Elysian:IT

Microsoft Partner
Microsoft
Gold Cloud Platform
Gold Cloud Productivity
Gold Datacenter
Silver Enterprise Mobility Management
Silver Collaboration and Content

CYBER ESSENTIALS PLUS

nqa
ISO 27001
INFORMATION SECURITY MANAGEMENT

Security Whitepaper

Key Microsoft Security Features

Version 1.0

Authors

Brendan Cavanagh – Technical Architect

November 2023

Microsoft 365 Windows Microsoft Azure

Acknowledgements

This whitepaper was created by our Technical Architect Brendan Cavanagh. Brendan has an extensive background in on-premise infrastructure starting from Server 2008 through to the current Server 2022, and cloud technologies like Microsoft 365 and Microsoft Azure. Brendan has helped dozens of organisations ranging from SMB's to Enterprise, to deploy Microsoft technologies like Microsoft Intune, Security and Compliance, SIEM integrations and migrations from various platforms into the Microsoft ecosystem. He brings a wealth of experience not only in honing the full potential of Microsoft licensing but bridging the gaps between Microsoft technologies and 3rd party services.

Brendan has written this paper with the intent of highlighting some of the available Microsoft technologies and how they can help to fulfil requirements within most businesses.

Point of Contact

For further information regarding the contents of this document, then please contact the following:

email: info@elysianit.com
telephone: +44 1256 976650

Copyright

Contents

1. Background

ElysianIT are a Microsoft Gold and Solutions Partner, established in 2014. We provide professional services/consulting and Managed Support with staff that have extensive experience of Microsoft on-premise and cloud services, working with Microsoft 365, Azure, Entra ID (fka Azure AD), Active Directory, Windows server and desktop clients and Enterprise Mobility and Security (EMS), alongside the second-generation cloud products that are now reaching maturity, including elements such as the Power Platform and Azure PaaS services.

Our heritage comes from the design and implementation of Microsoft on-premises technologies, ranging from Exchange, SharePoint and System Centre through to Active Directory, Public Key Infrastructure and Windows Client Deployments. As Microsoft have transitioned their own key focus to cloud services, we have followed suit, developing a wide-ranging experience across the product stack as they have reached maturity over the last 8 or so years.

We pride ourselves in building partnerships with our clients to identify targeted changes to technologies which provide the business with multiple benefits. These include the end user experience of IT, increased productivity and security, and/or reduced overall costs.

ElysianIT are a managed services provider providing a range of services to clients requiring ongoing support, from remote 3rd line to full end user desktop and estate wide infrastructure management with an on-site presence. This includes the provision of Microsoft Cloud licensing via our Cloud Solutions Provider (CSP) relationship with Microsoft, through which we can provide customers with clear and concise advice regarding their licensing needs and provide them at competitive prices.

With our long-term heritage, working with public sector and private organisations we have developed a series of security baselines and processes inline with NCSC Guidance, CIS Benchmark and Microsoft Best Practices which we use to accelerate the design and build phases. These are known as our Zero to Hero security baselines.

We place great emphasis on building effective and trusted partnerships with our clients to identify targeted and considered changes to technologies which provide the business with multiple benefits. These include the end user experience of IT, increased productivity and security, and/or reduced overall costs.

1.1. Overview

This security paper lays out the available technologies from Microsoft, the features and benefits of these and what that roadmap should look like in terms of priority as well as the licensing required to deploy. If you are in a security role and have an investment in Microsoft technology, then this will provide a baseline for the technologies available and what they will deliver for you.

This whitepaper focuses on the following key Microsoft security features all organisations should be adopting:

1. **Phishing Resistant MFA** – Phishing Resistant MFA uses password-less methods of authentication such as Certificate Based Authentication (which requires a certificate to be a device before it can access the estate) and FIDO2 based security keys (which requires a physical hardware token to be put into the machine),
2. **Defender for Endpoint** – Most organisations focus exclusively on AV and firewall benefits, however the Attack Surface Reduction and EDR functionality of Defender for Endpoint expands further into automation and AI based technologies to proactively address threats and vulnerabilities before they happen. Additionally Attack Surface reduction disables elements of the operating system which are regularly exploited by hostile actors.
3. **Defender for Cloud Apps** – Defender for Cloud Apps monitors all web traffic through endpoints allowing businesses to discover the usage of Shadow IT. Pivoting from there additional controls, monitoring and alerting allows for access control around web usage and reverse web proxy functionality to apply restrictions such as copying, pasting, uploading or downloading. Additionally, Defender for Cloud Apps can work with Defender for Endpoint to manage Web Filtering across the estate.
4. **Password Protection** – The NCSC have produced a list of the top 100 000 most exploited passwords. This list can be ingested into Entra ID to prevent users from being able to use any of those identified passwords and therefore reduce the risk that a password spray attack will successfully compromise their account. Furthermore, depending on licensing, this functionality can be extended into the on-premise allowing organisations to restrict passwords used on Active Directory mastered identities.
5. **Azure Identity Protection** – User accounts, activity, sign-in's and access can be fed through a technology called Azure Identity Protection to leverage AI to identify and block potentially malicious activities (for example a compromised account) or malicious user activity before it happens. This is done by either blocking the sign-in or requiring an MFA response to verify the users identity. This effectively means applying "intelligence" to the conditions that allow/disallow a user access to corporate data but taking into consideration their behaviours, locations or activities.
6. **Defender for Endpoint (Vulnerability Management)** – Advanced Vulnerability Management allows for the ability to block the use of risky applications (for example due to risky versions or out of data applications) as well as limit the use of web browser extensions through their management portal. In addition to the above this feature set can monitor BIOS firmware versions highlighting to IT professionals that upgrades are required.
7. **Microsoft Purview** – With GDPR and compliance standards being a topic of utmost importance right now it's more relevant than ever that businesses begin the process of outlining requirements and defining a suitable compliance solution to meet those requirements. Microsoft Purview will provide the means for labelling and protecting content

through features like Sensitivity Labels, Data Loss Prevention and the associated auditing technologies around them.

