

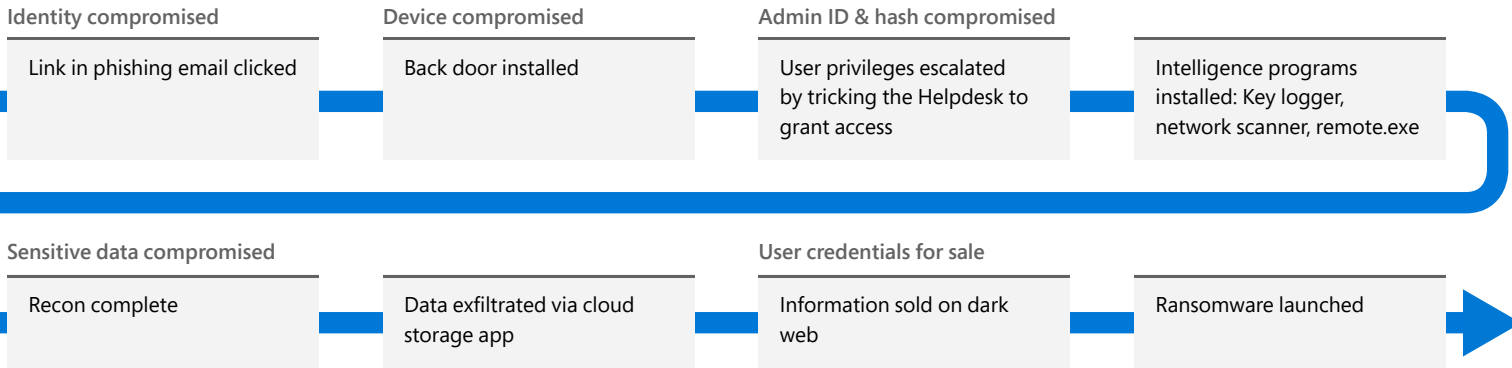
A breach is inevitable. How can Microsoft help me detect and respond fast?



SCENARIO:

Our HR coordinator came to the helpdesk with a ransomware message on their computer. We tried to get rid of it, but ultimately paid the ransom to get our files back. Our investigation uncovered that someone had been in the network for 52 days. We need to figure out what was compromised, how to fix the problems, and ensure this doesn't happen again.

Attack Timeline



Microsoft 365 helps protect

- Filter spam, phishing attacks, and malware across emails and files
- Detect ransomware across endpoints and cloud apps
- Block ransomware and automatically detonate attacks
- Detect anomalies and suspicious user/endpoint behavior without the need to create and fine-tune rules
- Automatically block endpoint threats
- Alert on: privileged identity usage, new program installs, or sensitive information downloads
- Automatically block or alert on unusual data downloads from managed apps
- Establish impossible geographic logins
- Automatically enforce risk-based policies
- Scan the dark web for stolen credentials

Microsoft 365 helps recover

- Automatically investigate and remediate endpoint threats
- Drill into alert details through a visual attack timeline
- Visualize a hacker's lateral movement
- Pivot from device analysis to user profiles or affected emails without losing context
- Recommend what to investigate and remediate
- Investigate across company-wide email to help remediate threats
- Run advanced hunting queries against endpoint data for forensic investigation
- Remove ransomware and recover files from OneDrive
- Teach users to guard against email phishing by simulating an attack
- Automatically require Multi-Factor Authentication and password changes based on risk-based policies

Microsoft 365 provides holistic security across Identity and Access Management, Information Protection, Threat Detection, and Security Management

Microsoft 365 Enterprise E5 includes powerful security tools that work together in different combinations to protect your organization in a variety of ways. These products come together to secure your organization against advanced threats and compromised identities:



Get complete, intelligent enterprise security

Test it yourself with a free trial, get serious with a proof of concept, or learn more at <https://aka.ms/M365E5/Security>

