06.07.2023

rhipe

A Crayon company

Welcome – Webinar will start shortly

rhipe

A Crayon company

Keeping your clients Secure

How to use, operate and monetise the Microsoft Security platform, to efficiently protect your clients

Sydney

Meet our Speaker today

Paul Bristow

Productivity Solutions

rhipe

A Crayon company

How to Productise and Package Security as a Service with the Microsoft Security platform

Microsoft Security platform brings enterprise grade Security to SMB with Microsoft 365 Business Premium

[Business Premium Service Description with Add-ons]

Feature and Function		Microsoft 365 Business Premium	Microsoft Defender for Business standalone
eDiscovery and Audits	eDiscovery	•	
	Litigation Hold	•	
	Email Archiving	•	
Information Protection	Information Rights Management	•	
	File classification/labeling	•	
	File tracking and revocation	•	
Data Loss Prevention	Message Encryption	•	
	Data Loss Prevention	•	
	Data App Security	•	
Email and Collaboration Security	Safe links	•	
	Safe Attachments	•	
	Anti-phishing	•	
Device management	Windows device setup & management	•[1]	
	Device health analytics	•	
	Mobile Device Management	•	
	Mobile App Management	•	
Identity and Access Management and Security	Risk based Conditional access	•	
	Multi-factor authentication	•	
Endpoint Security	Centralized management	•	•
	Simplified client configuration	•	•
	Next-gen protection	•	•
	Attack Surface Reduction	•	•
	Network Protection	•	•
	Web Category blocking	•	•
	Endpoint detection and response	•	•
	Cross platform support (iOS/Android/Mac)	•	•
	Automated investigation and response	•	•
	Threat and vulnerability	•	•
	Threat intelligence	•	•

Who is your customer

- What is the right Security Posture for your clients.
- Should you have more than one offering.
- Every client should have a default Basic Security setting. Some clients need more.
- There is no such thing as entry level Security. There is only the right Security.

Financial Advisors Employs 30 people B2C

- Personal Details
- Financial Status
- Transaction Details
- Taxation information
- Share trading App
- B2B with Accountants

Building Supplies Employs 30 people B2B

- Co Account names
- EFTPOS Machine
- Warehousing App
- Shared mailboxes

What do you pick, what do you add

Control	Control Action examples	Components	Licence SKU
Application Control	Block executable mail content. Execution in temp folders. Protect against un-wanted Apps. Restrict ActiveX. App Control W/L.	Defender for Office, MDE ASR rules, WDAC	M365 Bus Premium, Defender for Office P2
Patch Applications	Disable un-supported Apps. Manage Security on Internet facing servers. Review vulnerabilities daily.	Intune, Win update for Bus, Defender for endpoint, MS Edge, Intune.	M365 Bus Premium, Defender for Business, Defender for Endpoint P2.
Configure MS Office macro settings	Disable un-necessary Macros. Macros from Internet blocked. Use of Macros	MS Defender for endpoint, MS Defender for office safe-links, ASR	M365 Bus Premium, Defender for Business, Defender for Office P1
User Application hardening	Block internet Ads. Restrict web browser processing Java	Intune, Defender Smartscreen, MS Edge managed by Intune.	M365 Bus Premium
Restrict Administrative privileg es	Restrict and limit PA access, and PA Internet, services, email, access. Role based PA, Manage PA's. Limit use of roles	Azure AD.	M365 Bus Premium, AAD P1 & P2
Patch Operating Systems	Update Internet facing servers and run vulnerability scans. Replace un-supported Operating systems.	Intune, Def for endpoint, Win up-date for Business.	M365 Bus Premium, Defender for Business
Multi-Factor Authentication	Enable MFA for all users. Enable MFA for third party users	Azure AD.	M365 Bus Premium, AAD P1 & P2
Regular Back-ups	Create and retain Back-ups. Back-up policies and procedures.	Azure Back-up, M365 Back-up	Azure Back-up, M365 Back-up