These are discussed in more detail in the subsequent sections, summarising the technology, the key benefits, when Your organisation are currently licensed for the technology and what the licensing and cost implications would be if they are not.

1.2. Recommendations Summary

To help you to prioritise the implementation of the discussed security services we have developed the following table.

Feature	Priority	Value
Phishing Resistant MFA	1	Provides the most resilient MFA offering to protect identities
Defender for Endpoint	2	Protects endpoints from viruses, malware, misconfigurations and risk generally
Defender for Cloud Apps	3	Allows for the monitoring of web-site access and controls around doing so (allow/block), additionally provides extended security functionality around web usage.
Password Protection	4	Allows the restriction of specific passwords within the business
Azure Identity Protection	5	Implement AI driven monitoring around user activity, actions and sign-ins to protect against account compromise
Microsoft Purview	6	Allow the business to label content and apply controls around that labelled content, such as blocking the sending of confidential information externally

If you did only one item discussed in this report it would be the implementation of MFA to all users using Phishing resistant MFA as detailed in section 2.

A license assessment would need to be undertaken to understand which features would provide the best value. ElysianIT can help with this review and is a core part of our Zero-to-Hero offerings discussed in the next section.

1.3. Our Offerings

At ElysianIT we have a number of offerings to help to accelerate the deployment and configuration of Microsoft Security and Compliance features as discussed in this report.

Below is a highlight of these offering:

- **Zero-to-Hero Security** - This service delivers to your business a implementation of the core Microsoft 365 Security and Microsoft Defender features such as Microsoft Endpoint Manager (aka Intune), Azure Active directory, Microsoft Intune Endpoint/App protection, we call this our Zero-to-Hero security baseline. At the end of the “build and test” phase, we will support you through a pilot to trial the implementation of a well-constructed, secure architecture. The output of this service is an environment which is understood and appropriate for your real-world requirements. For more information please see section 2.3.1.
- **Zero-to-Hero Endpoint Protection** – Deployment of Microsoft Defender for endpoint providing support for App Governance, Web Filtering, Indicators, URL authorisation, vulnerability scanning, zero-day threat, malicious actor protection. For more information please see 3.3.1.
- **Zero Trust Service Accelerator** - Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network. Regardless of where the request originates or what resource it accesses, the Zero Trust model teaches us to "never trust, always verify.“ Our service implements the conditions, controls and policies to protect your organisation. For more information please see section 4.3.1.
- **Zero-to-Hero Compliance** - Focused on Content Classification (Sensitivity Labels) and Data Loss Prevention using Microsoft Purview. Classifying and labelling content is a key element to compliance, once you classify your content you can start monitoring, reporting and controlling it effectively. For more information please see section 7.3.1.

Each of our Zero-to-Hero offerings are typically delivered within a two-week period.

2. Phishing Resistant MFA

As security technologies have improved so has the rising use of the term “Phishing Resistant” Multi-Factor Authentication. This refers to a set of technologies that provide multiple factor responses to a user authentication request but do so in such a way that they are resilient against typical hacker man-in-middle attacks. The focal idea around “Phishing Resistant” MFA is that users do not type their usernames or passwords in, or use a passwordless sign-in, to connect to corporate resources. Because the users do not enter these credentials (password) there is no risk of a hacker seeing or having the opportunity to capture these credentials and impersonate the user.

Phishing Resistant MFA comes in three options:

- **Certificate Based Authentication**: A certificate is installed on devices that is used during authentication. This requires certificate infrastructure to support this service. Without the certificate being installed there can be no connection.
- **Security Keys:** A physical key called a FIDO2 key (think USB stick) is plugged into the device you are trying to sign-into. This requires certificate infrastructure to support this service.
- **Windows Hello for Business:** Biometrics and a PIN can be used to sign-into devices, supported on-premise resources and cloud applications. Due to recent changes, the introduction of Cloud Trust specifically, Windows Hello for Business is now highly sort after to meet general business needs. This does not require certificate infrastructure to support this service.

2.1. Benefits

Users would have access to using biometric signals to sign-into devices and access on-premise resources such as file shares. As users are no longer continuously signing in with their credentials it reduces the risk that a hacker phishes or obtains these credentials through social engineering.

2.2. Licensing Information

The following table breaks down each license and its associated features.

