



Identity Posture Assessment

Powered by Managed ISPM



For M365 – Huntress Labs Eng 2

October 19, 2026

Compliance Rating

57.7%

M365 - Huntress Labs Eng 2 has a Compliance Rating of 57.7%, based on 45 of 78 assessed controls being configured correctly. 29 non-compliant controls can be automatically remediated by enabling Huntress ISPM recommendations, raising your score to 94.9%. An additional 3 controls require manual configuration by an administrator in Microsoft 365.

This assessment scored 78 Microsoft 365 security controls against 3 capabilities. Controls that your tenant is not licensed for were excluded from all counts, charts, and percentages in this report.

Compliant

45

of 78 controls

Not Compliant

29

Huntress can deploy these

Manual Action

3

Require admin change

Risk Accepted

1

Signed off by your team



Increase your compliance rating to 94.9%

Each ISPM recommendation in this report points to a gap in your Microsoft 365 configuration. Fixing them improves your security posture and raises your compliance rating.

Posture by Capability

78 controls assessed

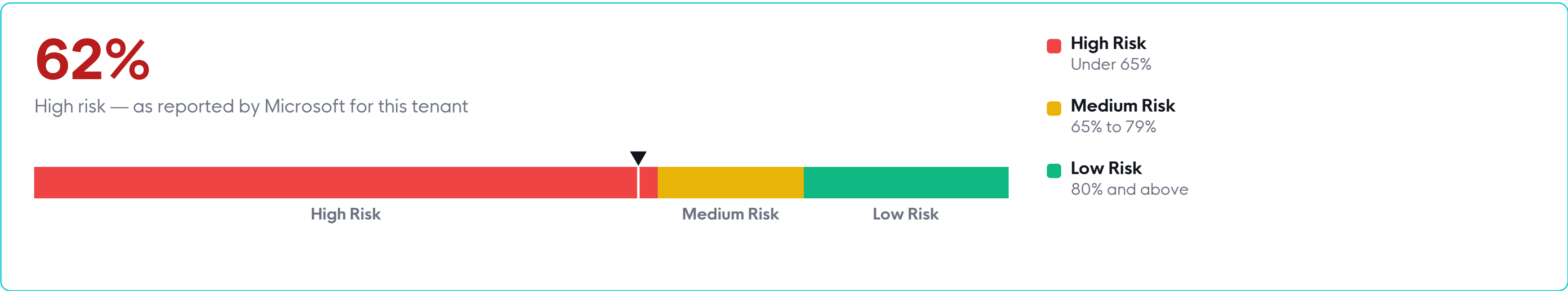
A Huntress capability is a focused part of the product that uses a clear threat model and a tightly scoped set of data to prevent specific hacker tradecraft.

Capability	Controls	Compliant	Not Compliant	Manual Action	Risk Accepted	Compliance
Unwanted Access	35	22	11	1	1	62.9%
Shadow Workflows	39	20	17	2	0	51.3%
Rogue Apps	4	3	1	0	0	75.0%

Microsoft Secure Score

Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more recommended actions taken. It is reported by Microsoft and is scored separately from the Huntress control assessment above.

[For more information on Microsoft Secure Score](#)



Gaps & Next Steps



Listed below are all the non-compliant controls in your organization, grouped by those you can deploy with Managed ISPM and those that must be configured manually.

🛡️

Increase your compliance rating to 94.9%
Each ISPM recommendation in this report points to a gap in your Microsoft 365 configuration. Fixing them improves your security posture and raises your compliance rating.

- **Compliant**
Configured to the Huntress ISPM framework
- **Not Compliant**
Huntress ISPM can deploy the fix
- **Manual Action**
An administrator must configure this in M365
- **Risk Accepted**
Your team has accepted the risk

Deploy with Huntress ISPM

29 controls

One-click fix these controls directly within Huntress and keep them enforced with drift remediation.