rhipe
A Crayon company

Refine, add, delete, and make it yours

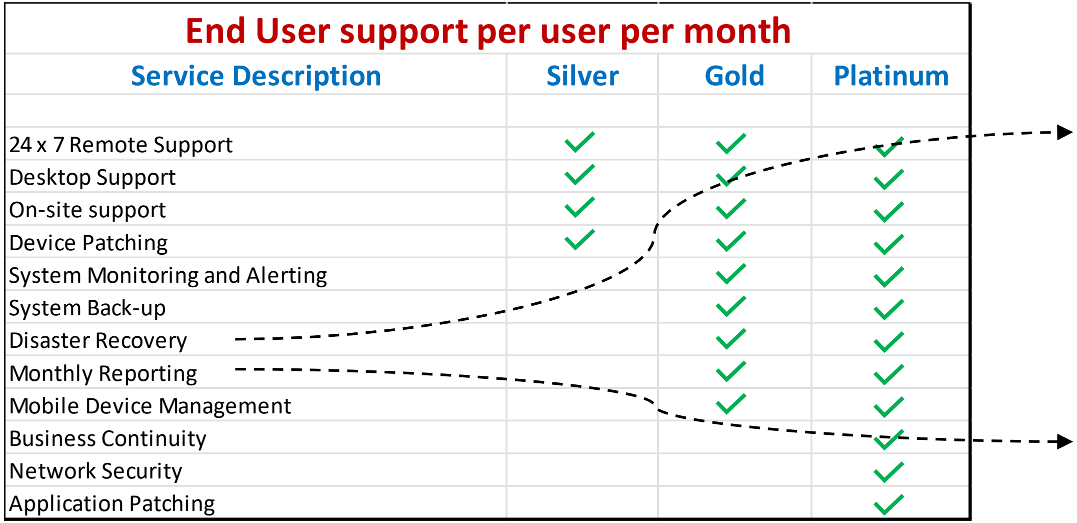
Control	Control Action	Assumptions & Comments	Licence SKU
Application Control	Block executable mail content. Execution in temp folders. Protect against un-wanted Apps. Restrict ActiveX. App Control W/L.	Defender for Office, MDE ASR rules, WDAC	M365 Bus Premium, Defender for Office P2
Patch Applications	Disable un-supported Apps. Manage Security on Internet facing servers. Review vulnerabilities daily.	Intune, Win update for Bus, Defender for endpoint, MS Edge, Intune.	M365 Bus Premium, Defender for Business, Defender for Endpoint P2.
Configure MS Office macro settings	Disable un-necessary Macros. Macros from Internet blocked. Use of Macros	MS Defender for endpoint, MS Defender for office safe-links, ASR	M365 Bus Premium, Defender for Business, Defender for Office P1
User Application hardening	Block internet Ads. Restrict web browser processing Java	Intune, Defender Smartscreen, MS Edge managed by Intune.	M365 Bus Premium
Restrict Administrative privileg es	Restrict and limit PA access, and PA Internet, services, email, access. Role based PA, Manage PA's. Limit use of roles	Azure AD.	M365 Bus Premium, AAD P1 & P2
Patch Operating Systems	Update Internet facing servers and run vulnerability scans. Replace un-supported Operating systems.	Intune, Def for endpoint, Win up-date for Business.	M365 Bus Premium, Defender for Business
Multi-Factor Authentication	Enable MFA for all users. Enable MFA for third party users	Azure AD.	M365 Bus Premium, AAD P1 & P2
Regular Back-ups	Create and retain Back-ups. Back-up policies and procedures.	Azure Back-up, M365 Back-up	Azure Back-up, M365 Back-up
User Training	User Awareness and Anti-Phishing campaigns	If not Defender for O365 P2	Plenty to choose from

User acceptance is key to adoption

Look after your data Shared Responsibility

rhipe
A Crayon company

A Service Description for End User Support



End User support per user per month			
Service Description	**Silver**	**Gold**	**Platinum**
24 x 7 Remote Support	✓	✓	✓
Desktop Support	✓	✓	✓
On-site support	✓	✓	✓
Device Patching	✓	✓	✓
System Monitoring and Alerting		✓	✓
System Back-up		✓	✓
Disaster Recovery		✓	✓
Monthly Reporting		✓	✓
Mobile Device Management		✓	✓
Business Continuity			✓
Network Security			✓
Application Patching			✓

Link to description in main body of document

Service Description End User Management main document

Description of Services

Disaster Recovery

Included in the service is a Disaster Recovery service provided by MSP in client's Azure service that captures data of client servers at regular intervals including its data, operating system application and configuration and replicates those images to a secondary Azure data centre, for purposes of restoration of service.

Monthly Reporting

MSP will provide clients with monthly reporting detailing resolved tickets, patching, antivirus performance, service availability and network reliability.

A Service Description Security Service

End User support per user per month				
Service Description	**Silver**	**Gold**	**Platinum**	**Cyber Security**
24 x 7 Remote Support	✓	✓	✓	
Desktop Support	✓	✓	✓	
On-site support	✓	✓	✓	
Device Patching	✓	✓	✓	
System Monitoring and Alerting		✓	✓	
System Back-up		✓	✓	
Disaster Recovery		✓	✓	
Monthly Reporting		✓	✓	
Mobile Device Management		✓	✓	
Business Continuity			✓	
Network Security			✓	
Application Patching			✓	
Include or keep separate				
End Point Protection				✓
Email Security				✓
Detection and Response				✓
Auto Threat Remediation				✓
Password and Sign in Management				✓
Monthly Security Reporting				✓
Application Protection				✓
User Awareness Training				✓

Link to description in main body of document

Service Description Cyber-Security main document

Description of Services

End Point Protection

All antivirus licensing is included for Servers, MAC's and PC's. MSP monitors the antivirus software 24/7 and in the event of a virus/ad-ware/spyware etc. being detected a service ticket be created in MSP's ticket management system. MSP will address viruses as requiring an emergency response by a technician to confirm virus removal.

User Awareness Training

MSP includes and requires all computer users at client to participate in regular security awareness training as provided. Training may include simulated phishing attacks, instruction in company IT policies and best practices, compliance training and testing.

rhipe
A Crayon company

New Security client or prospect

- What do they currently do about Security.
- What is status of their IT.
- How will we get them to our Security baseline that meets their needs.
- Existing customer question:
  - “What do you think we have you covered for when it comes to Cyber-Security”
  - “What about those questionnaires from your Insurance company, we helped you with”