Plan	What’s included
Entra ID Free	Entitlement to enable each of the Phishing Resistant MFA technologies

2.3. Offerings

ElysianIT have the following offerings available to help accelerate the deployment of this solution:

2.3.1. Zero to Hero Security

The ElysianIT “Zero to Hero Microsoft 365 Security” service delivers your business a implementation of the core Microsoft 365 Security and Microsoft Defender features such as Microsoft Endpoint Manager (aka Intune), Azure Active directory, Microsoft Intune Endpoint/App protection, we call this our Zero-to-Hero security baseline. At the end of the “build and test” phase, we will support you through a pilot to trial the implementation of a well-constructed, secure architecture. The output of this service is an environment which is understood and appropriate for your real-world requirements.

The Zero to Hero Package is designed to give organisations a quick-start baseline environment to immediately take advantage of enhanced security in just 2 weeks and start getting value from their Microsoft 365 licenses.

Benefits:

- Has concerns about verifying access to corporate data / systems, particularly from external sources such as mobile workers
- Has high overheads, both in man hours and productivity, from remedying forgotten passwords
- Wants to secure and protect corporate data on end user devices to reduce the chances of data breaches
- Would like to gain Cyber Essentials Plus for the Microsoft 365 Workloads

Service Offering

The Zero to Hero service provides the following Security service implementation:

- Conditional Access Policies to protect the environment against hostile actors accessing corporate data via account compromise as well as restrict user access where desired.
- Multi-Factor Authentication (MFA) – This will be configured so that when users are outside of the corporate network, they are prompted for a secondary form of authentication
- Block Legacy protocols
- Risk-based authentication to block access and logon risk. Required to enable MFA
- Self-Service Password Reset (SSPR) – configure and enabled Self-Service Password Reset
- Intune Polices to enable:
- Mobile Intune App Protection – enable mobile application management policy to protect core Office apps across Android and iOS for Bring Your Own Devices
- Device Policies to restrict legacy Android, iOS and Windows Devices from accessing your tenancy
- Technical Documentation – detailed documentation of configured services and user guides for MFA and SSPR
- Admin Oversight and Handover – Technical walkthrough for System Admins (limited to 3 people) and run though of Technical Documentation

Typical Engagement Approach

The Zero to Hero service engagement approach is detailed below:

- Workshop –remote session to provide an overview of the Microsoft EM+S product suite and audit existing environment
- Documentation – Provide recommendations based on the audit and define prerequisites
- Implementation – Configure the services as detailed in the service offering

- Documentation Update – Finalise documentation based on configuration and complete user guide
- Admin Oversight and Handover – remote technical training and handover

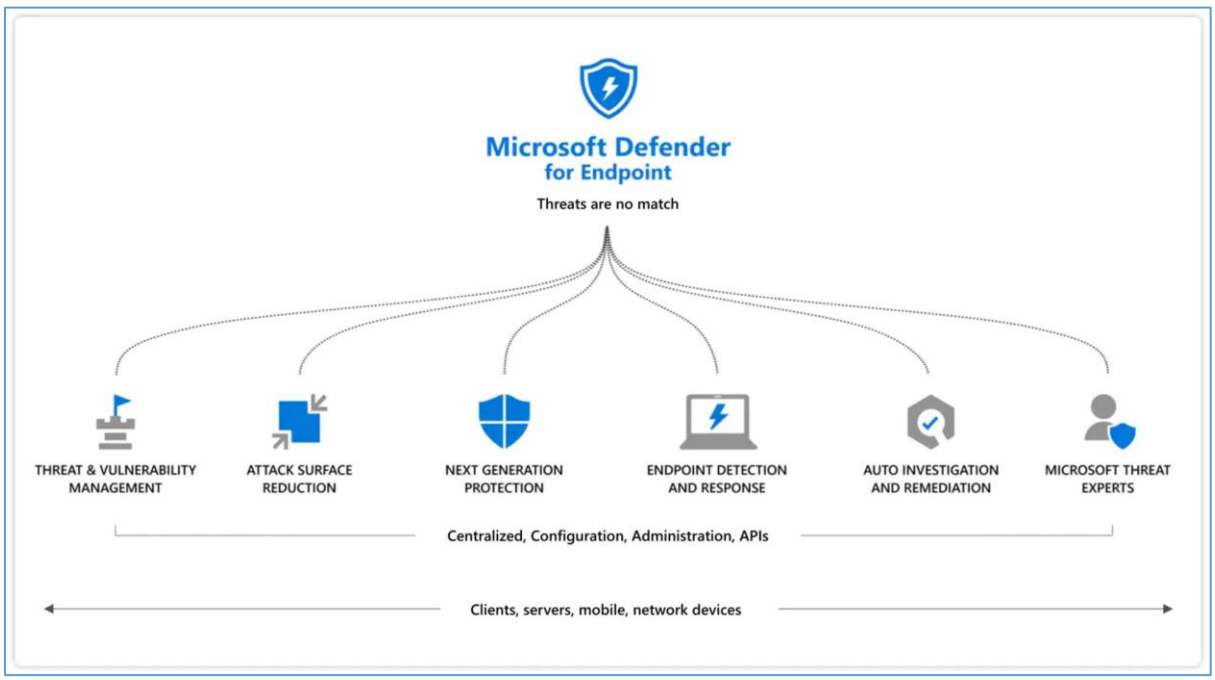
Contact us at info@elysianit.com for pricing and more information.

3. Defender for Endpoint

Defender for Endpoint is Microsoft's endpoint security product. It's focused around detecting vulnerabilities, malicious file content and malicious behaviour on endpoints and either providing information to administrators of this activity, or automatically remediating threats.

