ManageEngine
AD360

Inside one of largest pipeline breaches

How a single compromised password led to a
$4.4 million ransom and national crisis

The numbers that shocked critical infrastructure

$4.4M	6 days	45%
Ransom paid	Shutdown duration	East coast fuel supply affected

The day the pipes ran dry

What actually happened

STEP 1

Compromised credentials

Attackers gained access to the pipeline's VPN using a compromised password for a legacy account. The account had no MFA enabled.

> **The vulnerability:** One stolen password was enough to access critical infrastructure systems.

STEP 2

VPN access granted

Using the compromised credentials, attackers logged into the pipeline's VPN, gaining remote access to the corporate network.

> **The critical failure:** No MFA enforcement on VPN access meant stolen credentials worked without additional verification.

STEP 3

Lateral movement

Once inside, attackers moved laterally through the network, escalating privileges and identifying critical systems. This access ultimately enabled affiliates of DarkSide—a ransomware-as-a-service group known for targeting large enterprises—to prepare the environment for attack.

> **The escalation:** The attackers appeared as legitimate users, blending into normal activity without triggering alerts.

STEP 4

Ransomware deployment

DarkSide deployed ransomware, encrypting corporate IT systems and forcing the organization to shut down pipeline operations as a precaution.

> **The outcome:** Critical systems were locked, operations halted, and the organization was forced into a high-pressure decision between prolonged disruption and paying the ransom.

STEP 5

Cascading impact

The incident escalated beyond IT systems into the physical world, disrupting fuel distribution. Long queues formed at gas stations, media coverage intensified, and emergency measures were introduced to stabilize supply.

> **The ripple effect:** Widespread service disruption, public anxiety, regulatory response, and a lasting wake-up call for critical infrastructure cybersecurity.

Systems impacted

- Billing and business systems
- Operational monitoring systems
- Internal communications
- Supply chain coordination tools

The aftermath:

- Fuel shortages
- Panic buying
- National security concerns
- $4.4M ransom payment

The root cause

A single account with a reused or leaked password and no MFA protection opened the door.

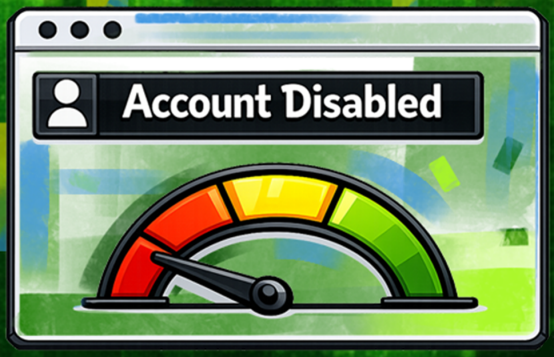
- No exploit
- No zero-day
- Just weak identity security

Keeping the pipes flowing

Strong password politics stop weak credentials.

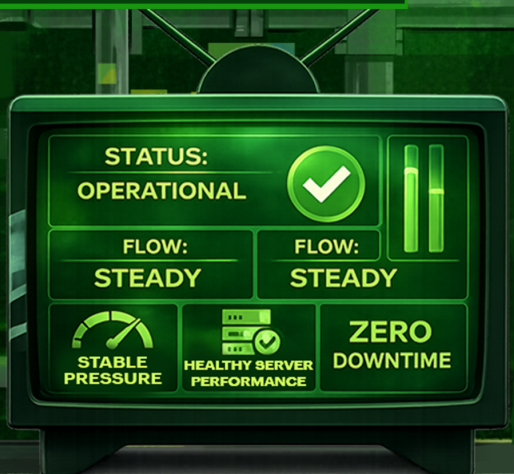
VPN MFA blocks stolen passwords.

Risky login triggers step-up authentication.



Instant alerts and audit trails enable fast action.

Pipeline stays operational. Zero downtime.



What if AD360 was deployed?

STEP 1

Strong password hygiene from day one

AD360's security component ADSelfService Plus, enforces strong password policies and enables secure self-service resets, reducing weak and reused passwords that often get leaked or sold.

> **How it stops the attack:** Compromised or reused passwords would be replaced with strong, policy-compliant credentials, closing the initial entry point.

STEP 2

Mandatory MFA for VPN and remote access

ADSelfService Plus, enforces MFA for VPN, endpoints, and cloud apps.

> **How it stops the attack:** Even with the correct password, attackers can't log in without the second factor (push notification, OTP, biometric, or token).

STEP 3

Adaptive MFA for suspicious logins

ADSelfService Plus has risk-based authentication which flags logins from new locations, devices, or unusual times.

> **How it stops the attack:** Suspicious VPN logins trigger step-up authentication or are blocked and alerted.

STEP 4

Built-in reports

Every authentication event is logged, enabling businesses to audit authentication activity, detect suspicious access patterns, and ensure compliance with security policies.

> **How it stops the attack:** Security teams detect and disable compromised accounts before lateral movement begins.

STEP 5

Attack prevented, Colonial Pipeline stays online

Layered identity security stops attackers at the perimeter—before ransomware deployment.

The result:

- ✓ No unauthorized VPN access
- ✓ No operational shutdown
- ✓ No ransom payment

The business case

Without AD360 (The pipeline's reality)

- $4.4M ransom payment
- Nationwide fuel shortages
- Regulatory scrutiny
- Congressional hearings
- Long-term reputational damage

With AD360 (The alternate timeline)

- Attack blocked at VPN login
- Zero operational downtime
- No ransom payment
- Public trust maintained
- Stronger security posture

ROI insight

Preventing a single ransomware incident in critical infrastructure pays for identity security investments many times over.

- $4.4M+ ransom vs. fractional IAM deployment cost
- Six days downtime vs. zero downtime with MFA enforcement
- Millions in recovery costs vs. automated prevention
- One blocked attack = 1,000 × ROI potential

Lessons from the pipeline ransomware attack

Passwords without MFA are an open door	A single stolen credential led to a shut down in critical infrastructure
Remote access is the new perimeter	VPN accounts are high-value targets for ransomware groups
Legacy and dormant accounts are dangerous	Old accounts often lack modern security controls
Credential theft beats malware	Attackers didn't hack systems; they logged in
Lateral movement starts with identity	Legitimate credentials let attackers blend in undetected
Business systems are critical systems	IT disruption forced OT shutdowns
Identity visibility is essential	Suspicious logins went unnoticed until it was too late

Best practices to defend against credential-based attacks

Enforce MFA across VPN, endpoints, and cloud apps	Blocks access with stolen credentials
Use strong passwords and prevent reuse	Reduces credential compromise risk
Remove or secure legacy and inactive accounts	Eliminates hidden entry points
Monitor and detect anomalous login activity	Flags suspicious access in real time
Apply adaptive authentication for risky logins	Adds extra verification when needed
Maintain detailed authentication logs	Enables quick detection and investigation
Enable secure self-service password reset	Improves password hygiene safely
Automate account lockouts and access controls	Stops attacks before escalation

Don’t let a single password shut down your operations

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