

OFFICE PROTECT

Strengthen Your Microsoft 365 Environment
with the **Best Threat Prevention Settings and
Alerts**

Presentation by: **Your Name Here**

Agenda

Your Logo
300 x 100

Who Are We?

What is Office
Protect?

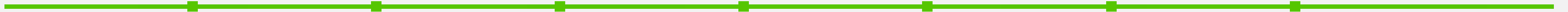
Our Office Protect
Offering

Contact Info

Is Microsoft 365
Secure?

Office Protect: Why
Your Business Needs It

Questions



Who Are We?

Company Name

Your Name

Your Profile – dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exercitation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio

Is Microsoft 365 Secure?

Is Microsoft 365 secure? Yes, but...

It's the most targeted platform for cybercrime—
70% of cyber attacks target Microsoft Office products.

Why is Microsoft 365 a growing target for hackers?

Because there's a lot at stake...



Sensitive Data

58.4% of a business's sensitive data in the cloud is stored in Microsoft Office documents.



Confidential Files

17.1% of the average company's files stored in OneDrive and SharePoint Online contain critical data, including financial records, forecasts, business plans and personal information.



Most Popular Enterprise Cloud

91.4% of businesses with at least 100 users are using Microsoft 365.

Microsoft 365 Security Risks: Root Causes

Persistent and sophisticated threats | Human error | Poor user education | Careless handling of data



Cyberattacks Skyrocketed in 2018

“We have seen a 350% increase in ransomware attacks, a 250% increase in spoofing or business email compromise (BEC) attacks and a 70% increase in spear-phishing attacks in companies overall.”

Ransomware

Ransomware is costing small and medium-sized businesses **\$75 billion a year**.

Anatomy

- Exploitation
- Infection
- Ransom
- Pay or Restore

Damage

- Data loss
- Downtime & lost productivity
- Ransom costs
- Investigation costs
- Data restoration and system cleanup
- Remittance paid to affected clients or users
- Damage to reputation

Botnet Attacks

In 2017, a botnet called KnockKnock was discovered **targeting businesses that run Microsoft 365.**

Anatomy

- Targets high-value accounts
- Keeps a low profile
- Exfiltrates data
- Spreads the malware across the network
- Difficult for internal IT to detect

Insider Threats

The biggest threats are **inside your company**.

57.1%

of organizations have at least one **insider** threat each month.

45.9%

of organizations have at least one **privileged user** threat each month.

Employee actions that can lead to costly data loss:

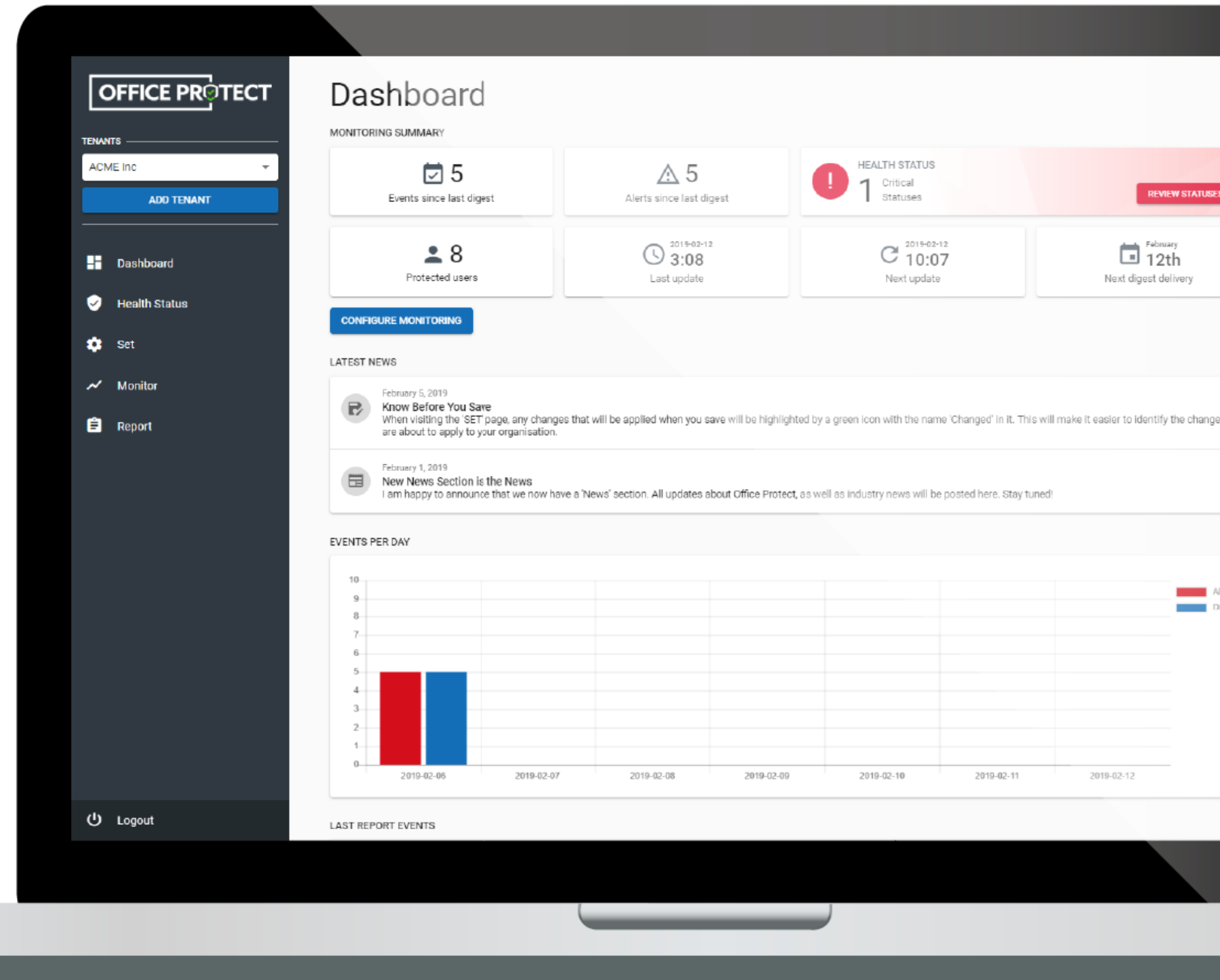
- Weak passwords
- Low awareness about phishing and other cybersecurity attacks
- Careless handling of data

What is Office Protect?

What is Office Protect?

Office Protect is an easy security management solution for Microsoft 365 that offers threat protection, monitoring, alerts and reporting to small and medium-sized businesses.

You get best practice security settings, account protection and better monitoring services.



1

Monitoring & Alerts

24/7 monitoring and alerts identify threats, so we can prevent and respond to potential future issues.

The screenshot displays the Office Protect web interface. On the left is a dark sidebar with the 'OFFICE PROTECT' logo at the top. Below the logo, there's a 'TENANTS' section with a dropdown menu showing 'ACME Inc' and an 'ADD TENANT' button. The sidebar contains a navigation menu with icons and labels for 'Dashboard', 'Health Status', 'Set', 'Monitor' (which is highlighted), and 'Report'. At the bottom of the sidebar is a 'Logout' button.

The main content area is titled 'Monitor'. It includes a sub-header 'Configure the events you want to monitor and recipients for your alerts and digests.' Below this, there's explanatory text: 'Alerts are sent as they happen and are meant to be things with immediate security impact for your tenant. Digest is a recap of recent event sent at regular interval. It should be used to compile for your review. All events will be accessible in the report section.'

The 'Select profile' section features a dropdown menu set to 'Focused'. A descriptive text box explains: 'A profile aimed at reducing the number of false positives to a minimum, while still alerting on what should be security issues. Could cause delays in detecting security incidents. Digest will include most events that are monitored by Office Protect.' Below the profile selection, there are two controls: 'Alerts Count' set to 5 and 'Digests Count' set to 17.