Most organisations use Defender for Endpoint to protect devices in a simple sense, using Anti-Virus Enhancement and likely some of the Attack Surface Reduction functionality. Largely though, a sizeable chunk of the available features in Defender for Endpoint are left unconfigured. Fully leveraging these features will result in a more proactive stance where businesses can detect vulnerabilities and misconfigurations in advance of them happening, offering IT professionals the opportunity to act proactively, avoiding these risks manifesting.

Defender for Endpoint Vulnerability Management expands on the existing Defender for Endpoint Plan 2 functionality by leveraging Microsoft threat intelligence. Vulnerability Management will perform assessments of machines, risk based prioritisation, includes built-in remediation functionality.



3.1. Benefits

Some of the important features that Defender for Endpoint includes:

- Vulnerability management
  - Scanning of systems for misconfigurations or vulnerabilities
  - Includes recommendations on remediation of the above
- Endpoint Detection and Response leverages Microsoft's interconnected web of signals and backend AI that identifies threats and addresses them proactively where possible and reactively where identified
- Management of alerts and incidents through the Microsoft Security Portal as "tickets" which can be assigned, noted, and closed when completed.
- Automatic remediation
  - In certain cases the system is able to automatically fix vulnerabilities
- Integrations with other Defender services like Defender for Cloud Apps and Defender for Office 365 and the Compliance features to provide advanced functionality like Endpoint DLP to prevent transfer of data to USB devices and even websites like Google Drive or attaching content to 3rd party webmail.
- Device Tagging and Device Groups to manage automation and allow for granular policy assignment.
- Custom "indicators" which are basically a means of allowing or blocking access to certain file hashes, URL's, IP Addresses, domains or certificates.
- Web content filtering
  - Block categories of what Microsoft have deemed to be "work inappropriate" content such as gambling, violence, social media, pornography etc.
  - These categories can be modified as needed

This solution is different to a standard Anti-Virus in the sense that they are usually dependant on receiving updates in order to be considered "current", with Defender for Endpoint your endpoints are effectively connected to Microsoft's backend at all times (as long as they have an internet connection) and are therefore able to stream telemetry regarding potential compromises, malicious code or misconfigurations directly to Microsoft for assessment.

3.2. Licensing Information

The following table breaks down each Defender for Endpoint license and its associated features.

Plan	What's included
Defender for Endpoint Plan 1	- Next-generation protection (includes antimalware and antivirus) - Attack surface reduction - Manual response actions - Centralized management - Security reports - APIs - Support for Windows PC, iOS, Android OS, and macOS devices
Defender for Endpoint Plan 2	All of the Defender for Endpoint Plan 1 capabilities, plus: - Device discovery

	- Device inventory - Core Defender Vulnerability Management capabilities - Threat Analytics - Automated investigation and response - Advanced hunting - Endpoint detection and response - Endpoint Attack Notifications - Support for Windows (client only) and non-Windows platforms (macOS, iOS, Android, and Linux)
Defender for Endpoint Vulnerability Management Add-on	- Discover, assess and remediate misconfigurations or threats on user endpoints. For example show devices susceptible to Log4j vulnerability and provide guidance on remediating the issue - Warn on or block vulnerable versions of applications. For example if MS identify a vulnerable version of Adobe Reader, that specific version could be blocked from use requiring the user to undergo an update before proceeding - Monitor compliance against industry standards like ISO27001 - Provide a continuous assessment and score for Your organisation against other similar industries and businesses - Capture and illustrate via a portal, which Applications and Browser Extensions are being used across all Your organisation devices and provide risk score assessments for each - Allows for centralised remediation through the Microsoft Security portal to deploy automatic resolutions for application and configuration vulnerabilities. - The ability to scan hardware and firmware on devices and receive recommendations from Microsoft on which remediation steps need to be taken to address the risk.

3.3. Offerings

ElysianIT have the following offerings available to help accelerate the deployment of this solution:

3.3.1. Zero-to-Hero Endpoint Protection

Defender for Endpoint Protection is a security service that protects your endpoints from malicious software (malware) and actors (hackers) such as viruses, spyware, and other potentially harmful software or websites.

Our Endpoint Protection service is underpinned by Microsoft Defender and Azure AD which are industry-leading antimalware, attack surface reduction, and device-based conditional access.

Endpoint Protection provides a Unified security tool which has a centralised management dashboard.

Our Endpoint Protection Services provides the following:

- Overview of Endpoint Protection covering:
- Defender for Endpoint

- Defender for Cloud Apps
- Azure AD P1
- Design of endpoint protection service to meet your organisational needs
- Implementation of the Design service
- Documentation and Handover of the admin operational tasks

