can undermine Active Directory security and enterprise resilience

01 Small AD change introduced

Example:
User added to privileged group / password set to never expire.

Without IAM:
Misconfiguration goes unnoticed.

With IAM:
Automated provisioning and deprovisioning ensures proper role alignment, blocking risky changes.

02 Misconfiguration goes undetected

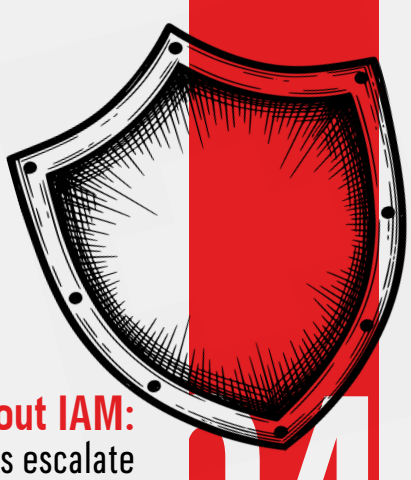
Without IAM:
Creates hidden Active Directory vulnerabilities.

With IAM:
Change auditing and real-time alerts detect and report risky modifications immediately.

03 Vulnerability becomes exploitable

Without IAM:
Attackers exploit privilege creep, shadow admins, or weak policies.

With IAM:
RBAC + Privileged access management (PAM) enforce least privilege and JIT access, removing standing admin rights.



04 Attack escalates (Lateral movement)

Without IAM:
Attackers escalate privileges and move laterally across systems.

With IAM:
Password policy enforcement + self-service resets eliminate weak credentials, cutting off lateral movement opportunities.

05 Domino effect across enterprise

Without IAM:
Leads to ransomware spread, outages, compliance violations.

With IAM:
Access reviews + compliance reporting + executive dashboards give CISOs visibility, ensure governance, and prevent cascading failures.

FINAL OUTCOME:

Without IAM:
Small AD change
↓
Domino effect
↓
Breach.

With IAM:
Controls, visibility, and automation break the chain, keeping **Active Directory security** intact.

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

Get in touch with our product demo experts for a free demo.

SIGN UP FOR A DEMO ▶