LEVACLOUD

Health-ISAC NAVIGATOR PROGRAM

Do More With Less:

Safeguard your Healthcare Organization from Ransomware Attacks using Microsoft solutions you already own.

TABLE OF CONTENTS

WHAT IS RANSOMWARE?

The US Governments Cybersecurity & Infrastructure Security Agency (CISA) describes ransomware as an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

WHY SHOULD HEALTHCARE ORGANIZATIONS BE CONCERNED ABOUT RANSOMWARE?

A Jama health report investigating the trends in ransomware attacks on US Hospitals, Clinics and other Healthcare Organizations identified that attacks doubled between 2016 and 2021, exposing the personal health information of nearly 42 million patients.

The 2022 Cyberthreat Defense Report, which surveys 1200 qualified IT security decision makers and practitioners globally, across several industry verticals, including healthcare, revealed that among cyberthreats, ransomware and account takeover (ATO) attacks are poised to take over from malware as the top concern. 71% of the organizations surveyed were victimized by a Ransomware attack. 57% of those organizations paid the ransom to regain access to their data. The average ransom payment made by organizations to regain access to their data in Q4 of 2021 was $322,168, the report also shows that the payment amount is trending upwards significantly each year.

Why are organizations paying the ransom instead of simply restoring the impacted systems and data from a backup? The Cyberthreat report has uncovered that ransomware gangs are performing “Double Extorsion” ransomware attacks. After gaining access to the victim’s environment, they will exfiltrate a copy of the data prior to encrypting it, then threaten to expose the sensitive data in addition to data loss.

There is clear evidence that ransomware attacks are not going to slow down as we move through 2023. The mission of a cybersecurity program within the healthcare industry is more complex that other industries. Not only does it need to balance the confidentiality, integrity and availability of the organizations systems and sensitive data, it also must have a focus on enabling the organization to provide the best possible patient care, without putting the patient’s sensitive information, or even their life at risk.

HOW CAN HEALTHCARE ORGANIZATIONS SAFEGUARD THEMSELVES FROM RANSOMWARE USING SOLUTIONS THEY LIKELY ALREADY OWN?

All of our healthcare customers have made some level of investment into Microsoft. At the minimum they have Windows PCs and an Active Directory Domain on-premises. A lot of them also have also made investments into Microsoft 365.

Generally, when you look for information on how to secure your organization from ransomware attacks, the answers will include recommendations on products and solutions to buy and add-on top of other tools and solutions you already own. Our philosophy for security revolves around being proactive by building a strong, secure foundation prior to adding anything else. We also strongly recommend implementing a Zero Trust security model.

The recommendations in the following sections of this whitepaper will focus on how you can start to build a strong foundation using the Microsoft tools and licensing we commonly see across our customer base, reducing your attack surface and the potential for a ransomware attack to be successful.

ASSESS YOUR CURRENT SECURITY POSTURE

Before you can make any changes to your environment, you need a picture of the current state. There are a couple of tools you can use to achieve this.

MICROSOFT SECURITY AND COMPLIANCE TOOLKIT

This is a set of tools that you can download and use to analyze your Group Policy Objects. Microsoft has published GPOs that contain best practice security configurations (aka Security Baselines), using the toolkit you can compare your current configuration to the security baselines and make informed changes to better secure your environment. It includes security baselines for Windows 11, Windows 10, Windows Server, Microsoft Office, Microsoft Edge and other Microsoft products.

The toolset includes Policy Analyzer, Local Group Policy Object (LGPO), Set Object Security and GPO to Policy Rules. Policy Analyzer analyzes and compares GPOs, while LGPO helps automate local group policy management. Set Object Security enables security descriptor setting for Windows objects, and GPO to Policy Rules converts GPO backups to Policy Analyzer files.

MICROSOFT SECURE SCORE

Microsoft Secure Score is a tool to measure an organization's security posture, available on the Microsoft 365 Defender portal. It provides an overview of the score and recommends actions that can be taken to improve it, organized into groups (Identity, Device, Apps, and Data). The score is displayed as a percentage and can be viewed in different ways, including with planned score, current license score, and achievable score. The recommended actions are ranked based on points left to achieve, implementation difficulty, user impact, and complexity. The tool allows users to take action on recommendations, update the status of each action, add notes, and share links.