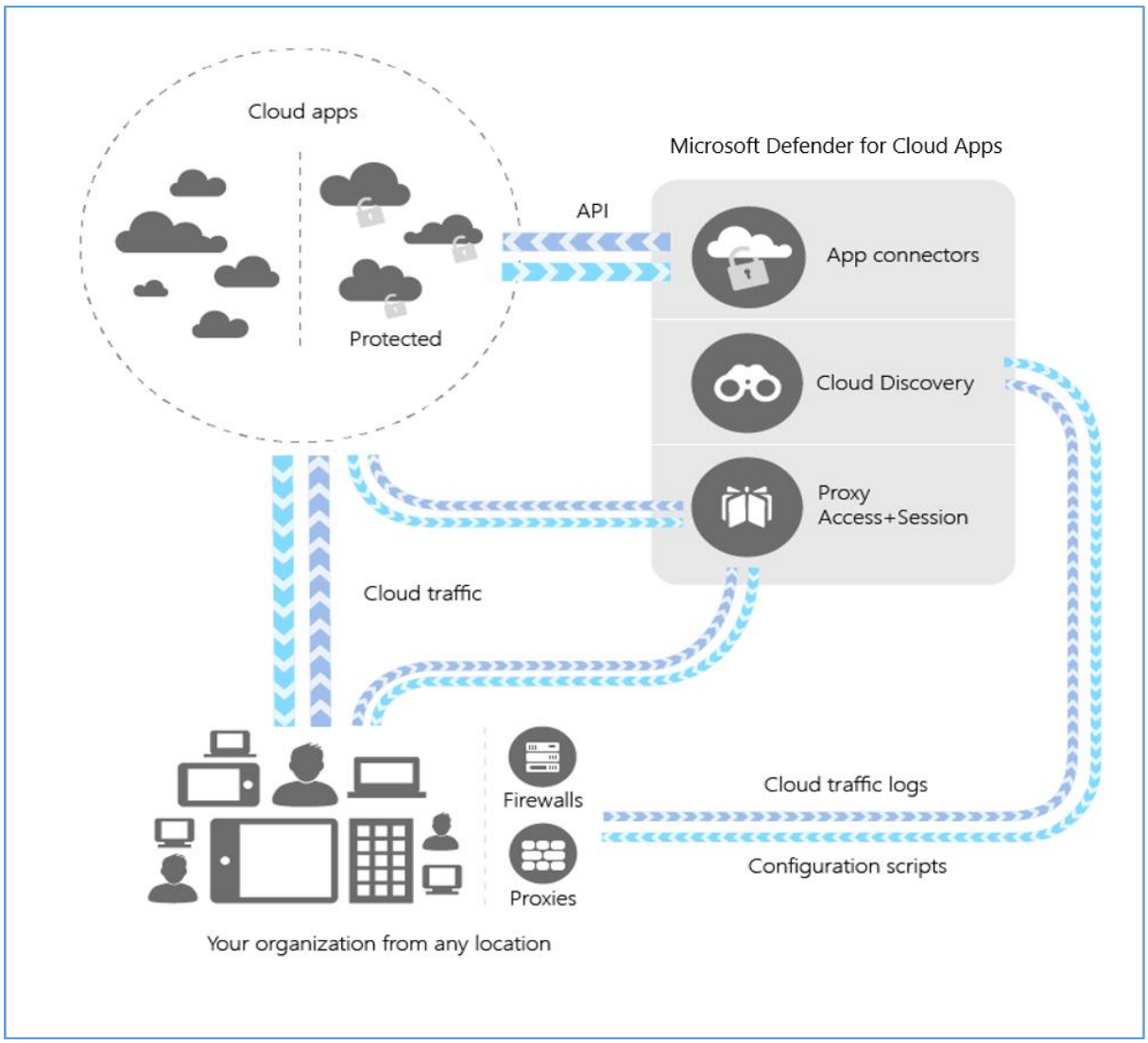
Contact us at info@elysianit.com for pricing and more information.

4. Defender for Cloud Apps

Defender for Cloud Apps simply put is a solution that sits between a user's desktop or laptop and the internet. It gathers telemetry on which websites are being accessed, who's accessing them, where they are being accessed from etc. In addition to those elements, it also becomes a system that can manage user interactions with those websites (i.e.: Block access, warn, monitor, prevent copying, pasting, downloading etc.).

It's important to note that Your organisation's culture is not one of an "Iron Fist" when it comes to monitoring and controlling user access to websites but it's in Your organisation's best interest to maintain a service like Defender for Cloud Apps if even from the perspective of being able to audit these activities in the event of a breach or malicious attack.

In addition to the above surface level features Defender for Cloud Apps offers a feature called File Monitoring which will, in detail, provide an audit trail of data being accessed via SharePoint or OneDrive and give a line by line break down of what user actions have occurred around that data, for example the actions of sharing a file, the recipient accessing the file, authenticating to verify their identity and opening, editing and closing that file. It's truly one of the most detailed audit trails available within the Microsoft suite.



4.1. Benefits

Defender for Cloud Apps integrates with solutions like Defender for Endpoint and Microsoft Sentinel further adding to the concept of a centrally managed ecosystem. Defender for Cloud Apps also includes the following big-ticket features:

- Discover the user of Shadow-IT, or web applications, that your users may be accessing without your knowledge.
    - A good example would be users opening up a website like Dropbox, Google Drive etc and potentially saving confidential information there.
- Web Application Governance provides the ability to allow, monitor or block access to websites with a simple process.
- Apply policies to alert on, control or mediate access to Web Applications
    - A good example would be to prevent guest users from downloading, copying or pasting information from your SharePoint
    - Another would be to prevent users from setting up forwards on their corporate email accounts to external webmail clients like Gmail or Outlook.com
- All of the above can be done granularly as well through Scoped Profiles, meaning you can for example block access to a website for 90% of the business and allow it for 10% or vice versa.

4.2. Licensing Information

The following table breaks down each Defender for Endpoint license and its associated features.