Security Assessment

- Everything or just endpoints
- Just the results or Analysis too
- Prioritised

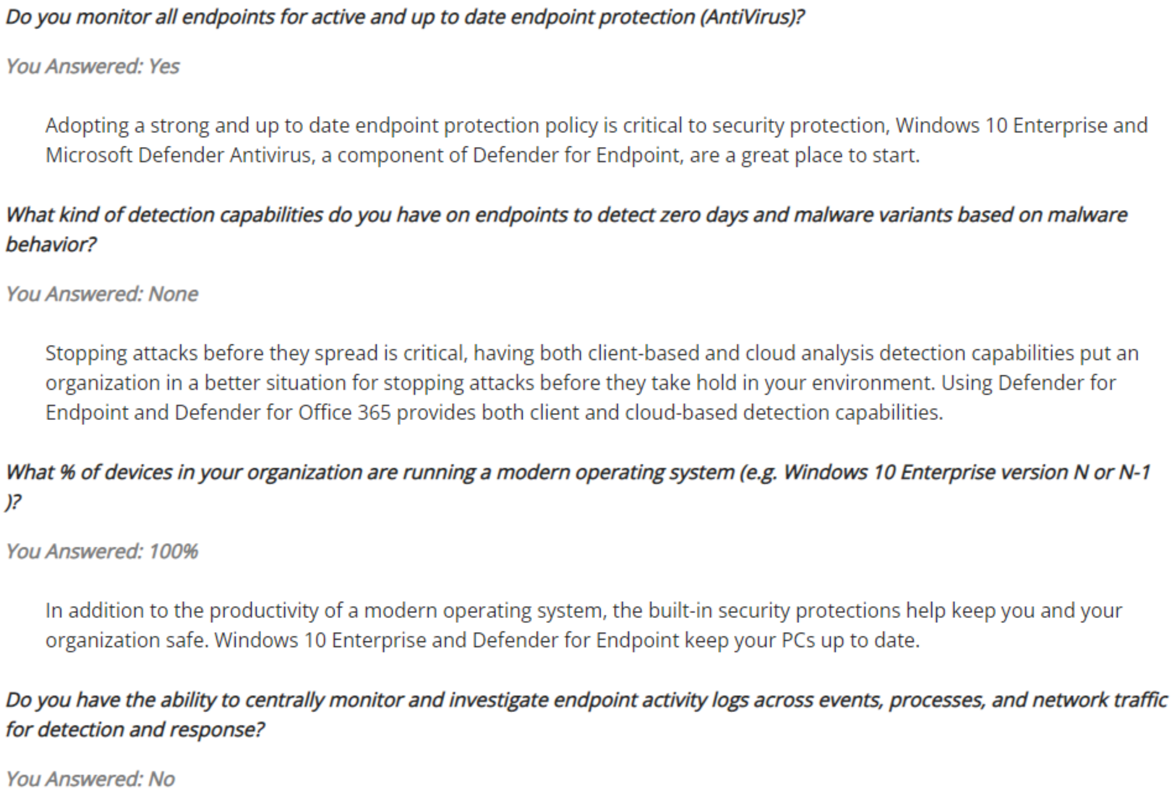
Desktop or Tools

- Crayon White Label
- Microsoft Free x 2
- Microsoft Secure Score
- Build your own

Example

Microsoft free Security Assessment
Microsoft Security

- Desktop based
- Multiple choice questions



Do you monitor all endpoints for active and up to date endpoint protection (AntiVirus)?

You Answered: Yes

Adopting a strong and up to date endpoint protection policy is critical to security protection, Windows 10 Enterprise and Microsoft Defender Antivirus, a component of Defender for Endpoint, are a great place to start.

What kind of detection capabilities do you have on endpoints to detect zero days and malware variants based on malware behavior?

You Answered: None

Stopping attacks before they spread is critical, having both client-based and cloud analysis detection capabilities put an organization in a better situation for stopping attacks before they take hold in your environment. Using Defender for Endpoint and Defender for Office 365 provides both client and cloud-based detection capabilities.

What % of devices in your organization are running a modern operating system (e.g. Windows 10 Enterprise version N or N-1)?

You Answered: 100%

In addition to the productivity of a modern operating system, the built-in security protections help keep you and your organization safe. Windows 10 Enterprise and Defender for Endpoint keep your PCs up to date.

