

Microsoft 365 Monitoring, Alerting and Reporting tool

Inside Agent is a covert SaaS platform engineered for in-depth security monitoring and auditing of Microsoft 365 environments. It seamlessly integrates with Microsoft 365 services, providing real-time alerts for potential security threats, automating compliance checks to ensure adherence to industry standards, and optimizing license usage to maximize efficiency and cost-effectiveness.

Over 90 Critical Intel Checks

- Entra Operations
- Exchange & Defender for 365
- License SKU Analysis
- MFA Status Analysis
- User Roles
- SharePoint & Teams Monitoring
- User Status & Device Compliance
- Defender Endpoint Analysis
- Conditional Access Analysis

Operational Advantages

Mitigate Cyber Risks

Proactively detect and address potential security threats before they impact your organization.

Reduce IT Burden

Automate routine security tasks and compliance checks, allowing your IT team to focus on strategic initiatives.

Optimize Costs

Streamline license management to minimize unnecessary expenses and maximize the value of your Microsoft 365 investment.

Ensure Compliance

Automatically align with industry regulations and standards, reducing the risk of non-compliance.

Deliver critical reports with precision and reliability. Whether you're analyzing NCSC guidelines, implementing Best Practice protocols, or navigating the Essential 8 security frameworks, our platform equips you with the necessary tools to ensure accuracy. Dive deeper into the intricacies of NIST 2.0, decoding complex standards to stay ahead of evolving threats. Inside Agent supports you every step of the way, helping to streamline security processes and keep your organization aligned with industry requirements.

Key Benefits

Enhance Security Posture

Strengthen your organization's security with continuous auditing and real-time monitoring to address potential vulnerabilities.

Automate Compliance

Ensure compliance with industry standards such as CIS, GDPR, and HIPAA by automating daily security and audit checks.

Optimize License Usage

Identify unused or underutilized licenses to streamline costs and improve Microsoft 365 license efficiency.

Reduce IT Overhead

Minimize manual security and audit tasks, freeing up your IT team to focus on critical, strategic initiatives.

Streamline Cloud Security

Proactively detect and address potential security threats before they impact your organization.

Proactive Threat Detection

Automate routine security tasks and compliance checks, allowing your IT team to focus on strategic initiatives.

Simplify M365 management

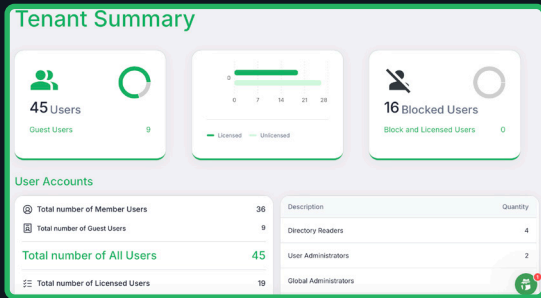
Centralize the management of your entire Microsoft 365 environment with an intuitive, user-friendly platform.

Multi-Tenant Management

Automatically align with industry regulations and standards, reducing the risk of non-compliance.

Continuous Security Auditing

Automated daily evaluations against industry standards such as CIS Benchmark.

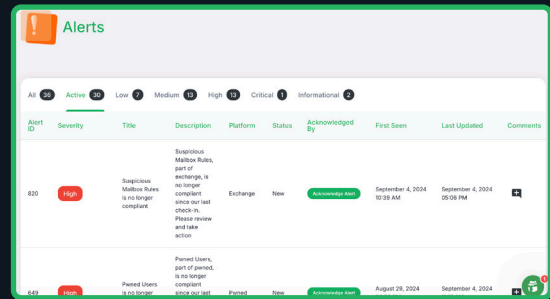


Keep your organization's Microsoft 365 security posture under constant surveillance, always aligned with top-tier protocols. Our platform executes covert, daily assessments across all Microsoft 365 services, detecting and neutralizing threats before they emerge.

Real-Time Alerts and Monitoring

Immediate notifications when critical changes or incidents occur.

Stay ahead of threats with real-time alerts for configuration changes or security incidents within Azure AD, Microsoft Teams, Exchange, and SharePoint Online. These proactive notifications ensure that your IT team can respond instantly to potential risks, reducing the likelihood of breaches.

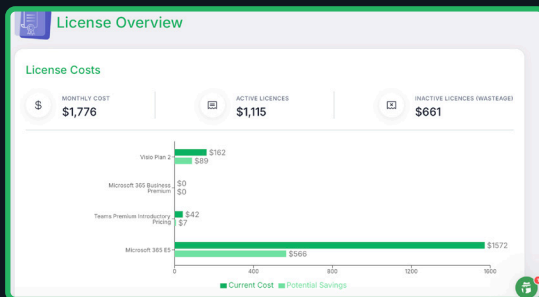


Alerts

Alert ID	Severity	Title	Description	Platform	Status	Acknowledged By	First Seen	Last Updated	Comments
820	High	Suspicious Mailbox Rules, part of exchange, is no longer compliant since not set check-in. Please review and take action	Suspicious Mailbox Rules, part of exchange, is no longer compliant since not set check-in. Please review and take action	Exchange	New	Acknowledged	September 4, 2024 10:39 AM	September 4, 2024 10:39 AM	
828	High	Permitted Users, part of permitted, is no longer compliant since not set check-in. Please review and take action	Permitted Users, part of permitted, is no longer compliant since not set check-in. Please review and take action	Permitted	New	Acknowledged	August 28, 2024	September 4, 2024	

License Auditing & Optimization

Eliminate unnecessary costs by optimizing Microsoft 365 license usage.

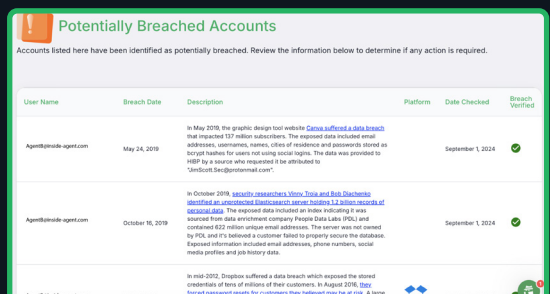


Track your Microsoft 365 licenses and eliminate waste. Our platform conducts regular license audits, providing insights into usage patterns, helping you reclaim underutilized licenses, and ensuring maximum return on your Microsoft 365 investment.

Built-in HaveIBeenPwned Integration

Monitor user credentials for potential breaches in real time.

Utilize our covert HaveIBeenPwned integration to discreetly monitor user credentials throughout your organization. Detect compromised accounts with early warnings and execute preemptive measures to shield your data and personnel from external threats.



Potentially Breached Accounts

Accounts listed here have been identified as potentially breached. Review the information below to determine if any action is required.

User Name	Breach Date	Description	Platform	Date Checked	Breach Verified
Agent@inside-agent.com	May 24, 2019	In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as target hashes for users not using social logins. The data was provided to HBP by a source who requested it be attributed to "SecurityData@protonmail.com".		September 1, 2024	✓
Agent@inside-agent.com	October 16, 2019	In October 2019, security researchers VirusTotal and BitDefender identified an unpatched vulnerability in the Joomla! 3.9.15 version of the Joomla! CMS. The exploit data included an exploit including it was awarded from data environment company Proton Data Labs (PDL) and contained 822 million unique email addresses. The server was not named by PDL, and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.		September 1, 2024	✓
Agent@inside-agent.com	July 1, 2022	In mid-2022, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, Day Social released results for customers who selected can be at risk. A large		September 1, 2024	✓