The bottom section is titled 'REVIEW OR CUSTOMIZE INDIVIDUAL EVENTS...'. It contains a table with columns for 'Event', 'Alert', and 'Digest'. Each row represents a specific security event with a description and toggle switches for alerting and digesting.

Event	Alert	Digest
Account Deleted Whenever an account is deleted in Office 365, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Administrator Role Change Whenever a change to user permission involving administrator privilege happens, this event will trigger.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email Impersonation Whenever an email is sent using Exchange 'Send As' functionality to impersonate someone else, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Email Transport Rule to External Domain Created If an Exchange transport rule automatically forwarding emails to an external domain is created, this event will trigger.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Shared Publicly (anonymous) Whenever a file is shared from SharePoint or OneDrive in a way that allows anonymous users (i.e. anybody) to access it.	<input type="checkbox"/>	<input type="checkbox"/>
Health Status Decline If a Health Status declines in your organization, this event will trigger.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Health Status Improvement If a Health Status improves in your organization, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
License Assigned Whenever an additional license is assigned to an existing account, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

What We Monitor

- Any change to security policies
- Sign-in from unusual locations, unknown devices or IP
- Suspicious mailbox activities
- Administrator abuse
- Any deleted accounts from hackers
- Emails sent to external sources
- Public sharing of company data
- Management impersonation via email by hackers
- Newly created accounts by hackers
- The creation of SharePoint sites

OFFICE PROTECT

TENANTS

ACME Inc

ADD TENANT

Dashboard

Health Status

Set

Monitor

Report

Logout

Monitor

Configure the events you want to monitor and recipients for your alerts and digests.

Alerts are sent as they happen and are meant to be things with immediate security impact for your tenant. Digest is a recap of recent event sent at regular interval. It should be used to compile for your review. All events will be accessible in the report section.

Select profile

Focused

A profile aimed at reducing the number of false positives to a minimum, while still alerting on what should be security issues. Could cause delays in detecting security incidents. Digest will include most events that are monitored by Office Protect.

Alerts Count: 5

Digests Count: 17

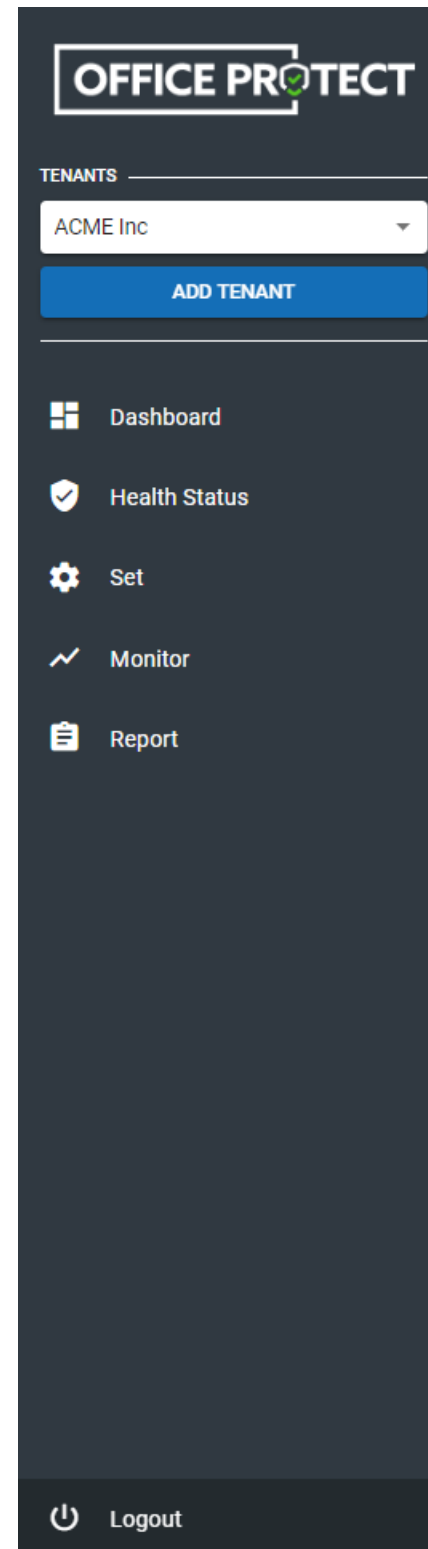
REVIEW OR CUSTOMIZE INDIVIDUAL EVENTS...

