Infocyte

If they try it, we'll stop it.

MICROSOFT 365 SECURITY OVERVIEW

Microsoft 365 is the most popular SaaS productivity platform in the market today, used by 100M+ businesses worldwide. While the platform capabilities and embedded security can be excellent when configured properly, the burden to do this is on the subscriber. Without proper configuration and monitoring, Microsoft 365 customers are particularly vulnerable to the two most active and successful attack vectors: phishing and account takeover.

The good news is that the best practices are well known and established. However, once a customer has a good baseline that conforms to these standards, they must also monitor it continuously and follow up on alerts to ensure the environment stays secure.

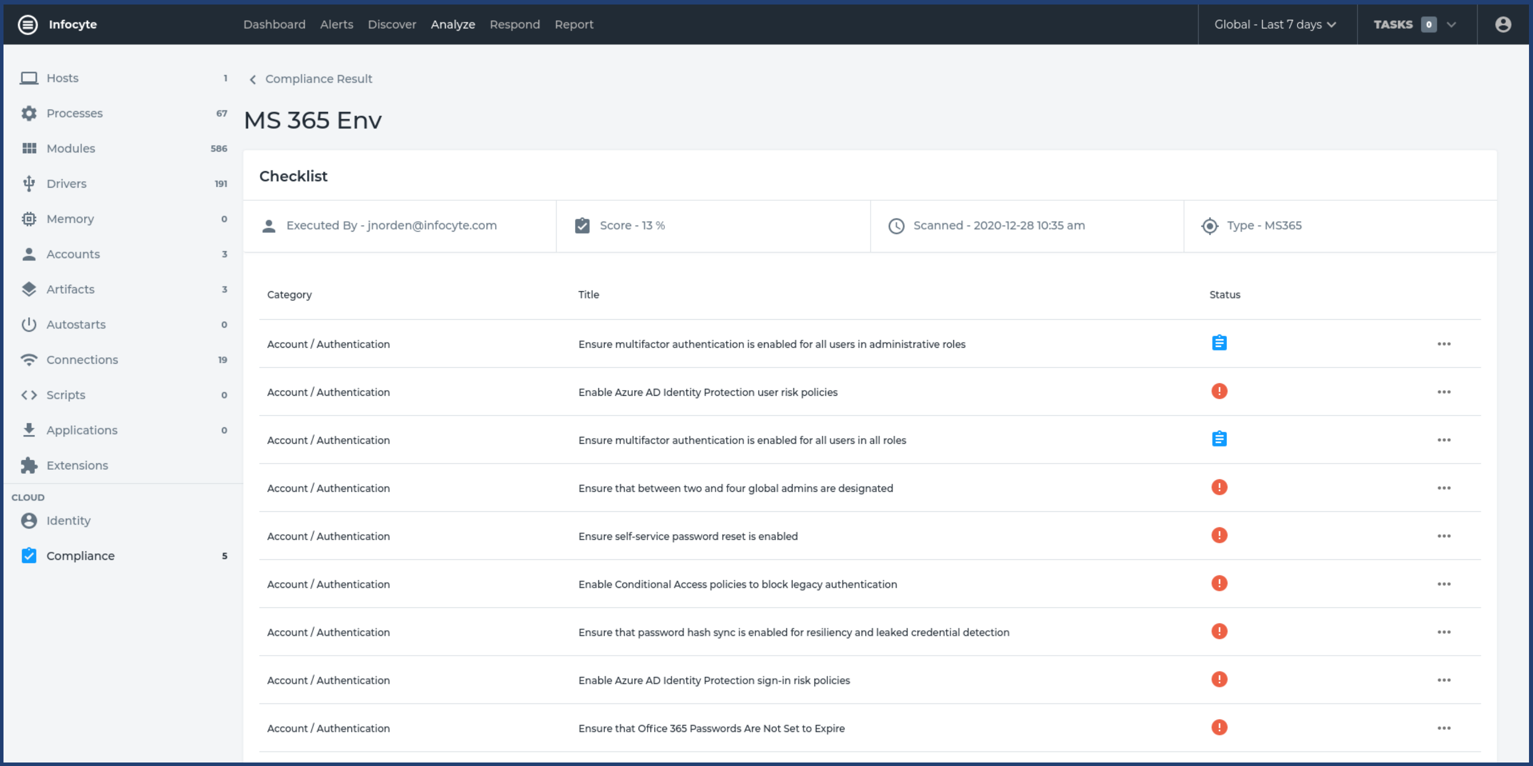
INFOCYTE'S OFFERING

Infocyte's Microsoft 365 Security Module leverages industry standards (CIS Benchmark) and quickly inspects the customer environment via a read-only API to ensure it is compliant with these best practices. Infocyte then reports back a pass/ fail rating for each setting or control, identifying issues and providing **recommended remediation actions**. Infocyte also provides an overall **Risk Score**. Once the baseline is set, Infocyte will also monitor the environment and alert when the score decreases or critical controls are removed.

For our Command subscribers, the Infocyte SOC provides the monitoring and will be at your side to help with remediation or address any issues.

- Exchange Online
- SharePoint Online
- OneDrive for Business
- Azure Active Directory
- Skype & Teams
- inTune

Preview



Infocyte   Dashboard   Alerts   Discover   Analyze   Respond   Report   Global - Last 7 days   TASKS 0

Hosts	1
Processes	67
Modules	586
Drivers	191
Memory	0
Accounts	3
Artifacts	3
Autostarts	0
Connections	19
Scripts	0
Applications	0
Extensions	
CLOUD	
Identity	
Compliance	5

< Compliance Result

MS 365 Env

Checklist

Executed By - jnorden@infocyte.com   Score - 13 %   Scanned - 2020-12-28 10:35 am   Type - MS365

Category	Title	Status	
Account / Authentication	Ensure multifactor authentication is enabled for all users in administrative roles	📋	•••
Account / Authentication	Enable Azure AD Identity Protection user risk policies	❗	•••
Account / Authentication	Ensure multifactor authentication is enabled for all users in all roles	📋	•••
Account / Authentication	Ensure that between two and four global admins are designated	❗	•••
