ManageEngine
AD360

Inside a large-scale media industry data breach

How stolen employee credentials and a spear **phishing email led to the industry's biggest cybersecurity disaster**

The numbers that shook the entertainment industry

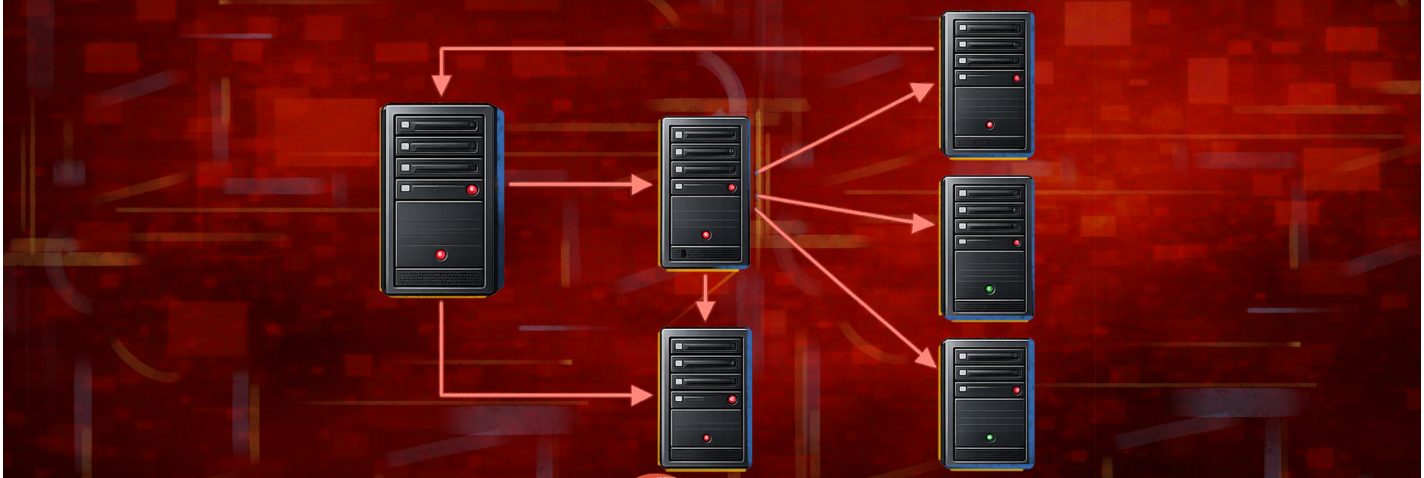
100TB+	$15M+	45%
Data stolen	Estimated total damages	Employees' personal records exposed

The day the screens went dark

Highly targeted phishing emails tricked employees into handing over credentials.

One stolen password opened the network – more credentials lay exposed inside.

Attackers moved as trusted admins, spreading silently through the network.



100TB of sensitive data was quietly siphoned out over weeks.

Wiper malware erased systems – bringing operations to a standstill.

What actually happened

STEP 1

Spear phishing for credentials

Attackers sent highly targeted spear phishing emails impersonating Apple, Google, and Facebook aimed specifically at employees of a large entertainment company with broad network access, including system engineers and SCCM administrators. Employees were tricked into entering their credentials on fake login pages.

> **The vulnerability:** Employees had no MFA protecting their accounts. A convincing fake email was all it took to hand over the keys to the media houses' entire network.

STEP 2

Credentials harvested, network door opened

Using the stolen login credentials, attackers accessed the studios' internal network. The malware embedded in the studio's systems already contained server names and administrator credentials—confirming that the attackers had done deep reconnaissance before striking.

> **The critical failure:** Passwords stored in unsecured spreadsheets and text documents on the studio's own servers handed attackers escalated access without any additional effort.

STEP 3

Lateral movement through the network

Armed with legitimate credentials, attackers moved laterally across the network for weeks undetected. They used stolen System Center Configuration Manager (SCCM) credentials, which gave them software distribution rights across the entire enterprise.