Severity	Control	Category	Capability
High	Block Exchange Forwarding	Exchange	Shadow Workflows
High	Ensure Direct Send is disabled	Exchange	Shadow Workflows
High	Ensure outbound spam policies set explicit sending limits and block senders that exceed them	Exchange	Shadow Workflows
High	Ensure sign-in is blocked for member accounts inactive for 90 days	Entra	Unwanted Access
High	Require Huntress Managed 'Block Device Code Flow' Policy	Conditional Access	Unwanted Access
High	Require Huntress Managed 'Block Legacy Authentication' Policy	Conditional Access	Unwanted Access
High	Require Huntress Managed 'Disable Desktop and Mobile Client Access for Guests' Policy	Conditional Access	Shadow Workflows
High	Require Huntress Managed 'Require MFA for all users' Policy	Conditional Access	Unwanted Access
High	Require Huntress Managed 'Restrict Azure Portal Management' Policy	Conditional Access	Unwanted Access
High	Security Defaults are disabled	Entra	Unwanted Access
Medium	Anonymous sharing links are disabled in SharePoint and OneDrive	SharePoint	Shadow Workflows
Medium	Ensure Anti-Phishing policies meet the Microsoft Standard impersonation protection baseline	Exchange	Shadow Workflows
Medium	Ensure Anti-Phishing policies meet the Microsoft Standard spoof protection baseline	Exchange	Shadow Workflows
Medium	Ensure Anti-Spam policies meet the Microsoft Standard baseline	Exchange	Shadow Workflows
Medium	Ensure Safe Attachments protection meets the Microsoft Standard baseline	Exchange	Shadow Workflows
Medium	Ensure Safe Links policies meet the Microsoft Standard baseline	Exchange	Shadow Workflows
Medium	Ensure organizational terms have been added to the banned password list	Entra	Unwanted Access
Medium	Guest resharing of SharePoint and OneDrive files is disabled	SharePoint	Shadow Workflows
Medium	Idle session timeout for SharePoint and OneDrive is enabled	SharePoint	Shadow Workflows
Medium	Non-admin users cannot create applications in the tenant	Entra	Rogue Apps
Medium	Require Huntress Managed 'Require Frequent Signin for Admins' Policy	Conditional Access	Unwanted Access
Medium	Require Huntress Managed 'Require MFA to Register or Join Devices' Policy	Conditional Access	Unwanted Access
Medium	Restrict Temporary Access Pass to Single Use Only	Entra	Unwanted Access
Low	Block attachment downloads in Outlook on the web on unmanaged devices	Conditional Access	Shadow Workflows

Severity	Control	Category	Capability
Low	Deleted user OneDrive content is retained for at least 90 days	SharePoint	Shadow Workflows
Low	Ensure users installing Outlook add-ins is not allowed	Exchange	Shadow Workflows
Low	Non administrative users should be prevented from retrieving BitLocker keys	Entra	Unwanted Access
Low	Restrict Shared Bookings creation to selected users	Exchange	Shadow Workflows
Low	User creation of SharePoint sites is disabled	SharePoint	Shadow Workflows

Manually Configure

3 controls

These controls sit outside what ISPM can deploy and need an administrator to change them in Microsoft 365.

Severity	Control	Category	Capability
High	Ensure Exchange Online Spam Policies are set to notify administrators	Exchange	Shadow Workflows
High	Ensure administrative accounts use licenses with a reduced application footprint	Entra	Unwanted Access
High	Ensure notifications for internal users sending malware is Enabled	Exchange	Shadow Workflows

Compliance Breakdown by Capability

A Huntress capability is a focused area of Microsoft 365 identity security, built around a specific threat model and a tightly scoped set of controls. Each section below shows your compliance rating for that capability and breaks down control statuses so you can identify where gaps exist and what actions are needed.

Unwanted Access

Unwanted Access focuses on preventive controls for authentication and external access.