Plan	What's included
Microsoft 365 E5, Office 365 E5 or Microsoft 365 F5 **Separately the Microsoft 365 E5 Security or Compliance licenses, The EMS E5 or Microsoft F5 Security or Compliance standalone licenses will provide this functionality.**	- Shadow IT Discovery - Web Application Reporting and Monitoring - Reverse Proxy Brokering for Web Applications - Web filtering - Integration into non-Microsoft 3rd party applications via SSO - SIEM integration - Information Protection - Data Loss Prevention

4.3. Offerings

ElysianIT have the following offerings available to help accelerate the deployment of this solution:

4.3.1. Zero Trust Accelerator

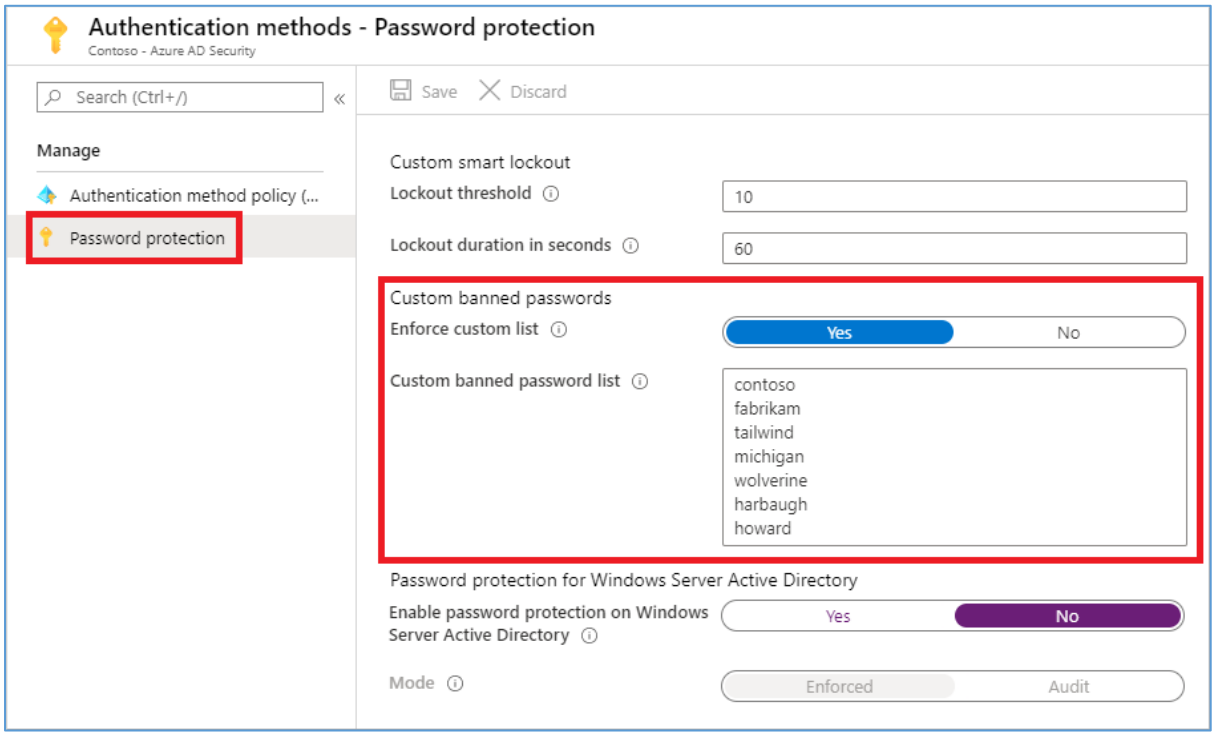
Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network. Regardless of where the request originates or what resource it accesses, the Zero Trust model teaches us to "never trust, always verify." Our service implements the conditions, controls and policies to protect your organisation

Contact us at info@elysianit.com for pricing and more information.

5. Password Protection (Custom Block List)

Azure Password Protection is a feature that allows an organisation to define a list of passwords that are not permitted to be used. The NCSC provide a list of 100 000 most used passwords seen in cases of compromise that can be filtered down and imported (as there is a limit of 1000 that can be imported) into your estate to prevent their use.

It should be noted that with MFA in place there is less emphasis on passwords however it may still be a concern and consideration for Your organisation as an organisation.



5.1. Benefits

The benefit of Password Protection is that it would allow Your organisation to specifically restrict the use of certain passwords going forward. Additionally, by importing the top 1000 common passwords (filtered down based on existing Your organisation password policy) Your organisation would be able to implement a password protection policy preventing users from potentially using highly risky passwords.

5.2. Licensing Information

The following table breaks down each license and its associated features.

Users	Microsoft Password Protection with banned password list	Microsoft Entra Password Protection with custom banned password list
Cloud-only users	**Microsoft Entra ID Free**	**Microsoft Entra ID P1 or P2**
Users synchronized from on-premises AD DS	**Microsoft Entra ID P1 or P2**	**Microsoft Entra ID P1 or P2**

Note: On-premises AD DS users that aren't synchronized to Microsoft Entra ID also benefit from Microsoft Entra Password Protection based on existing licensing for synchronized users.