Event	Alert	Digest
Account Deleted Whenever an account is deleted in Office 365, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Administrator Role Change Whenever a change to user permission involving administrator privilege happens, this event will trigger.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Email Impersonation Whenever an email is sent using Exchange 'Send As' functionality to impersonate someone else, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Email Transport Rule to External Domain Created If an Exchange transport rule automatically forwarding emails to an external domain is created, this event will trigger.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File Shared Publicly (anonymous) Whenever a file is shared from SharePoint or OneDrive in a way that allows anonymous users (i.e. anybody) to access it.	<input type="checkbox"/>	<input type="checkbox"/>
Health Status Decline If a Health Status declines in your organization, this event will trigger.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Health Status Improvement If a Health Status improves in your organization, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
License Assigned Whenever an additional license is assigned to an existing account, this event will trigger.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

2

Best Practice Security Settings

Automated threat protection to prevent malicious activity from hackers and insiders with industry best practice security settings.



OFFICE PROTECT

TENANTS

ACME Inc

ADD TENANT

- Dashboard
- Health Status
- Set
- Monitor
- Report

Logout

Set

Select one of the profiles below to easily apply a set of Office 365 security settings to your tenant. We recommend the strongest profile your company is comfortable with. Consult the descriptions in the table below for more details or to customise the configuration.

Select profile

Custom Profile

You have modified some security settings and your profile is now different from any of our suggested profile. It is not inherently unsafe to create your own profile, but we cannot provide a security rating or impact rating for a custom profile.

Security Impact

Custom

Use Cases:

User Impact

Custom

If our profiles do not meet your need, you are encouraged to create your own selection of security settings.

Customise your profile to meet your need and make sure you review all settings and how they may interact.

