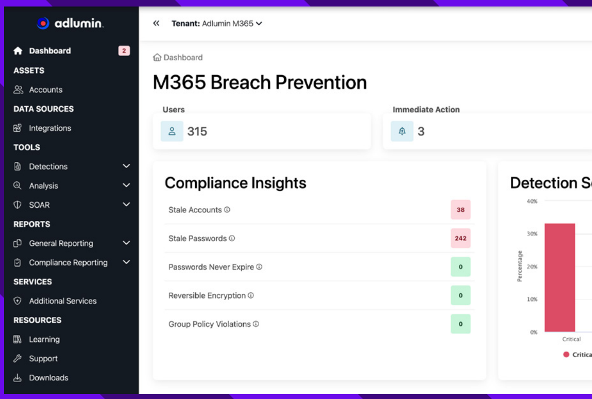
Breach Prevention for Microsoft 365

Detect and Stop Identity Attacks

Cybercriminals are increasingly bypassing traditional endpoints and networks and are instead targeting cloud identities to infiltrate organizations. Once access to an account is gained, they often roam freely, going undetected. Understanding when a user is performing actions that deviates from their typical routine is critical to stopping threats early.



M365 Breach Prevention

Users: 315

Immediate Action: 3

Compliance Insights

Stale Accounts	38
Stale Passwords	242
Passwords Never Expire	0
Reversible Encryption	0
Group Policy Violations	0

Quickly Spot Unusual Activity

- Uncover user behavior that indicates a potential account compromise.

Disrupt Attacks at the Start

- Automated response prevents threats from spreading and causing more severe damage.

Keep Your Data Protected

- Rapid response helps to safeguard sensitive data from unauthorized access or theft.

Adlumin focuses on identity protection by ingesting your Microsoft 365 telemetry. By applying machine learning models, baselines are developed for every user account. When a user deviates from expected behavior, Adlumin's intelligent response adapts in real-time, neutralizing threats based on their severity to keep your environment secure.

How Adlumin Detects and Stops Threats

Secure user accounts and prevent breaches at the most vulnerable entry point — your people.

- **Proactive Threat Detection**: Adlumin continuously monitors user and application activity in your Microsoft.
- **Dynamic Response**: Intelligent response analyzes data and behavior analytics to assess the risk level and adjust action accordingly.
- **Automated Threat Mitigation**: When suspicious activity is detected, the account in question either forces a password reset or is disabled.
- **Incident Summary and Recommendations**: Receive details on what occurred, what actions were taken, and steps to resolve the matter.

Advanced Identity Threat Detection

Adlumin uncovers hidden threats by analyzing a wide range of events and behaviors, helping to ensure cybercriminals don't go unnoticed. Key detection areas include:

- **Suspicious Sign-Ins**: Flags unauthorized login attempts, malicious IP access, and password spraying to stop account takeovers early.
- **Security Setting Tampering**: Detects unauthorized changes to MFA policies, service principal permissions, and security configurations that could expose your environment.
- **Application-Level Threats**: Identifies unauthorized mailbox access and enterprise application modifications that signal persistent threats.
- **Email-Based Attacks**: Catches stealthy tactics like email forwarding rules and inbox manipulations designed to exfiltrate sensitive data.

With Adlumin, your most vulnerable assets—user accounts—stay protected while reducing the burden on your security team. Our intelligent detection and automated response capabilities help you stay ahead of attacks, keeping your Microsoft environment secure.

adlumin.com