> **The escalation:** The attackers appeared as legitimate administrators. Malware was distributed to the media houses' devices through SCCM—the same channel used for legitimate software updates—making it virtually invisible to security teams.

STEP 4

Mass data exfiltration

Over an estimated two months of undetected access, attackers quietly exfiltrated over 100TB of data—unreleased content, confidential executive emails, employee Social Security numbers (SSNs), salaries, medical records, contracts, and scripts.

Data compromised:

- Unreleased content
- Private executive emails
- Salary data
- Employee SSNs
- Medical records
- Insurance information
- Business contracts
- Scripts
- Strategic documents
- Network credentials
- System configuration

STEP 5

Malware deployed, systems destroyed

The cyber attackers deployed a destructive wiper malware that overwrote the master boot record of thousands of the company machines, rendering them permanently inoperable. Employees arrived at work to find blank screens and their files gone.

Systems impacted

- Corporate workstations and servers across the enterprise
- Internal communications and email systems
- Content production and distribution infrastructure
- HR and financial management systems
- IT administrative tools and backup systems

The aftermath

- Massive operational disruption
- Global media fallout
- Sensitive data leaked publicly
- Enterprise-wide system shutdown
- Multi-million-dollar recovery costs
- Production halted across the enterprise

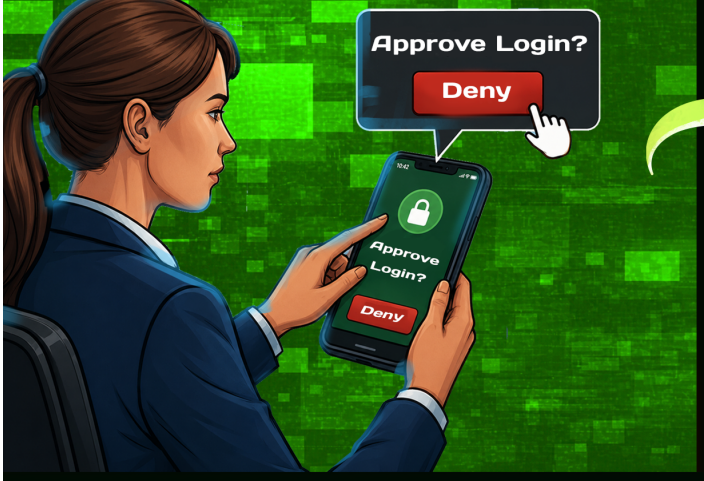
The root cause

Stolen credentials from a phishing email, stored in plain-text files on the media houses' own servers—no MFA, no anomaly detection, no access controls to stop lateral movement.

This attack happened with no zero-day exploits. No sophisticated network breach. Just stolen passwords and a complete lack of identity security.

Keeping the cameras rolling

Phishing fails – stolen passwords are useless without MFA.



No exposed credentials – passwordless authentication eliminate risky storage.

Suspicious logins are flagged and blocked instantly.

Even admin accounts require verification – no unauthorized escalation

Anomalies are detected early – stopping breaches before damage begins.

What if AD360 was deployed?

STEP 1

Phishing-resistant MFA stops credential theft at the source

AD360's security component, ADSelfService Plus, supports phishing-resistant FIDO2 authentication and enforces MFA across endpoints, enterprise applications, and email—making stolen passwords alone worthless.

> **How it helps:** Even if employees enter credentials on a fake phishing page, attackers can't proceed without the second factor—a push notification, OTP, biometric, or hardware token that only the legitimate user possesses. The credential theft yields nothing.

STEP 2

Passwordless authentication eliminates stored credentials entirely

ADSelfService Plus enables passwordless authentication using FIDO2 passkeys, biometrics, smart cards, and authenticator apps—removing passwords as a factor altogether.