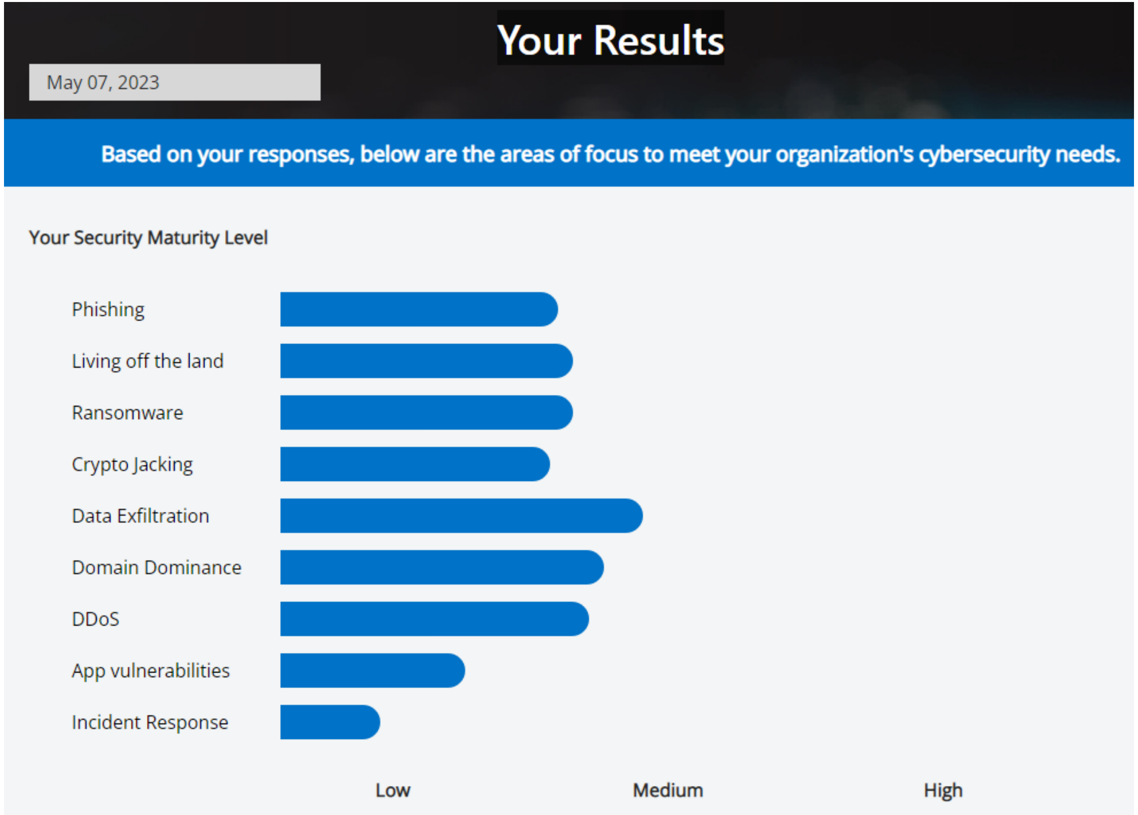
Do you have the ability to centrally monitor and investigate endpoint activity logs across events, processes, and network traffic for detection and response?

You Answered: No

Example

Microsoft free Security Assessment Results

- Simple assessment
- Presentable to the client



May 07, 2023

Your Results

Based on your responses, below are the areas of focus to meet your organization's cybersecurity needs.

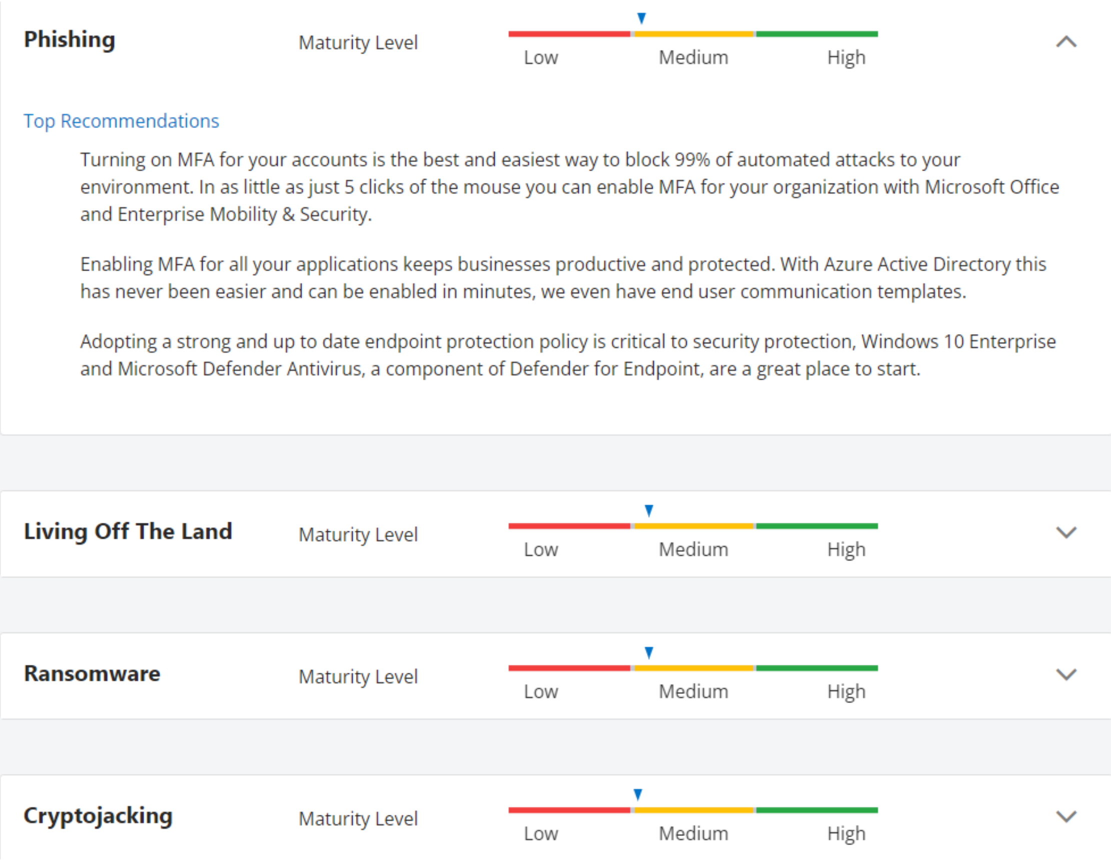
Your Security Maturity Level

rhipe
A Crayon company

Example

Microsoft free Security Assessment Recommendations

- General in nature
- Microsoft focused



Phishing Maturity Level

Low Medium High

Top Recommendations

Turning on MFA for your accounts is the best and easiest way to block 99% of automated attacks to your environment. In as little as just 5 clicks of the mouse you can enable MFA for your organization with Microsoft Office and Enterprise Mobility & Security.