MICROSOFT PURVIEW COMPLIANCE MANAGER

Microsoft Purview Compliance Manager is a feature in Microsoft Purview that helps organizations manage their compliance requirements with ease and convenience. It provides pre-built assessments for common regulations, standards, and policies, or custom assessments to meet unique compliance needs. It offers workflow capabilities, step-by-step guidance, and a risk-based compliance score to help organizations understand their compliance posture and improve it. Compliance Manager uses several data elements, such as controls, assessments, templates, and improvement actions, to manage compliance activities.

If you have a Microsoft 365 or Office 365 E1, E3, F1 or F3 license then you have access to compliance manager with the Data Protection Baseline Assessment, there is some overlap between this and a subset of the secure score recommendations, but it also has a lot to offer beyond secure score and should be a part of assessing your current state. E5 customers get the Data protection baseline plus access to 3 premium assessment templates (i.e., HIPAA) as part of their licensing.

TAKE A ZERO TRUST APPROACH TO SECURITY

Zero Trust security is a cybersecurity model that assumes that any device, user or system within an organization's network might have already been compromised and poses a potential security risk. It eliminates the concept of a trusted network and instead, verifies and authenticates access for every request to the network, data or system, regardless of the source and location. Zero Trust security relies on continuous security validation, multi-factor authentication, and encryption to secure access to resources, reduce attack surfaces and ensure the confidentiality and integrity of sensitive data.

The Microsoft Zero Trust Security Architecture takes a modular approach to Zero Trust, the following sections detail configurations and tools you likely already own, aligned to the pillars or domains contained within Microsoft Zero Trust, you can choose to implement some or all depending upon which of the pillars you find you are exposed.

IDENTITIES

TAKE A LEAST PRIVILEGE APPROACH FOR ADMINS

The principle of least privilege asserts that users and applications should only have access to data and operations necessary for their job. Whilst there are tools in the E5 suite that help enable this such as Privileged identity Management, in the E1/E3 and all other licensing levels we must take a more manual approach. Make use of Role Based Access control and consider account separation for administrative privileges to reduce the blast radius should a user's regular account be compromised during an attack.

CREATE SEPARATE ADMINISTRATOR ACCOUNTS

Separate administrator accounts from standard user accounts to restrict access and improve security. Create dedicated administrator accounts for administrative tasks, each with different user rights based on job responsibilities, and standard user accounts for regular tasks without administrator rights. To further increase security, sensitive administrator accounts should not have access to email or internet browsing.

REMOVE DORMANT PRIVILEGED ACCOUNTS

Regular checks should be performed to remove inactive user accounts in Active Directory. Over 10% of user accounts in AD can be inactive and pose a security risk as they can be used by attackers or former employees. The inactive accounts can be found using a PowerShell script. The recommended approach is to disable the accounts for a period and then delete them if no issues are reported. This process should be done regularly, with a focus on accounts where the password hasn't been changed in the last 6 months.

AZURE AD PASSWORD PROTECTION

Azure AD Password Protection is an on-premises solution for detecting and blocking weak passwords and password variants. It uses the same global and custom banned password lists that are stored in Azure AD and performs the same checks for on-premises password changes as Azure AD does for cloud-based changes. This can be used to ensure secure passwords are used for any service accounts or admin accounts not synchronized to Azure AD. The deployment of Azure AD Password Protection can be incremental and only enforced where the Domain Controller Agent is installed, but all DCs in a domain must have the software installed for consistent and secure behavior. The on-premises components of Azure AD Password Protection work together with the Azure AD Password Protection Proxy service forwarding password policy download requests, the DC Agent processing

password-validation requests, and the DC Agent monitoring for updated policies. This capability is included in Microsoft 365 E3/F3 and above.

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is an important security measure that adds an extra layer of protection to user accounts. MFA requires users to provide two or more forms of identification, such as a password and a security token, to access sensitive information. This makes it more difficult for hackers to gain access to an account, even if they have obtained the password, as they would also need access to the other forms of identification. MFA can significantly reduce the risk of cyber-attacks and data breaches, as it helps to prevent unauthorized access to sensitive information.