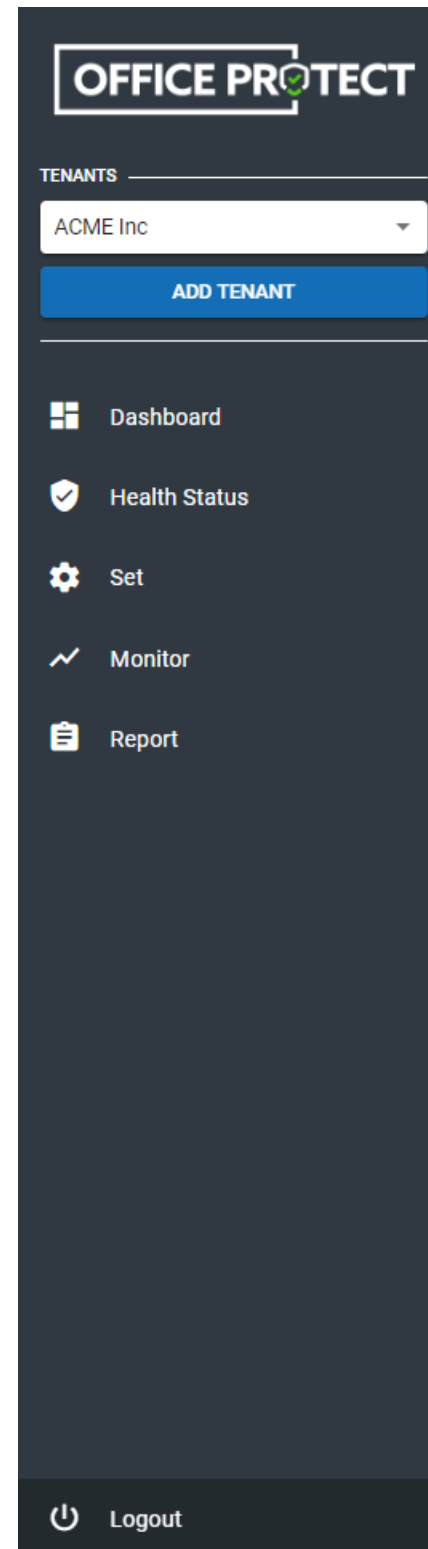
SAVE AND APPLY

REVIEW OR CUSTOMIZE INDIVIDUAL SETTINGS...

Account Passwords Never Expire Passwords on accounts will never expire and request to be changed.	Currently Apply All	Apply All	▼ ▼
Audit Logs Always-On Force back on the audit logs if they are ever turned off.			☑ ▼
Block "Bad" File Extension Attachments This will block bad known file extensions as email attachments.	19 selected values ace, ani, app, bat, cmd, ...		☑ ▼
Do Not Allow Calendar Details Sharing This will prevent users from sharing the full details of their calendar with external users.	Changed	Currently Authenticated Only	Disabled ▼ ▼
Do Not Allow Third-Party Integrated Applications This will prevent your users from giving permissions on O365 to third-party apps		Currently enabled	☑ ▼
Enable Client Rules Forwarding Block This will create a rule preventing auto-forward from your tenant to external organisations.	Changed	Currently enabled	☐ ▼
Enable Multi-Factor Authentication Enable Multi-Factor Authentication for admins or all users.		4 of 7 accounts set	Apply to all admins ▼ ▼
Mailbox Audit Logs Always-On Force back on the mailbox audit logs if they are ever turned off.	Changed		☑ ▼

What We Handle

- Audit Logs Always On
- Mailbox Audit Logs Always On
- Multi-factor authentication
- Spam notifications
- Block harmful email attachments
- Prevent users from making their personal info public through their calendar
- Block mass exfiltration of company email to an external destination
- Alert you if users are spamming
- Improve users' password habits



Set

Select one of the profiles below to easily apply a set of Office 365 security settings to your tenant. We recommend the strongest profile your company is comfortable with. Consult the descriptions in the table below for more details or to customise the configuration.

Select profile

Custom Profile

You have modified some security settings and your profile is now different from any of our suggested profile. It is not inherently unsafe to create your own profile, but we cannot provide a security rating or impact rating for a custom profile.

Security Impact Custom

Use Cases:

User Impact Custom

If our profiles do not meet your need, you are encouraged to create your own selection of security settings.

Customise your profile to meet your need and make sure you review all settings and how they may interact.

SAVE AND APPLY

REVIEW OR CUSTOMIZE INDIVIDUAL SETTINGS...

Account Passwords Never Expire Passwords on accounts will never expire and request to be changed.	Currently Apply All	Apply All	▼ ▼
Audit Logs Always-On Force back on the audit logs if they are ever turned off.			☑ ▼
Block "Bad" File Extension Attachments This will block bad known file extensions as email attachments.	19 selected values ace, ani, app, bat, cmd, ...		☑ ▼
Do Not Allow Calendar Details Sharing This will prevent users from sharing the full details of their calendar with external users.	Changed	Currently Authenticated Only	Disabled ▼ ▼
Do Not Allow Third-Party Integrated Applications This will prevent your users from giving permissions on O365 to third-party apps		Currently enabled	☑ ▼
Enable Client Rules Forwarding Block This will create a rule preventing auto-forward from your tenant to external organisations.	Changed	Currently enabled	☐ ▼
Enable Multi-Factor Authentication Enable Multi-Factor Authentication for admins or all users.		4 of 7 accounts set	Apply to all admins ▼ ▼
Mailbox Audit Logs Always-On Force back on the mailbox audit logs if they are ever turned off.	Changed		☑ ▼

3

Real-Time Reporting

Built-in reporting gives us insights and more visibility into how your employees are using Microsoft 365.