Enabling MFA for all your applications keeps businesses productive and protected. With Azure Active Directory this has never been easier and can be enabled in minutes, we even have end user communication templates.

Adopting a strong and up to date endpoint protection policy is critical to security protection, Windows 10 Enterprise and Microsoft Defender Antivirus, a component of Defender for Endpoint, are a great place to start.

Living Off The Land Maturity Level

Low Medium High

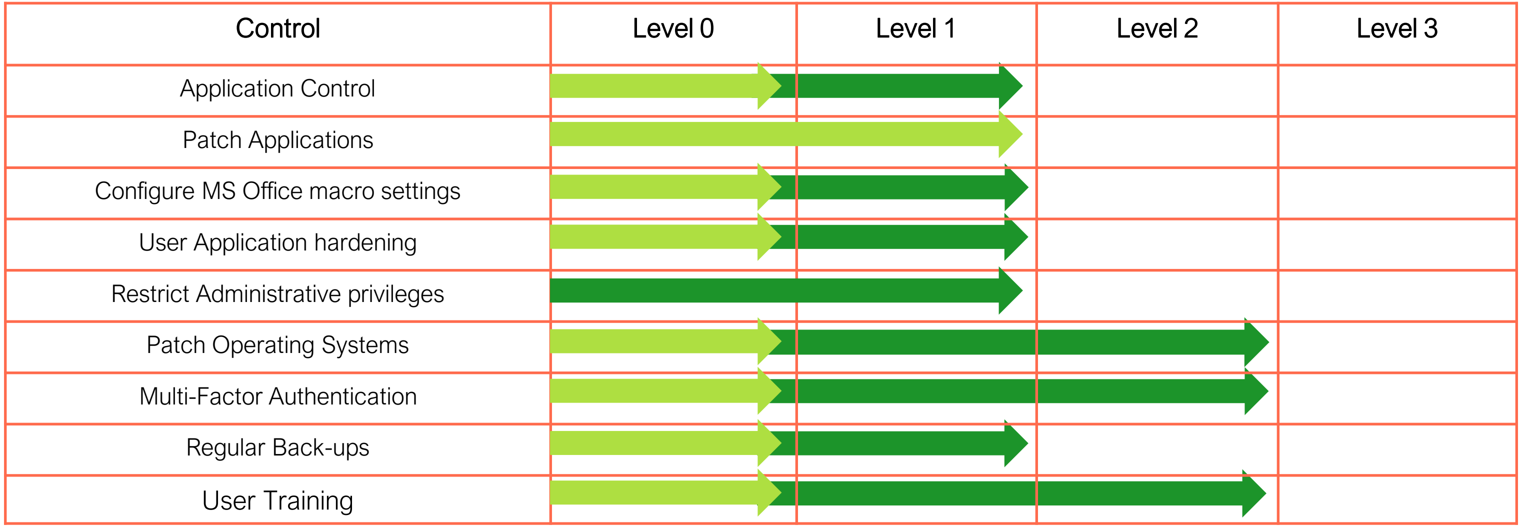
Ransomware Maturity Level

Low Medium High

Cryptojacking Maturity Level

Low Medium High

The conversation with the client



Control	Level 0	Level 1	Level 2	Level 3
Application Control				
Patch Applications				
Configure MS Office macro settings				
User Application hardening				
Restrict Administrative privileges				
Patch Operating Systems				
Multi-Factor Authentication				
Regular Back-ups				
User Training				

ASD-8 Security Assessment

- Where are you now The results ➡
- Where you need to be The Baseline ➡
- List, Prioritise and Explain the deltas

- When should the work be done
- How long will it take
- How much will it cost

The conversation with the client

- Assess your current Security Posture
- Get you to and keep on an agreed baseline
- For 12, 24, or 36 months
- On-boarding costs
  - Amortise
  - Ignore
- Includes assessment if they sign?
- You get a monthly Meeting and Reports

Managed/Master Services Agreement

End Point Protection				✓
Email Security				✓
Detection and Response				✓
Auto Threat Remediation				✓
Password and Sign in Management				✓
Monthly Security Reporting				✓
Application Protection				✓
User Awareness Training				✓

Service Description for Cyber-Security Service

Meetings and Reports

Monthly client Security meeting assets

Managed Security Service Report

- Show the value of your service
- Agree on what needs to be addressed
- Send in advance of the meeting