Azure MFA is included in all licensing levels of Microsoft 365, and we highly recommend implementing it using the Microsoft Authenticator mobile app as the second factor of authentication. Avoid using SMS and Phone Call as the second factor as they can be compromised via SMS Phishing (Smishing) and Sim Swapping attacks that allow a threat actor to port an end user's mobile number to another sim card.

CONDITIONAL ACCESS

Conditional Access is an identity-driven security mechanism that uses signals (user/group membership, IP location, device, application) to make access control decisions and enforce organizational policies. This is the heart of Microsoft's Zero Trust Security Architecture. Common access concerns that can be addressed with Conditional Access include enforcing multi-factor authentication for administrative roles, blocking legacy authentication, blocking non-compliant devices, blocking untrusted geographic locations, and blocking risky sign-ins. It is included with Microsoft 365 E3/F3 and above.

PASSWORDLESS AUTHENTICATION

Passwordless authentication in Microsoft 365 works by using alternatives to traditional passwords to securely authenticate users. We recommend using the following methods:

- Microsoft Authenticator app: enables users to authenticate using their mobile device by matching a number that is displayed on the sign-in page.
- FIDO2 security keys: allows users to authenticate using a physical security key that supports the FIDO2 standard.

Each of these methods verifies the identity of the user without requiring them to enter a password, providing an additional layer of security.

Passwordless authentication is also available for Windows 10/11 using Windows Hello for Business. Windows Hello for Business is a biometric authentication that allows users to sign into their devices and applications using facial recognition, fingerprint scanning, or a PIN, instead of a password. It enhances security by using strong public key infrastructure (PKI) and certificate-based authentication, and it can also simplify the sign-in process for users.

ENDPOINTS

ATTACK SURFACE REDUCTION RULES

Microsoft Attack Surface Reduction (ASR) rules are security controls that can help reduce the attack surface of Windows devices. They allow administrators to enforce security policies on managed devices. The rules include security measures such as disabling potentially dangerous system configurations, blocking malicious Office macro execution, and controlling the use of PowerShell scripts. The goal of ASR rules is to prevent malware from gaining access to a system, executing, or propagating. You can implement these rules through Microsoft Intune/Endpoint Manager included in the Microsoft 365 E3/F3 license or using Group Policy.

MICROSOFT INTUNE/ENDPOINT MANAGER

Microsoft Endpoint Manager (Soon to be renamed Intune) is a unified endpoint management solution that allows organizations to manage and secure all their endpoints including Windows, Mac, iOS and Android devices. It integrates Microsoft Intune and Configuration Manager, providing a single console for managing all devices. It is included with Microsoft 365 E3/F3

Microsoft Endpoint Manager can be used to protect against ransomware attacks through the following methods:

1. Security Baselines: pre-configured security policies that provide recommended security settings for Microsoft devices (such as Windows and Microsoft 365 apps) to help protect against threats. These baselines provide a starting point for organizations to secure their devices and can be customized to meet specific security needs. They are regularly updated by Microsoft to reflect the latest security threats and best practices.
2. Configuration Profiles: Endpoint Manager allows administrators to enforce device management policies, such as setting up firewalls, restricting certain apps.
3. Security updates: Endpoint Manager can help keep devices up to date with the latest security patches, which can help prevent ransomware attacks.
4. Threat protection: Endpoint Manager integrates with Microsoft Defender Antivirus and other threat protection solutions to detect and respond to ransomware attacks in real-time.

MICROSOFT DEFENDER FIREWALL

Microsoft Defender Firewall is a built-in firewall for Windows that helps protect devices from unauthorized network access and cyber threats by controlling incoming and outgoing network traffic based on predefined rules. It provides advanced features like creating custom rules, logging and alerting, and integration with Microsoft Defender for Endpoint for enhanced security. Microsoft Defender Firewall is included in Windows and can be managed through Group Policy or Microsoft Endpoint Manager. Best practice settings are included in the security baselines mentioned above.

MICROSOFT DEFENDER SMARTSCREEN

Microsoft Defender SmartScreen is a security feature in Windows and Microsoft Edge that helps protect users from downloading and running malicious software and websites. It checks websites and files that are downloaded from the internet against a constantly updated list of known threats and warns the user if it detects anything suspicious. Microsoft Defender SmartScreen also integrates with Microsoft Defender for Endpoint for additional protection against malware and other security threats. The feature is enabled by default and can be managed through Group Policy or Microsoft Endpoint Manager.