> **How it helps:** With no passwords to store, there are no credentials to steal, reuse, or expose in spreadsheets or documents. Even if attackers gain access to internal files, there are no plaintext passwords or reusable secrets available.

STEP 3

Conditional access blocks suspicious logins in real time

AD360's security component ADSelfService Plus, evaluates every login attempt using risk-based, adaptive MFA—analyzing IP address, geolocation, device, time of access, and behavioral patterns to detect anomalies instantly.

> **How it helps:** Logins from unrecognized devices or locations—such as an attacker accessing the media houses' SCCM from an unknown endpoint—trigger step-up authentication or automatic blocks, stopping lateral movement before it begins.

STEP 4

Privileged account protection locks down high-value credentials

AD360 enforces device-based MFA and role-based conditional access for privileged accounts, including system engineers, network administrators, and SCCM operators.

How it helps: With AD360, even a correctly entered administrator password triggers additional verification—making stolen privileged credentials unusable without the legitimate user's second factor.

STEP 5

Built-in reports and audit trails

Every authentication event—successful or failed—is logged and monitored. AD360's security component ADSelfService Plus, generates instant reports for anomalous access patterns, new device logins, and unusual authentication attempts.

How it helps: With AD360, security teams get visibility into suspicious behavior, enabling faster detection and response before mass exfiltration begins.

The result:

- Phishing emails yield no usable credentials
- Stolen passwords cannot authenticate without MFA
- Privileged lateral movement is blocked at every step
- Anomalous access is detected and stopped in real time
- No data exfiltration. No wiper malware. No shutdown.

The business case

Without AD360 (The studio's reality)

- $150M+ in total estimated damages
- 100TB of sensitive data stolen and published online
- Unreleased content leaked, causing millions in lost revenue
- Thousands of employees' personal data exposed
- Long-term reputational and stock damage to the media house

With AD360 (The alternate timeline)

- Stolen credentials rendered useless
- Zero data exfiltrated
- No wiper malware deployment
- No content leaks or production disruption
- Employees' personal data remains protected
- Full operational continuity maintained

ROI insight

Preventing a single breach of this scale pays for decades of identity security investment.

- $150M+ in damages vs. fractional IAM deployment cost
- 2+ months of undetected access vs. real-time anomaly detection
- 100TB of stolen data vs. zero exfiltration with MFA enforcement
- Class action lawsuits vs. zero legal exposure
- 1 blocked phishing attempt = incalculable ROI

Lessons from the media house cyberattack

Phishing is still the #1 entry point	A convincing fake email handed attackers the keys to a $70B company's network.
Credentials stored in plaintext are credentials waiting to be stolen	The media houses' own servers contained administrator passwords in text documents and spreadsheets.
No MFA means stolen passwords are all an attacker needs	There was no second factor standing between the attacker and enterprise-wide access.
Privileged accounts are the ultimate target	SCCM administrator credentials gave attackers software distribution rights across the entire company.
Undetected dwell time is the real damage multiplier	Two months of silent access turned a breach into a catastrophe.
Identity-based access looks legitimate	Attackers moved freely because they had real credentials, not because they bypassed firewalls.
Data at rest without access controls is data already stolen	Sensitive files accessible to anyone with a valid login are never truly secure.

Best practices to defend against credential-based attacks

Enforce phishing-resistant MFA across all endpoints, applications, and email	Make stolen credentials completely useless.
Implement passwordless authentication	Close the easiest door attackers walk through (credential exploitation).
Apply conditional access based on device, location, and behavioral signals	Catch attackers even when they have valid passwords.
Protect privileged and administrator accounts with device-based and role-based MFA	Your highest-access accounts are your highest-value targets.
Monitor every authentication event with real-time alerts and audit logs	Detect and respond before dwell time means damage.
Enable secure self-service password reset with identity verification	Eliminate the need for credentials ever to be stored insecurely.
Enforce least-privilege access and automate account controls	what stolen credentials can actually reach.

Don't let one phishing email rewrite your company's story

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