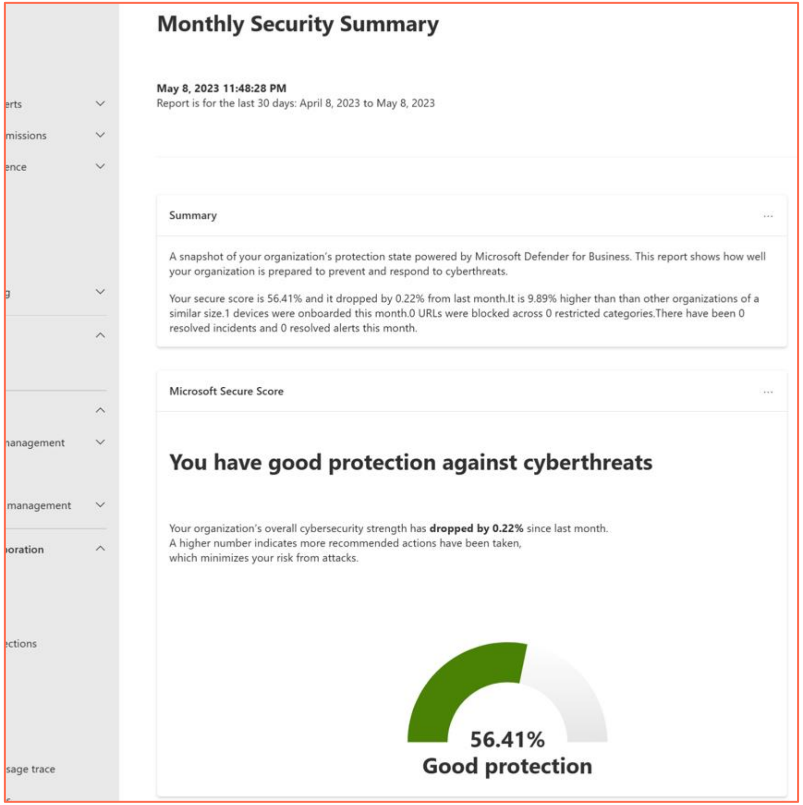
Risk Status Report

- Who’s risk? Yours or the Clients
- Document it and share with Client
- Show it every month

Our MSA includes Cyber-Security

Managed Security Service Report

Why is it so useful   [Reports in Microsoft Defender for Business | Microsoft Learn]



Monthly Security Summary

May 8, 2023 11:48:28 PM
Report is for the last 30 days: April 8, 2023 to May 8, 2023

Summary

A snapshot of your organization's protection state powered by Microsoft Defender for Business. This report shows how well your organization is prepared to prevent and respond to cyberthreats.

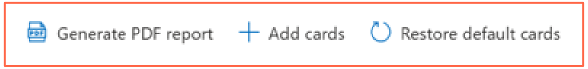
Your secure score is 56.41% and it dropped by 0.22% from last month.It is 9.89% higher than than other organizations of a similar size.1 devices were onboarded this month.0 URLs were blocked across 0 restricted categories.There have been 0 resolved incidents and 0 resolved alerts this month.

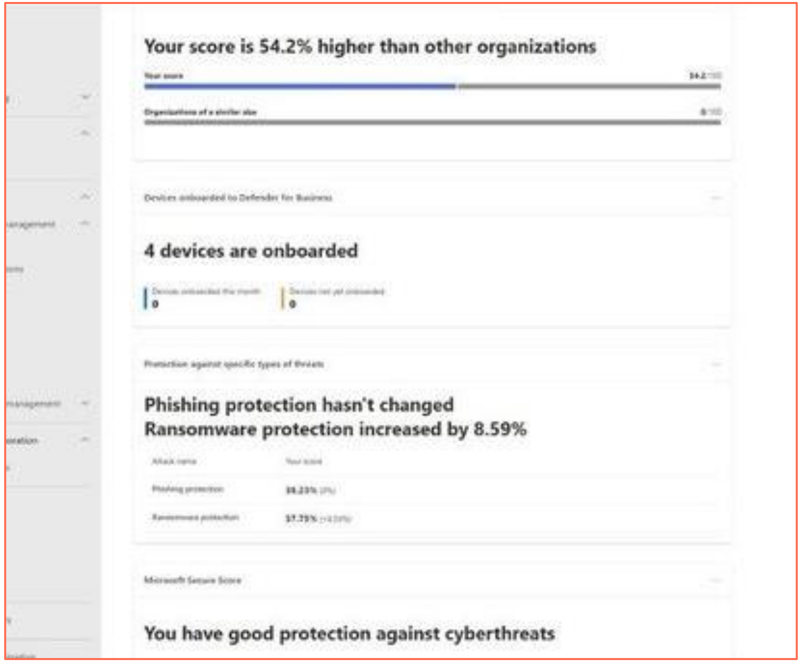
Microsoft Secure Score

You have good protection against cyberthreats

Your organization's overall cybersecurity strength has **dropped by 0.22%** since last month.
A higher number indicates more recommended actions have been taken,
which minimizes your risk from attacks.

56.41%
Good protection





Your score is 54.2% higher than other organizations

Your score 54.2/100

Organizations of a similar size 8/100

Devices onboarded to Defender for Business

4 devices are onboarded

Devices onboarded this month 0
Devices not yet onboarded 0

Protection against specific types of threats

Phishing protection hasn't changed
Ransomware protection increased by 8.59%

Attack name	Your score
Phishing protection	38.23% (0%)
Ransomware protection	57.75% (+8.59%)