MICROSOFT DEFENDER ANTIVIRUS

Microsoft Defender Antivirus is the built-in antivirus solution for Windows 10/11 that provides real-time protection against malware and other security threats. It uses signature-based detection, behavior analysis, and cloud-based protection to detect and remove malware, and automatically updates itself to stay up to date with the latest threats. Microsoft Defender Antivirus integrates with Microsoft Defender for Endpoint for enhanced security and can be managed through Group Policy or Microsoft Endpoint Manager. The feature is enabled by default on Windows 10 and Windows Server and provides comprehensive protection against a range of threats, including viruses, spyware, and ransomware.

CONTROLLED FOLDER ACCESS

Controlled Folder Access is a security feature in Windows 10/11 that helps protect files and folders from unauthorized changes by malware and other malicious software such as ransomware. You can specify important folders to be protected and it will automatically block unauthorized or malicious applications from making changes to those folders, It can be managed through the Group Policy or Microsoft Endpoint Manager.

APPS

EXCHANGE EMAIL SETTINGS

Whilst deploying an advanced email protection solution is the recommended approach to protecting your email from malicious messages that could contribute to a ransomware attack, there are a few basic configurations you can implement to help protect your organization.

1. Microsoft Defender Antivirus can scan email files and embedded objects (such as attachments and archived files) during on-demand and scheduled scans. It supports the scanning and remediation of DBX, MBX, MIME, and PST file formats used by Outlook 2003 or older (where the archive type is set to non-unicode). If a threat is detected, Microsoft Defender Antivirus displays information about the compromised email, including the subject and attachment name, to assist in identifying and manually remediating the threat. However, it cannot remediate threats detected inside PST files. You can configure this protection via Group Policy or Microsoft Endpoint Manager.

2. Exchange Online Protection (EOP) is a cloud-based anti-spam and anti-spoofing solution included with Exchange Online. EOP helps protect against spam, phishing, and other email-based threats by using advanced filtering techniques and machine learning algorithms to analyze incoming and outgoing email traffic

    a. Anti-spam: EOP uses various techniques to identify and filter out spam, including filtering based on sender reputation, message content analysis, and attachment filtering. It also integrates with Microsoft Defender Antivirus to scan email attachments for malware.
    b. Anti-spoofing: EOP provides anti-spoofing protection to help prevent phishing and other types of email fraud. It does this by checking the authenticity of the sender's email address and domain, and by verifying the message header information to ensure that it has not been altered or forged.

    Check your filtering settings to ensure you are blocking spoofed, spam and malicious emails.

MICROSOFT OFFICE/365 APPS SECURITY BASELINES

The Microsoft Security Baselines for Microsoft Office apps provide a set of recommended security settings for various Microsoft Office applications, such as Microsoft Word, Excel, PowerPoint, and others. These baselines aim to enhance the security posture of Microsoft Office by providing a default set of recommended security controls that are aligned with industry best practices. The security baselines cover various security domains, such as macro security, file block settings, and Protected View settings, among others. The baselines are updated periodically to reflect changes in the threat landscape and to provide the latest security recommendations for Microsoft Office applications. Presently, these can only be managed using Group Policy.

MICROSOFT EDGE SECURITY BASELINE

Like with the Microsoft Office apps, there are also security baselines for Microsoft Edge. The security baselines cover various security domains, such as SmartScreen filter, InPrivate browsing, and pop-up blocker settings, among others. These security baselines can be managed using Microsoft Endpoint Manager or Group Policy.

DATA

STORE SENSITIVE DOCUMENTS IN ONEDRIVE FOR BUSINESS / SHAREPOINT ONLINE

Outside of the security benefits of Microsoft 365 and Azure AD, it is highly recommended to store sensitive documents with OneDrive for Business or SharePoint online over legacy network file shares. OneDrive for Business has native capabilities that help safeguard your organization against ransomware attacks

Version history: OneDrive for Business keeps multiple versions of files, allowing users to easily revert to a previous version in case of ransomware attack or other data loss.

File restore: OneDrive for Business allows users to restore entire folders to a previous version in case of data loss due to a ransomware attack.