Easy-to-read activity dashboards and automated reports.

Date Time ↓	Event	User	Details	Source
<input type="checkbox"/> 1/17/19, 10:38 AM	Sign-In from Unauthorized Country	admin	Access to admin@acmesw.onmicrosoft.com account from unauthorized country Canada (CA) from address: 216.113.37.50. Validate if access is known. If not, consider suspending the account until the matter is clarified.	Azure AD
<input type="checkbox"/> 11/16/18, 10:49 PM	Administrator Role Change		Company Administrator role was added to mgelinas@acmesw.onmicrosoft.com. Validate for privilege abuse and ensure accounts have the most restricted permissions possible.	Office Protect
<input type="checkbox"/> 11/16/18, 2:21 PM	Sign-In from Unauthorized Country	admin	Access to admin@acmesw.onmicrosoft.com account from unauthorized country Canada (CA) from address: 69.156.166.122. Validate if access is known. If not, consider suspending the account until the matter is clarified.	Azure AD
<input type="checkbox"/> 11/15/18, 3:09 PM	Sign-In from Unauthorized Country	app	Access to app@sharepoint account from unauthorized country United States (US) from address: 185.151.160.12. Validate if access is known. If not, consider suspending the account until the matter is clarified.	SharePoint
<input type="checkbox"/> 9/20/18, 1:39 PM	Office 365 setting changed outside Office Protect		The 'Mailbox Audit Log Enabled' setting was changed directly in Office 365 from True to False (Setting has been enforced). You can re-apply the settings from Office Protect. We recommend investigating who made the change directly in Office 365.	Office Protect
<input type="checkbox"/> 9/20/18, 1:38 PM	New Account Created	exo_evo_migration	A new account was created by (exo_evo_migration@support.onmicrosoft.com). New user is testshared2 (testshared2@acmesw.onmicrosoft.com). Licenses: No licenses assigned.	Azure AD
<input type="checkbox"/> 9/20/18, 1:36 PM	New Account Created	exo_evo_migration	A new account was created by (exo_evo_migration@support.onmicrosoft.com). New user is testshared (testshared@acmesw.onmicrosoft.com). Licenses: No licenses assigned.	Azure AD
<input type="checkbox"/> 8/31/18, 12:04 PM	User Accessed with Previously Unknown Device and IP	admin	User ACME Inc (admin@acmesw.onmicrosoft.com) accessed Office 365 with an IP and Device we had both not seen before. Device: Chrome Windows 10 IP: 216.113.37.50 (Canada) User: ACME Inc (admin@acmesw.onmicrosoft.com) Validate this is a known user. You will not receive anymore alerts for this combination of device and IP, for this user.	Office Protect
<input type="checkbox"/> 8/17/18, 5:58 PM	Office 365 setting changed outside Office Protect		The 'Mailbox Audit Log Enabled' setting was changed directly in Office 365 from True to False (Setting has been enforced). You can re-apply the settings from Office Protect. We recommend investigating who made the change directly in Office 365.	Office Protect

Real-Time Reporting

- Uploaded, downloaded and restored files
- File, folder and site activities
- Sharing and access request activities
- Administrator activities