Microsoft Secure Score

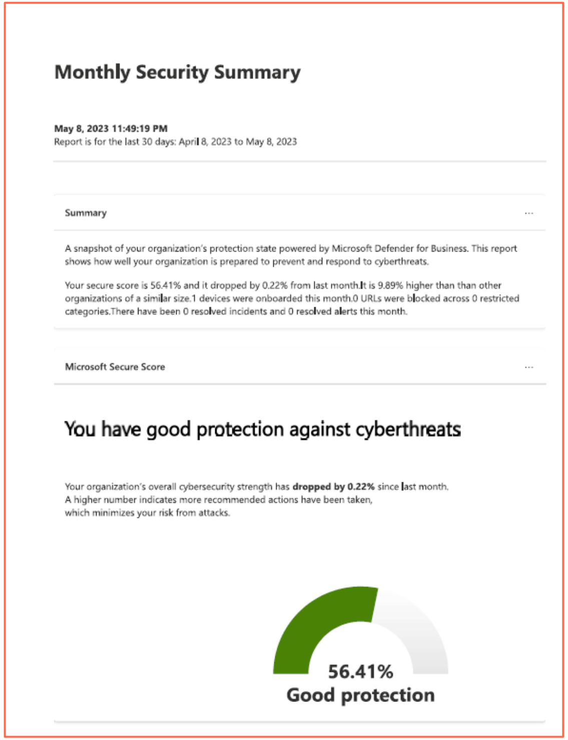
You have good protection against cyberthreats

rhipe
A Crayon company

Report pdf

Why is it so useful

[Reports in Microsoft Defender for Business | Microsoft Learn]



Monthly Security Summary

May 8, 2023 11:49:19 PM
Report is for the last 30 days: April 8, 2023 to May 8, 2023

Summary ···

A snapshot of your organization's protection state powered by Microsoft Defender for Business. This report shows how well your organization is prepared to prevent and respond to cyberthreats.

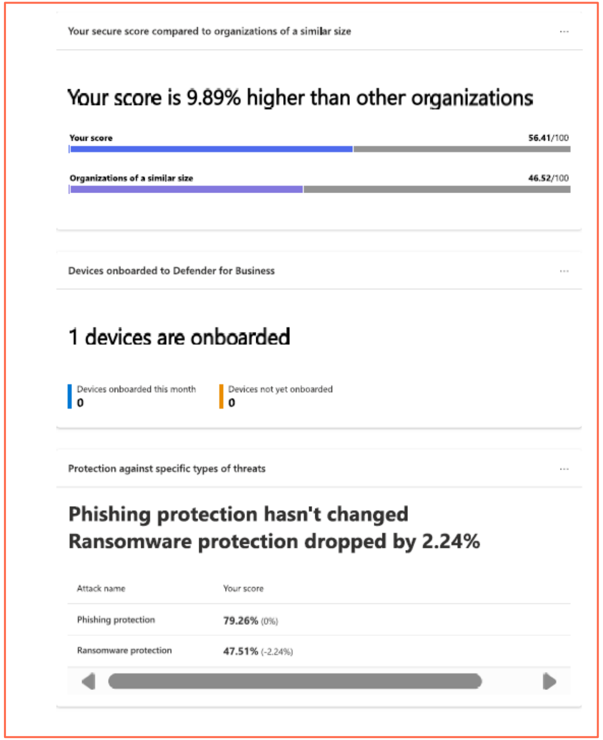
Your secure score is 56.41% and it dropped by 0.22% from last month.It is 9.89% higher than than other organizations of a similar size.1 devices were onboarded this month.0 URLs were blocked across 0 restricted categories.There have been 0 resolved incidents and 0 resolved alerts this month.

Microsoft Secure Score ···

You have good protection against cyberthreats

Your organization's overall cybersecurity strength has **dropped by 0.22%** since last month.
A higher number indicates more recommended actions have been taken,
which minimizes your risk from attacks.

56.41%
Good protection



Your secure score compared to organizations of a similar size ···

Your score is 9.89% higher than other organizations

Your score **56.41**/100

Organizations of a similar size **46.52**/100

Devices onboarded to Defender for Business ···

1 devices are onboarded

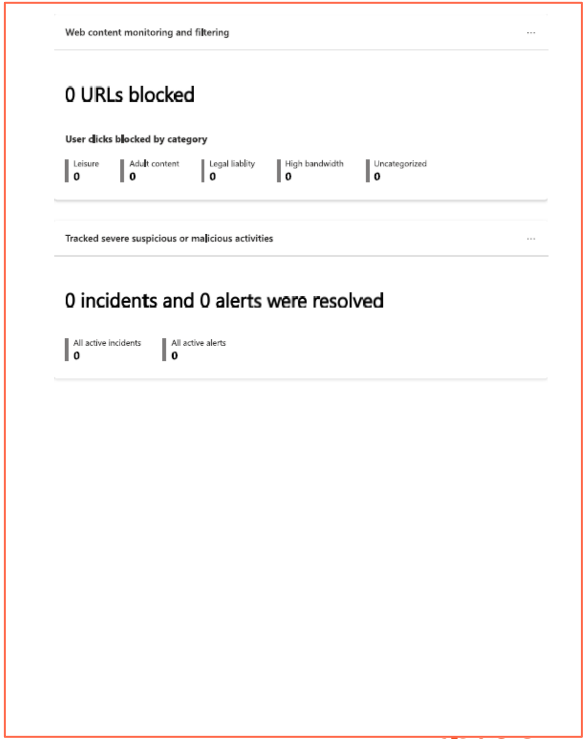
Devices onboarded this month
0

Devices not yet onboarded
0

Protection against specific types of threats ···

Phishing protection hasn't changed
Ransomware protection dropped by 2.24%

Attack name	Your score
Phishing protection	**79.26%** (0%)
Ransomware protection	**47.51%** (-2.24%)



Web content monitoring and filtering ···

0 URLs blocked

User clicks blocked by category

Leisure	Adult content	Legal liablity	High bandwidth	Uncategorized
0	**0**	**0**	**0**	**0**

