ManageEngine
AD360

The truth behind the largest-ever casino attack

How social engineering and identity gaps led to a **$100M+ disruption**

The numbers that shook the house

$100M+	10 days	10 mins
Total estimated losses	Casino operations disrupted	Time taken by attackers to gain access

Chaos in the casino

Public employee data became an attack blueprint.

A convincing call led to a password reset.

Stolen credentials enabled lateral movement.

Ransomware shut down MGM operations.

10 days of chaos and $100M+ in losses.

What actually happened

STEP 1

Social media reconnaissance

The attackers scoured social media to identify the casino's IT help desk employees and gather information about its organizational structure, internal terminology, and employee names.

> **The vulnerability:** Publicly available employee information became a weapon. Attackers knew exactly who to impersonate and which systems to target.

STEP 2

The social engineering call

Armed with employee details, attackers called the casino's IT help desk pretending to be a legitimate employee who had forgotten their password. The call lasted approximately 10 minutes.

> **The critical failure:** The help desk reset the password based on information the attacker had gathered from public sources—no robust identity verification was required.

STEP 3

Credential takeover

With the reset password, attackers gained access to the employee's account and privileges within the organization's network, including access to critical systems.

> **The escalation:** Once inside with legitimate credentials, the attackers moved laterally through the network without triggering security alerts. They appeared as a normal user.

STEP 4

Ransomware deployment

Using the compromised credentials, the attackers deployed ransomware across the organization's systems, encrypting critical data and shutting down major operations.

Operations impacted

- Hotel room key card systems
- Casino slot machines
- Reservation systems
- Internal communications
- Point-of-sale terminals

The aftermath

- Casino refused to pay the ransom
- Operations disrupted for 10 days
- Guests locked out of rooms
- Casino floors shut down
- Over $100 million in losses reported

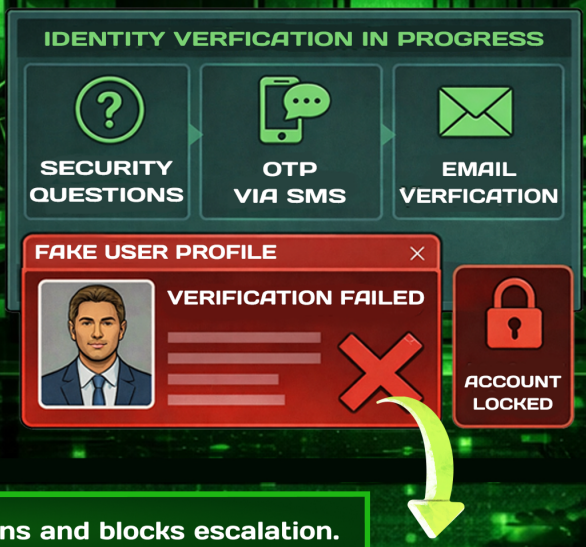
The root cause

A weak password reset process that relied on easily obtainable information allowed attackers to socially engineer their way past the front door. No technical exploit was needed—just a convincing phone call.

Silencing the sirens

Self-service password reset removes the helpdesk attack vector

MFA-based identity verification blocks social engineering.



Adaptive MFA detects risky logins and blocks escalation.

Real-time alerts stop the attack before ransomware deployment.

Attack stopped at identity layer–MGM operates without disruption.

What if AD360 was deployed?

STEP 1

Self-service removes the help desk attack vector

AD360's security component, ADSelfService Plus, has a self-service password reset portal which eliminates the need for employees to call the help desk for password resets entirely.

> **How it protects:** With no help desk involvement required, there's no human to socially engineer. Attackers can't call and impersonate employees because password resets happen through a secure, automated portal.

STEP 2

MFA for password resets

Even if an attacker somehow accesses the self-service portal, AD360 requires multiple forms of identity verification before allowing a password reset.

> **How it protects:** Social media profiles and public information aren't enough to prove an identity. AD360 requires:
>
> - ✓ Answers to personalized security questions (set by the user).
> - ✓ One-time passwords sent to registered mobile devices.
> - ✓ Email verification to registered corporate email addresses.
> - ✓ Biometric verification options (e.g., fingerprint, face recognition).
>
> **What happens:** Without the employee's physical device or biometric data, attackers can't complete the login.

STEP 3

Adaptive MFA for risky logins

Once passwords are reset, AD360's security module, ADSelfService Plus, enforces adaptive MFA for all subsequent login attempts, especially for suspicious activity.

> **AD360 requires:**
>
> - ✓ Mandatory second-factor authentication (e.g., authenticator app, push notification, biometric).
> - ✓ Risk-based authentication that flags unusual login locations or devices.
> - ✓ Step-up authentication for accessing sensitive systems.

What happens: Without the employee's physical device or biometric data, attackers can't complete the login.

STEP 4

Real-time audit trails

ADSelfService Plus logs and reports all reset and login activity.

How it protects: Alerts enable security teams to detect anomalous resets and logins (e.g., new location or device, repeated failures) and block compromised accounts before lateral movement.

STEP 5

Attack prevented, operations continue

With AD360's layered security approach, potential attackers are stopped at every turn.

The result:

- ✓ No help desk social engineering possible
- ✓ No unauthorized password resets
- ✓ No compromised credentials
- ✓ No network access
- ✓ No ransomware deployment
- ✓ Uninterrupted operations
- ✓ $100M+ in losses prevented

The business case

Without AD360 (The casino's reality)

- $100M+ in direct losses
- 10 days of operational disruption
- Immeasurable reputational damage
- Customer trust erosion
- Regulatory scrutiny and potential fines
- Stock price impact

With AD360 (The alternate timeline)

- Attack prevented at entry point
- Zero operational disruption
- No ransom payment
- Customer trust maintained
- Security posture strengthened
- Competitive advantage in security-conscious market

ROI insight

Preventing a single identity-driven ransomware incident delivers exponential ROI.

- $100M+ impact vs. fractional IAM deployment cost
- 10 days downtime vs. zero downtime with identity controls
- Millions spent in recovery vs. automated prevention

1 blocked identity attack = 1,000× ROI potential

Lessons from the casino cyberattack

Help desk is a critical attack surface	Attackers used social engineering to trick IT support into resetting credentials.
MFA isn't enough without strong verification	Weak identity checks allowed attackers to bypass protections.
Identity is the new perimeter	There were no exploits—just impersonation and access abuse.
Privileged access accelerates damage	Attackers quickly escalated access across systems.
IT attacks disrupt real-world operations	Hotels, casinos, payments, and room access were affected.
Lateral movement amplifies impact	Interconnected systems made it easier to spread disruption.
Downtime is costly	Even without paying ransom, operational losses were massive.
Reputation takes a hit fast	Customer trust and brand image suffered immediately.

Best practices to defend against ransomware attacks

Strengthen help desk identity verification	Prevents attackers from impersonating employees during password resets.
Enforce phishing-resistant MFA (FIDO2, biometrics)	Reduces risk of MFA bypass through social engineering.
Implement least privilege access controls	Limits how far attackers can move after initial access.
Monitor and alert on unusual account changes	Detects suspicious password resets, MFA changes, or privilege escalations.
Apply adaptive authentication for high-risk actions	Adds extra verification for sensitive operations like account recovery.
Log and audit all identity-related events	Enables rapid detection and forensic investigation.
Segment critical systems	Prevents attackers from easily moving across business-critical environments.
Use real-time threat detection and response	Reduces attacker dwell time and limits damage.

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