InfoTank
I.T. DONE BETTER

CASE STUDY



How Our Security Tool, **Account Compromise Protection (ACP),** Detected and Stopped a Compromise Before Damage Was Done.

THE SITUATION

Our security tool, Account Compromise Protection (ACP), detected suspicious activity on the CEO's Microsoft 365 account from multiple locations and an unmanaged device without MFA, creating a serious risk of financial fraud or Business Email Compromise.

WHAT WE DISCOVERED

- The compromised account belonged to the organization's CEO
- Multiple successful sign-ins from datacenter IPs within minutes
- Access from an unmanaged macOS device using a browser
- No Multi-Factor Authentication (MFA) was satisfied
- Malicious inbox rules were created to hide and move emails to a hidden folder
- Concealment targeted specific senders and keywords
- Hundreds of failed sign-in attempts from countries worldwide (password spray / credential stuffing)

ACTIONS TAKEN

- Investigated alerts, sign-in logs, and mailbox activity
- Removed malicious inbox rules and reviewed mailbox
- Forced sign-out of all active sessions
- Reset password and re-enrolled MFA
- Monitored the account and tenant for additional activity
- Notified and educated the user

THE POWER OF ACP

Without ACP, an attacker could have remained undetected inside the CEO's account, hiding emails and potentially committing financial fraud.

ACP provided early visibility and rapid alerting so we could stop the threat before damage occurred.

INCIDENT OVERVIEW

DATE DETECTED
August 18, 2026

INDUSTRY
Non-profit/ Public and Social Service

POTENTIAL LOSS
Business Email Compromise, Financial Fraud, Data Loss, Downtime, and Reputational Damage

SEVERITY
High

THE IMPACT

Threat actor detected before email fraud or financial loss could occur.

Unauthorized access stopped and account secured.

Business operations continued with no disruption.

Early detection saved time, resources, and potential recovery costs.

KEY TAKEAWAY

Account compromises are often invisible until damage is done. Our security tool, ACP, continuously monitors for suspicious behavior across your Microsoft 365 and SaaS environment-giving you the visibility you need to stop threats early and protect what matters most.

WHAT COULD HAVE HAPPENED

- Hidden emails could have enabled wire fraud or vendor changes.
- Business Email Compromise (BEC) could have resulted in financial loss.
- Continued access could have led to data theft or unauthorized forwarding.
- Damage to reputation, client trust, and operational disruption.
- Longer detection time could have meant higher recovery costs.

We invest in leading cybersecurity tools to help protect your people, data, and business.

www.infotank.com | 770-450-8783 | ali@infotank.com