Tracked severe suspicious or malicious activities ···

0 incidents and 0 alerts were resolved

All active incidents	All active alerts
0	**0**

rnipe
A Crayon company

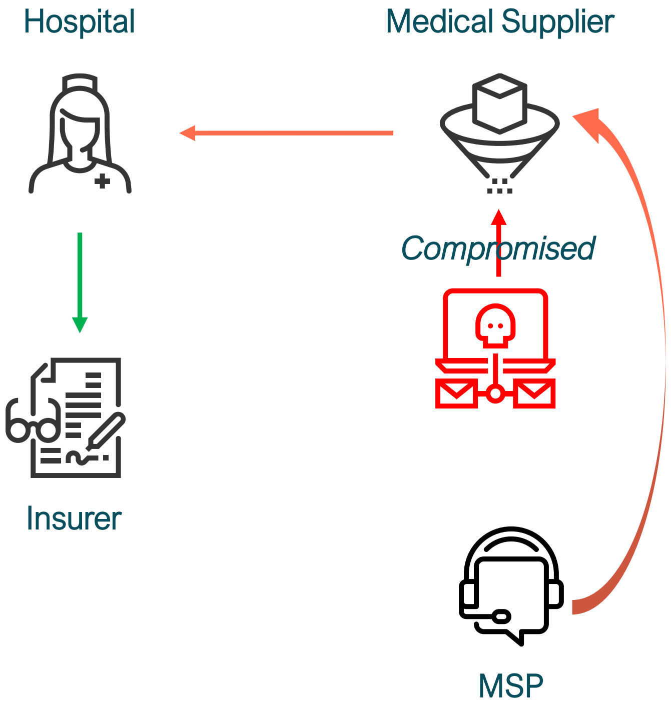
Risk Status Report

Why is it so important

Risk Status Report for Jedi Engineering							
Case No	Risk Title	Description	Notification Date	Client informed	Client Accepts	Comments and Date	Status
17	Some risky applications have been downloaded by users	End user are not happy with restrictions as they believe it is impacting their productivity	24/11/2022	Yes	TBA	29/11/23 Client will raise the issue at the next Executive Management meeting, in time for next Security Service meeting	Action Req
16	Some Admin Accounts are over priviledged	Certain Executives said they need to make changes on the M365 tenant if their team members have problems, because IT is too slow to respond.	13/09/2023	Yes	Yes	19/09/23 Client will raise the issue at the next Executive Management meeting, in time for next Security Service meeting. 29/09/23 Issue resolved Management agreed only IT MSP are allowed to make changes	Resolved

Risk & Insurance

Why is it so important



Claim Denied reasons

- Failure to maintain or follow an ongoing program or minimum standards
- Discrepancies, errors, omissions, or ambiguity in completing the initial risk assessment
- Event of an attack, the compromise occurred before the cyber insurance was purchased
- Ransomware by organizations deemed nation-state actors may be acts of war
- Conducting your own initial forensic discovery

Building a Security Practice with Crayon & Microsoft Business Premium

	Front End Operations	Back End Operations	Sell and Market
Key Action	• Use ASD-8 and other attributes to establish your Security Baseline or Baselines • Translate your Baseline to a Service Description for Managed Security	• Technical Enablement on: • Defender for Business • Defender for Office • Intune and AAD • Enablement on Crayon deployment & config scripts • Defender for Business • Defender for Office • AAD Px	• Sell M365 Business Premium uplift or new using Security and Security Assessments (for your sales team) • Conduct your own Security workshop using Do More with Microsoft 365 Business Premium
Partner Action	• Understand what other products you need to supplement and meet the Controls in your Baseline • Build you Service Description and fit it into your Master Services agreement • Understand what Security Baseline is right for your market and your clients	• Technicians and Engineers attend the Crayon in person Security Workshops • Technicians and Engineers attend SMB Masters series • Obtain Microsoft Cloud partner program certs for Modern Work or Security (recommended)	• Invite approx. 20 of your clients and prospects to a Do More with Microsoft 365 Business Premium, Security workshop • Learn how to use a Security assessment to engage with the client or prospect
Collateral (underlined means we provide this)	• ASD-8 mapped to the Microsoft Security platform Sample • Business Premium full Service Description with Add-Ons Document • Sample Service Description • Risk Report Sample • Monthly client Security Meeting use Secure Score Summary Report	• Enablement Training Slide Deck recording • Crayon deployment & config Scripts • Crayon Documentation • Complete set of Documentation on how to implement CISv8 controls with Microsoft Security functions found in Business Premium	• A Microsoft funded Do More with …. workshop using Crayon developed materials that you can customize for your own use • How to create and use a simple but effective low-cost Security Assessment • A comprehensive Security Assessment for clients that require Proof of Preparedness • Coming soon, Penetration Testing Service for clients that require Proof of Readiness

For qualifying Partners

Assets

Useful links

- Reports in Microsoft Defender for Business | Microsoft Learn Admin Portal > Security > Settings > Endpoints > Advanced features > Preview Features. Preview Features settings bottom of the page
- ACSC Essential Eight - Essential Eight | Microsoft Learn
- Service Description Focus Business Premium with Add-ons

rhipe

A Crayon company

Thank you for joining us

rhipe

A Crayon company

Questions

Questions and Open Forum