Date Time ↓	Event	User	Details	Source
<input type="checkbox"/> 1/17/19, 10:38 AM	Sign-In from Unauthorized Country	admin	Access to admin@acmesw.onmicrosoft.com account from unauthorized country Canada (CA) from address: 216.113.37.50. Validate if access is known. If not, consider suspending the account until the matter is clarified.	Azure AD
<input type="checkbox"/> 11/16/18, 10:49 PM	Administrator Role Change		Company Administrator role was added to mgelinas@acmesw.onmicrosoft.com. Validate for privilege abuse and ensure accounts have the most restricted permissions possible.	Office Protect
<input type="checkbox"/> 11/16/18, 2:21 PM	Sign-In from Unauthorized Country	admin	Access to admin@acmesw.onmicrosoft.com account from unauthorized country Canada (CA) from address: 69.156.166.122. Validate if access is known. If not, consider suspending the account until the matter is clarified.	Azure AD
<input type="checkbox"/> 11/15/18, 3:09 PM	Sign-In from Unauthorized Country	app	Access to app@sharepoint account from unauthorized country United States (US) from address: 185.151.160.12. Validate if access is known. If not, consider suspending the account until the matter is clarified.	SharePoint
<input type="checkbox"/> 9/20/18, 1:39 PM	Office 365 setting changed outside Office Protect		The 'Mailbox Audit Log Enabled' setting was changed directly in Office 365 from True to False (Setting has been enforced). You can re-apply the settings from Office Protect. We recommend investigating who made the change directly in Office 365.	Office Protect
<input type="checkbox"/> 9/20/18, 1:38 PM	New Account Created	exo_evo_migration	A new account was created by (exo_evo_migration@support.onmicrosoft.com). New user is testshared2 (testshared2@acmesw.onmicrosoft.com). Licenses: No licenses assigned.	Azure AD
<input type="checkbox"/> 9/20/18, 1:36 PM	New Account Created	exo_evo_migration	A new account was created by (exo_evo_migration@support.onmicrosoft.com). New user is testshared (testshared@acmesw.onmicrosoft.com). Licenses: No licenses assigned.	Azure AD
<input type="checkbox"/> 8/31/18, 12:04 PM	User Accessed with Previously Unknown Device and IP	admin	User ACME Inc (admin@acmesw.onmicrosoft.com) accessed Office 365 with an IP and Device we had both not seen before. Device: Chrome Windows 10 IP: 216.113.37.50 (Canada) User: ACME Inc (admin@acmesw.onmicrosoft.com) Validate this is a known user. You will not receive anymore alerts for this combination of device and IP, for this user.	Office Protect
<input type="checkbox"/> 8/17/18, 5:58 PM	Office 365 setting changed outside Office Protect		The 'Mailbox Audit Log Enabled' setting was changed directly in Office 365 from True to False (Setting has been enforced). You can re-apply the settings from Office Protect. We recommend investigating who made the change directly in Office 365.	Office Protect

**Office Protect:
Why Your Business Needs It**

Why do you need Office Protect?

Because it solves all of these problems in Microsoft 365...



Prevention

24/7 monitoring, alerts and reporting gives you better insight into risks and user behavior, allowing you to respond to potential issues quickly.



Protection

Get the best security settings to protect against advanced threats.

Why do you need Office Protect?

Because it solves all of these problems in Microsoft 365...



Persistent Threats

The average organization receives 2.7 threats each month in Microsoft 365. Cybercrime is a growing threat, especially ransomware.



Human Error

Nearly half of security incidents in SMBs are due to human error.



Lack of Awareness

It takes just one uneducated or distracted user to open a malicious file that can harm an entire company.

Our Office Protect Offering

\$ PRICE

/per
Microsoft
365 seat

Office Protect

Threat protection using best practice security settings
24/7 monitoring & alerts
Real-time reporting

\$ PRICE

/per month

Microsoft 365 Bundle

Microsoft 365
Office Protect
Online Backup
QuickHelp eLearning for Microsoft
365

Cybercrime is big business. Don't be a victim.

A worry-free security management solution to protect your data in Microsoft 365

Quickly Respond to Evolving Security Needs

Advanced account protection

Strategic planning & compliance

Event monitoring and fast intervention

Audit & testing

Simple & Reliable

We do all the heavy lifting

24/7 monitoring & alerts

Remote management

Stay on Top of User Activities

Increased visibility

Real-time reports on potential security risks, user behavior & incidents

Proactive prevention of threats and attacks

Your Logo

300 x 100

Questions?

Contact Info

Email: MyEmail@yourcompany.com

Phone Number: 123-456-7890

LinkedIn: www.linkedin.com/YourProfile