Compliance Rating

63%

Compliant

22

of 35 controls

Not Compliant

11

Huntress can deploy these

Manual Action

1

Require admin change

Risk Accepted

1

Signed off by your team

Severity	Control	Status
High	Security Defaults are disabled	Not Compliant
High	Require Huntress Managed 'Require MFA for all users' Policy	Not Compliant
High	Ensure 'Per-user MFA' is turned off	Compliant
High	Between two and four Global Administrators are designated	Compliant
High	Administrative accounts are cloud-only	Compliant
High	Require Huntress Managed 'Block Legacy Authentication' Policy	Not Compliant
High	Ensure administrators are blocked from using SSPR	Compliant
High	Ensure administrative accounts use licenses with a reduced application footprint	Manual Action
High	Ensure Modern Authentication is enabled	Compliant
High	Legacy authentication protocols are blocked for SharePoint and OneDrive	Compliant
High	Require Huntress Managed 'Block Device Code Flow' Policy	Not Compliant
High	Require Huntress Managed 'Block Unused Device Types' Policy	Risk Accepted
High	Require Huntress Managed 'Restrict Azure Portal Management' Policy	Not Compliant
High	Ensure sign-in is blocked for guest accounts inactive for 30 days	Compliant
High	Ensure sign-in is blocked for member accounts inactive for 90 days	Not Compliant
Medium	Restrict Temporary Access Pass to Single Use Only	Not Compliant
Medium	Ensure the most secure Authentication Methods are used	Compliant
Medium	Ensure that Password protection for on-premises is turned on and set to Enforced mode	Compliant
Medium	Ensure that Password Lockout thresholds are correctly configured	Compliant
Medium	Password hash sync is enabled for hybrid deployments	Compliant
Medium	The 'Password expiration policy' is 'Set passwords to never expire (recommended)'	Compliant

Unwanted Access (continued)

Severity	Control	Status
Medium	Entra Connect Sync is configured with Service Principal credentials	Compliant
Medium	Ensure organizational terms have been added to the banned password list	Not Compliant
Medium	Microsoft Authenticator is configured to protect against MFA fatigue	Compliant
Medium	Authentication Policy Migration Status	Compliant
Medium	Ensure SMTP AUTH is disabled	Compliant
Medium	Require Huntress Managed 'Require Frequent Signin for Admins' Policy	Not Compliant
Medium	Require Huntress Managed 'Require MFA to Register or Join Devices' Policy	Not Compliant
Low	System-preferred multifactor authentication is turned on	Compliant
Low	Non administrative users should be prevented from retrieving BitLocker keys	Not Compliant
Low	Local Admin Password Solution (LAPS) for Windows is deployed for Entra	Compliant
Low	A dynamic group for guest users is created	Compliant
Low	MFA is required to join a device to Entra	Compliant
Low	Ensure sign-in to shared mailboxes is blocked	Compliant
Low	Ensure accounts blocked from signing in hold no mailbox, OneDrive or Teams licenses	Compliant

Shadow Workflows

Shadow Workflows focuses on preventative controls for Exchange, Teams, and SharePoint workflows.

Compliance Rating

51%

Compliant

20

of 39 controls

Not Compliant

17

Huntress can deploy these

Manual Action

2

Require admin change

Risk Accepted

0

Signed off by your team

Severity	Control	Status
High	Guest User Access Restrictions are configured	Compliant
High	The Guest invitation policy successfully limits guest permissions	Compliant
High	Block Exchange Forwarding	Not Compliant
High	Transport Rules Should Not Bypass Security Controls	Compliant
High	Connection Filter Should Not Bypass Spam Filtering	Compliant
High	Ensure notifications for internal users sending malware is Enabled	Manual Action
High	Ensure Exchange Online Spam Policies are set to notify administrators	Manual Action

Shadow Workflows (continued)