Account / Authentication	Ensure self-service password reset is enabled	❗	•••
Account / Authentication	Enable Conditional Access policies to block legacy authentication	❗	•••
Account / Authentication	Ensure that password hash sync is enabled for resiliency and leaked credential detection	❗	•••
Account / Authentication	Enable Azure AD Identity Protection sign-in risk policies	❗	•••
Account / Authentication	Ensure that Office 365 Passwords Are Not Set to Expire	❗	•••

KEY FEATURES

Infocyte

- Conducts an on-demand inspection of an authenticated account
- Explains the details of the check or pass/fail rating, what failed, and how to remediate
- One-click to integrate with Microsoft 365 accounts (no Azure apps needed)
- Supports Microsoft 365 Business Basic and above

SIMPLE, EFFECTIVE SECURITY FOR MICROSOFT 365

Easy to deploy | Analyze quickly and accurately | Cut out the noise

Understand what needs to be fixed

ADDITIONAL ENHANCEMENTS COMING SOON:

Application Permissions

- Third Party Integrated Application
- Disable Sharing of Calendar Details to External Personnel
- Microsoft 365 ATP SafeLinks for Office Applications

Data Management

- Ensure Data Classification Policies Exist
- Ensure LockBox feature is enabled
- Ensure External Domains are not Allowed
- External Users Sharing Permissions

Account and Authentication:

- Add Checks for Skype and SharePoint

Email Security / Exchange Online

- Spam Policy Configuration
- Mail Transport Rule Configuration
- Basic Authentication for Exchange Online is Disabled
- Ensure Anti-Phishing Policies have been Created
- ATP Safe Attachments is Enabled

PHONE: 844.463.6298

EMAIL: sales@infocyte.com

ABOUT INFOCYTE

Founded by the leaders of the United States Air Force Cyber Incident Response Team (AFCIRT), Infocyte is the globally trusted leader in proactive threat detection and incident response. The world's leading security and incident response companies use Infocyte's platform to proactively detect and respond to vulnerabilities and threats within their customers' endpoints, data centers, and cloud environments. Infocyte's team and partner ecosystem help organizations maintain compliance, stop ransomware and account takeover, reduce risk, optimize security operations, and scale security teams. Infocyte is the faster, simpler, smarter way to detect and orchestrate response to sophisticated threats. Learn more at infocyte.com or follow us on Twitter: @InfocyteInc.