ManageEngine
AD360

Inside a global hospitality chain data breach

How years of undetected access and identity sprawl

exposed 300M+ guest records

The numbers that shocked the hospitality industry

300M+	4 years	$52M+
Guest records exposed	Attackers remained undetected	Regulatory settlement and remediation costs

The merger mess

M&A created identity sprawl and unmanaged accounts.

Dormant privileged accounts remain active.

Attackers move laterally for years undetected.

Hundreds of millions of guest records stolen.

One of the largest hospitality breaches in history.

What actually happened

STEP 1

Identity sprawl after acquisition

A global hospitality chain acquired another major hotel group for billions of dollars, inheriting massive guest databases and two separate AD environments. Legacy directories, service accounts, and access policies were never fully consolidated.

> **The vulnerability:** M&A-driven identity sprawl created blind spots. Inconsistent provisioning, orphaned accounts, and unmanaged service identities gave attackers more doors than security teams knew existed.

STEP 2

Dormant and over-privileged accounts persisted

Two years before the deal closed, attackers had already breached the acquired hotel chain's reservation system. Inherited along with it were stale accounts, unused admin credentials, and privileged group memberships nobody owned. Cleanup never happened because integration took priority over access governance.

> **The critical failure:** Inactive and over-privileged accounts inflated the attack surface and gave attackers persistent footholds. With no periodic access review, dormant identities looked like noise instead of standing risk.

STEP 3

Long-term undetected access and lateral movement

Using inherited credentials, attackers moved quietly through the merged hospitality environment for nearly four years, escalating privileges and pivoting to the guest reservation database.

> **The escalation:** Without behavioral baselines, abnormal logons—at odd hours, from new machines, by long-dormant accounts—blended into normal traffic. There was no signal separating a real admin from an attacker imitating one.

STEP 4

Massive data exfiltration

When the breach surfaced, attackers had exfiltrated personal data on an estimated 300 to 500 million guests, including names, addresses, passport numbers, payment card data, and reservation details.

The outcome:

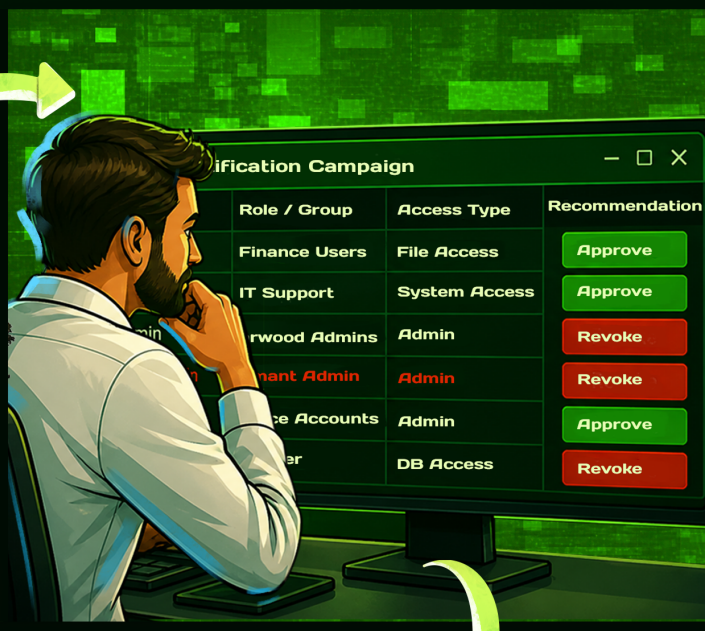
An £18.4M fine, $52M settlement, and class-action litigation across multiple jurisdictions. The company had no idea who held privileged access in its own environment for four straight years.

The root cause

Identity and access sprawl across merged environments without centralized governance, automation, and reporting.

No zero-day. No advanced exploit.
Just compromised access and invisible privilege.

The merger managed



What if AD360 was deployed?

STEP 1

Automated identity life cycle governance across merged environments

AD360's IGA component, ADManager Plus, automates provisioning, deprovisioning, and access assignment across hybrid AD environments using templates, HR-driven workflows, and identity orchestration.

> **How it helps:** At acquisition, every inherited identity would be mapped, standardized, or disabled based on policy. The attacker footholds inherited through the acquisition would be deprovisioned during integration, not preserved for four years.

STEP 2

Access certification validates every inherited privilege

ADManager Plus has access certification campaigns that let managers and security teams periodically review and recertify access. Smart recommendations flag excessive or unusual permissions based on peer comparison and behavioral baselines.

> **How it stops the attack:** Every inherited group membership and NTFS permission is reviewed by an accountable owner. Users outside their role's peer group are flagged for revocation. Recertification runs on schedule with audit trails. Dormant admin accounts fail recertification and get revoked—removing the exact accounts attackers were riding on.