5.3. Offerings

ElysianIT have the following offerings available to help accelerate the deployment of this solution:

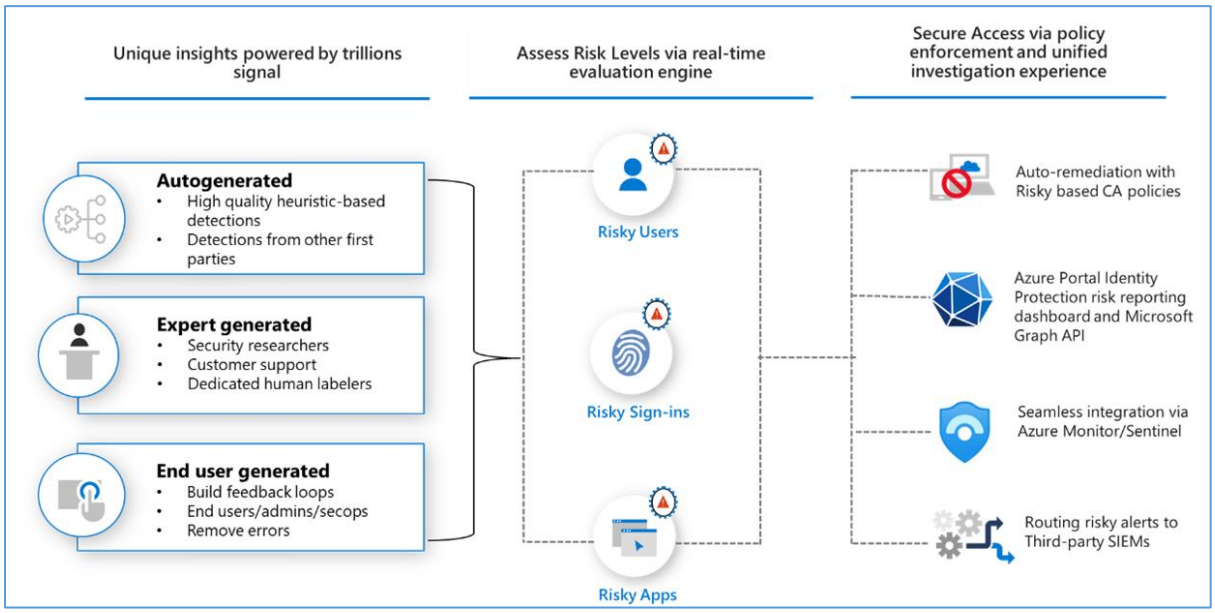
5.3.1. Zero-to-Hero Security

See our Zero to Hero Security offering in Section 2.3.1

Contact us at info@elysianit.com for pricing and more information.

6. Azure Identity Protection

Azure Identity Protection is a feature that applies Microsoft analytical backend analysis to user activity and sign-ins. What this means is that Microsoft tracks what is deemed to be typical behaviour for a specific user, and should the users deviate from this “baseline” then the system will analyse this behaviour and apply a risk score to that user.



6.1. Benefits

With the concept of a “Risk Score” now implemented using Identity Protection, policies can be configured to perform certain automated actions based on that risk score such as requiring MFA, blocking access, or having the user reset their password (Your organisation would be able to choose).

This becomes highly valuable in picking up instances where a user has become compromised or is acting in a potentially harmful manner to the business as it would effectively leverage automation to pick up this behaviour and act to protect the business from harm.

Some of the risky behaviour that Azure Identity Protection looks for include:

- Anonymous IP address use
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray
- and more...

6.2. Licensing Information

The following table breaks down each license and its associated features.

Plan	What's included
Microsoft Entra ID P1	- Security reports for Risky Users and Sign-ins - Security reports for Risk Detections
Microsoft Entra ID P2	- All features of P1 - Risk Policies for Risky Users and Sign-ins - Notifications - MFA registration policy

6.3. Offerings

ElysianIT have the following offerings available to help accelerate the deployment of this solution:

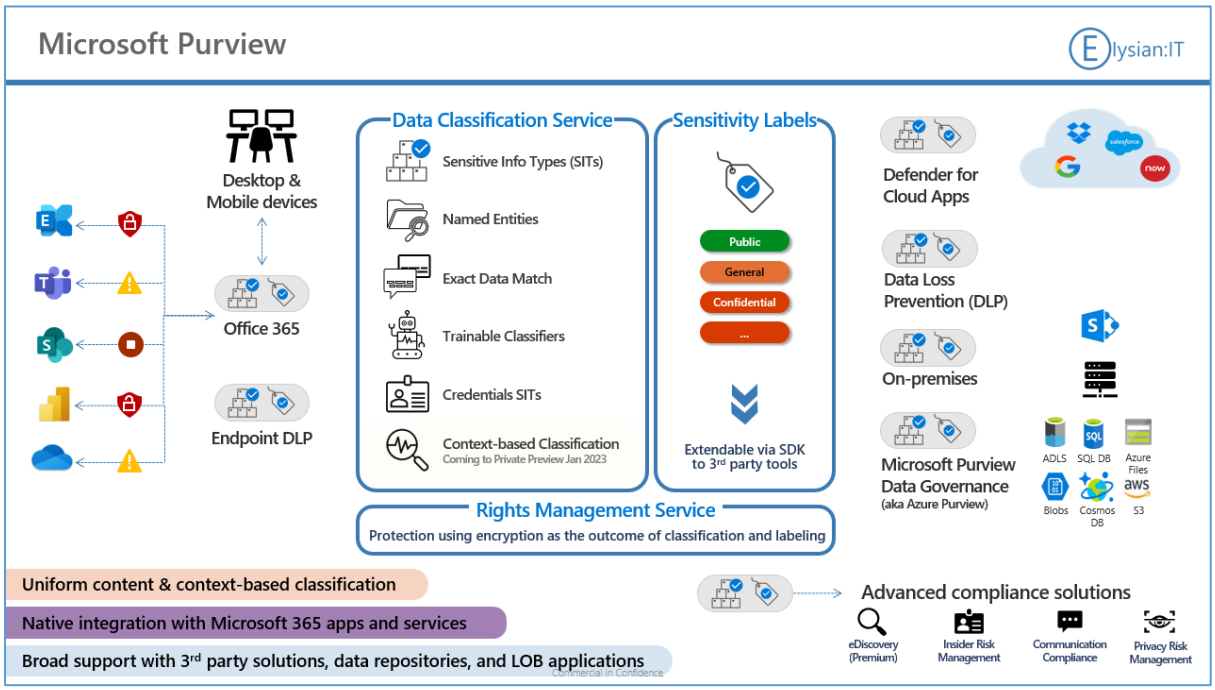
6.3.1. Zero-to-Hero Security

See our Zero to Hero Security offering in Section 2.3.1

Contact us at info@elysianit.com for pricing and more information.

7. Microsoft Purview

A challenge for any organisation is the management of its data, especially when there are processes like ISO27001 and GDPR to consider. On top the stress of processes you have the risk of a fine or damage to reputation in the event that a leak of sensitive data occurs. Microsoft Purview is a compliance solution made up of a number of products all specialising in the ability to identity sensitive content and apply labels and controls around how that sensitive data can be interacted with.



7.1. Benefits

Enter Microsoft Purview, a suite of technologies from Microsoft all designed to help address this risk by allowing the business the option to:

- Scan through files and identify sensitive information where it exists, for example credit card numbers, names, NI numbers, passports etc.
- Allow users to manually apply labels to content so that they and other users understand how to work with that data based on its label.
- Scan through and either automatically apply labels to content or recommend on the most appropriate label based on the content itself.
- Apply automated controls if sensitive content is identified and labelled, for example if someone tries to share or email content containing credit card information, prevent them from doing so.
- Apply educational tips and pop ups to advise users on best practices where sensitive data is identified
- Apply retention policies to retain identified data for a period and purge it thereafter, this aids in “pruning” your data estate.
- Use Advanced Compliance Solutions to search for confidential information in places like local machines (C: Drive), user OneDrive’s etc. and provide advice and guidance to users on where this data would be more appropriately stored.

- Monitor user communications and highlight areas where inappropriate language might be used and inform the business of this activity.

7.2. Licensing Information

The following table breaks down each license and its associated features.

Plan	What's included
Business Premium, Microsoft 365 E3, A3, F3	- Sensitivity Labels - Sensitive Info Types (Bank numbers, NIN, CC's) - Custom Sensitive Info Types - Data Loss Prevention (Partial) - Reporting, monitoring and alerting
Microsoft 365 E5, Office 365 E5 or Microsoft 365 F5/A5 **Separately the Microsoft 365 E5 Security or Compliance licenses, The EMS E5 or Microsoft F5/A5 Security or Compliance standalone licenses will provide this functionality.**	- Sensitivity Labels - Data Loss Prevention - Endpoint Data Loss Prevention - Automatic/Recommended Labelling - Trainable classifiers, keywork dictionaries, regular expressions - Reporting, monitoring and alerting - Compliance assessments (ISO 27001 etc.) - Compliance Manager

7.3. Offerings

ElysianIT have the following offerings available to help accelerate the deployment of this solution:

7.3.1. Zero-to-Hero – Compliance

This Package is focused on Content Classification (Sensitivity Labels) and Data Loss Prevention. Classifying and labelling content is a key element to compliance, once you classify your content you can start monitoring, reporting and controlling it effectively.

This offering provides an overview of Purview Content Classification and the associated Data Loss Prevention (DLP) control of the content.

We will setup our baseline classification Labels and DLP Policies (in your M365 Tenancy) for you so you can test and run a short Proof of Concept to hone and crystallise your classification requirements to subsequently plan a rollout of the capability

Package Provides

- ❖ Workshop - Overview of the Classification and DLP Purview Toolset
- ❖ Proof of Concept - Implementation and Configuration of our Baseline Labels & DLP Policies (for PoC)
- ❖ PoC Baseline Kick off Activities (to ready your PoC Users)
- ❖ Review PoC Feedback

- ❖ Copy of the Workshop Presentation
- ❖ Next Steps Q&A

Benefits

- ✓ Provides you with an understanding of Purview Classification and DLP
- ✓ Demonstrable use of technology though a PoC
- ✓ Deployed Classification Labels & DLP Policies
- ✓ Review of Licencing entitlement for selected capability
- ✓ Provides you with a Next Steps “start point” aligned to Purview classification & DLP to meet your Compliance needs

Outcome

- ❖ “Jump start” to understanding and using Classification & DLP Policies
- ❖ Baseline Labels deployed & DLP Baseline Policies Configured
- ❖ PoC provides the context for rollout planning
- ❖ Enables you to make decisions on what to do next

Contact us at info@elysianit.com for pricing and more information.