Severity	Control	Status
High	Ensure that SPF records are published for all Exchange Domains	Compliant
High	Require Huntress Managed 'Disable Desktop and Mobile Client Access for Guests' Policy	Not Compliant
High	Ensure that DKIM is enabled for all Exchange Online domains	Compliant
High	Ensure DMARC Records for all Exchange Online domains are published	Compliant
High	Ensure Direct Send is disabled	Not Compliant
High	Tenant Allow/Block list should contain zero entries in the allow list	Compliant
High	Ensure outbound spam policies set explicit sending limits and block senders that exceed them	Not Compliant
Medium	Non-admin accounts cannot create Microsoft 365 groups	Compliant
Medium	The Guest self-service sign-up via user flow is turned off	Compliant
Medium	Non-admin users cannot create tenants	Compliant
Medium	Ensure MailTips are enabled	Compliant
Medium	Ensure External Flag is visible within Outlook	Compliant
Medium	Ensure 'AuditDisabled' organizationally is set to 'False'	Compliant
Medium	Ensure the Common Attachment Types Filter is enabled	Compliant
Medium	Guest resharing of SharePoint and OneDrive files is disabled	Not Compliant
Medium	Anonymous sharing links are disabled in SharePoint and OneDrive	Not Compliant
Medium	Idle session timeout for SharePoint and OneDrive is enabled	Not Compliant
Medium	Ensure Anti-Malware policies meet the Microsoft Standard baseline	Compliant
Medium	Ensure Anti-Phishing policies meet the Microsoft Standard impersonation protection baseline	Not Compliant
Medium	Ensure Anti-Phishing policies meet the Microsoft Standard spoof protection baseline	Not Compliant
Medium	Ensure Anti-Spam policies meet the Microsoft Standard baseline	Not Compliant
Medium	Ensure Safe Attachments protection meets the Microsoft Standard baseline	Not Compliant
Medium	Ensure Safe Documents is turned on for Office clients	Compliant
Medium	Ensure Safe Links policies meet the Microsoft Standard baseline	Not Compliant
Low	Non-admin accounts cannot create Microsoft Security groups	Compliant
Low	Block Exchange Calendar Sharing External	Compliant
Low	Block Outlook External Storage Providers	Compliant
Low	Ensure users installing Outlook add-ins is not allowed	Not Compliant
Low	User creation of SharePoint sites is disabled	Not Compliant
Low	Deleted user OneDrive content is retained for at least 90 days	Not Compliant
Low	Restrict Shared Bookings creation to selected users	Not Compliant
Low	Block attachment downloads in Outlook on the web on unmanaged devices	Not Compliant

Rogue Apps

Rogue Apps focuses on preventive controls for OAuth consent and application creation.

Compliance Rating

75%

Compliant

3

of 4 controls

Not Compliant

1

Huntress can deploy these

Manual Action

0

Require admin change

Risk Accepted

0

Signed off by your team

Severity	Control	Status
Medium	Non-admin users cannot create applications in the tenant	Not Compliant
Medium	An Application Consent policy is deployed	Compliant
Low	Non-admin users cannot consent to third-party applications to the tenant	Compliant
Low	Self-service sign-up for Microsoft applications is turned off	Compliant

Your Path to Stronger Security

Harden Before Attackers Strike

Identity attacks succeed because of misconfigured settings, overpermissioned accounts, and gaps in authentication policy — not just because attackers are sophisticated. Huntress ISPM identifies these weaknesses and closes them before they can be exploited.

Deploy Controls in One Click

For controls Huntress can enforce directly, remediation takes a single click. No manual configuration in the Microsoft 365 admin center, no waiting on IT tickets — the fix is applied immediately to your tenant.

Keep Settings Enforced Over Time

Security controls drift. Admins make changes, new users get provisioned, and configurations slip out of compliance. Huntress ISPM can continuously monitor your tenant and automatically correct drift — so your posture stays strong without ongoing manual effort.



About Huntress

Huntress is a fully managed cybersecurity platform built for the 99% — the small and mid-sized businesses that are targeted by hackers every day but are often overlooked by enterprise security vendors. Powered by a 24/7 human-operated Security Operations Center (SOC), Huntress detects, investigates, and responds to threats that automated tools miss.

Contact

Sales
sales@huntress.com

Support
support@huntress.com