STEP 3

Risk exposure management surfaces hidden attack paths

ADManager Plus has risk exposure management that continuously analyzes AD groups, nested memberships, and delegation chains to visualize real-world attack paths to sensitive data.

> **How it helps:** Excessive admin rights and risky delegations are flagged with remediation suggestions.
>
> The exact route attackers used:
> **legacy account → privileged group → reservation system**, would be flagged as critical attack path and severed before exploitation.

STEP 4

UBA detects lateral movement and dormant account reactivation

AD360 applies machine learning to build behavioral baselines for every user—logon times, machines accessed, files touched. Deviations trigger real-time alerts that plain auditing misses.

How it helps: Dormant account activity, first-time access to new systems, unusual logon patterns, and abnormal data access volumes are flagged in real time, raising risk scores and triggering alerts. The moment a long-inactive account reactivates or behaves abnormally, security teams are immediately notified—collapsing the attacker's stealth window.

STEP 5

Breach prevented, guest data protected

With AD360's layered governance and behavioral monitoring, the inherited attacker footholds would have been closed within weeks of acquisition

The result:

- ✓ No dormant access surviving the acquisition
- ✓ Every inherited privilege validated through access certification
- ✓ Attack paths visualized and severed before exploitation
- ✓ Lateral movement and anomalous logons detected in real time
- ✓ Years of silence replaced by continuous visibility
- ✓ 500M+ guest records protected
- ✓ £18.4M fine and $52M settlement avoided

The business case

Without AD360 (The reality)

- $72M+ in direct costs (£18.4M fine + $52M settlement)
- 4 years of undetected attacker access
- 300M+ guest records exposed
- Passport and payment data compromised
- Lasting brand and trust damage in a loyalty-driven industry
- Stock price impact and shareholder lawsuits

With AD360 (The alternate timeline)

- Inherited access closed within weeks of acquisition
- Zero dormant accounts surviving the merger
- Attack paths severed before exploitation
- Guest data—including passports and payment cards—protected
- Regulatory fines and settlements avoided
- Customer trust and loyalty preserved
- Security posture strengthened across merged environments

ROI insight

Preventing a single breach of this magnitude pays for identity governance investments many times over.

- $52M+ penalties vs. fractional IAM deployment cost
- 4 years undetected access vs. real-time visibility
- Reactive forensics vs. proactive attack-path remediation

1 prevented identity governance gap = 1,000× ROI potential

Lessons from the hospitality data breach

M&A inherits identity debt	Acquisitions bring legacy accounts, directories, and privileges that quietly expand the attack surface.
Dormant accounts are prebuilt backdoors	Stale identities gave attackers years of unmonitored access.
Privileged access without governance is a time bomb	Nobody knew who held admin rights across merged environments.
Auditing without behavior analytics is blind	Four years of anomalous activity went unflagged.
Attack paths form silently	Nested groups and inherited permissions create routes attackers walk undetected.
Periodic access reviews aren't optional	Privileges accumulated for years without recertification.
Detection delay is the real damage multiplier	Four years of dwell time turned a breach into a historic exposure.

Identity governance strategies every organization needs

Standardize and consolidate identities post-M&A	Eliminates inherited sprawl and orphaned accounts.
Automate stale account cleanup and privilege revocation	Removes persistent footholds at the source.
Run access certification campaigns on schedule	Validates every privilege under an accountable owner.
Map and remediate AD attack paths continuously	Severs privilege chains before exploitation.
Apply UBA to detect lateral movement and dormant account reactivation	Flags anomalies plain auditing misses.
Enforce least privilege through role-based access	Prevents privilege creep across merged environments.
Maintain compliance-ready audit trails	Supports HIPAA, PCI DSS, SOX, and GDPR investigations.
Monitor privileged groups with tighter controls	Detects unauthorized escalation in real time.

Don’t let identity sprawl expose your customer data

Talk to an expert

Our Products

ADManager Plus | ADAudit Plus | ADSelfService Plus | Exchange Reporter Plus | RecoveryManager Plus

AD360 | Log360 | EventLog Analyzer | DataSecurity Plus | M365 Manager Plus

ManageEngine
AD360

ManageEngine AD360 is a unified identity platform that seamlessly connects people, technology, and experiences while giving enterprises full visibility and control over their identity infrastructure. It offers automated life cycle management; secure SSO; adaptive MFA; and risk-based governance, auditing, compliance, and identity analytics—all from a single, intuitive console. With extensive out-of-the-box integrations and support for custom connectors, AD360 easily integrates into existing IT ecosystems to enhance security and streamline identity operations. Trusted by leading enterprises across healthcare, finance, education, and government, AD360 simplifies identity management, fortifies security, and ensures compliance with evolving regulatory standards. For more information, please visit https://www.manageengine.com/active-directory-360/.

$ Get Quote Download