IMPLEMENT MICROSOFT PURVIEW DATA LOSS PREVENTION POLICIES

With Ransomware gangs leveraging double extortion attacks to increase the likelihood that a victim will pay the ransom, it is more important than ever to ensure you have data loss prevention configured. Microsoft Purview Data Loss Prevention is included with E3/F3 licensing.

At the most basic level you can create DLP policies to alert and/or block sensitive information being shared externally via Exchange Online email or from SharePoint Online/OneDrive for Business.

IMPLEMENT MICROSOFT PURVIEW INFORMATION PROTECTION

Microsoft Purview Information Protection, included within Microsoft 365 E3/F3, enables your users to apply sensitivity labels to documents and files. Configuring sensitivity labels provides added encryption and access controls for individual files. The owner of the file can also specify user accounts and permitted actions for the file. If a file bearing a sensitivity label is stolen from your tenant, it can only be accessed by the user accounts defined in the label.

CONCLUSION

Ransomware is a significant threat to healthcare organizations and has become a top concern for IT security decision makers. Ransomware attacks have doubled between 2016 and 2021 and the payment amount demanded by the attackers is trending upwards. Healthcare organizations are vulnerable to ransomware attacks due to the complexity of their cybersecurity programs and the need to balance the confidentiality, integrity, and availability of their systems and sensitive data while providing the best possible patient care.

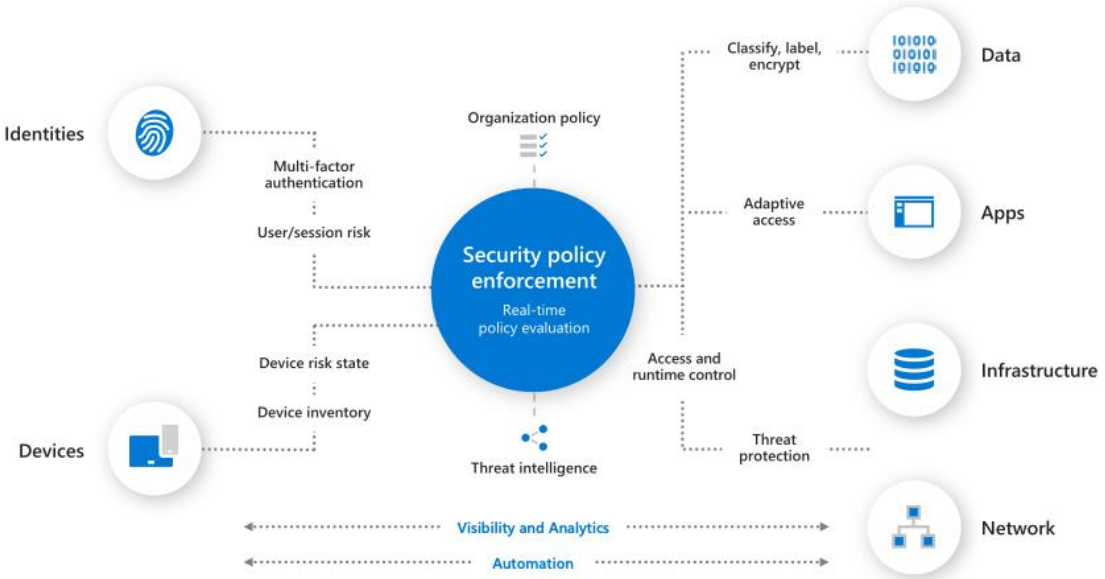
To safeguard against ransomware, healthcare organizations can build a strong foundation using the Microsoft tools they already own. These tools include Microsoft Security and Compliance Toolkit, Microsoft Secure Score, Microsoft Purview Compliance Manager, Azure AD Password Protection, Multi-Factor Authentication, Microsoft Intune/Endpoint Manager, Microsoft Defender Firewall, and Microsoft Purview Information Protection.

To store sensitive data securely, organizations can store it in OneDrive for Business. By implementing these measures, healthcare organizations can proactively secure their systems and sensitive data from ransomware attacks.

REFERENCES

- CISA Definition of ransomware: https://www.cisa.gov/stopransomware/ransomware-faqs#
- Jama Health Report; Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021: JAMA Health Forum – Health Policy, Health Care Reform, Health Affairs | JAMA Health Forum | JAMA Network
- Cyberedge Group 2022 Cyberthreat Defense Report
- Deploy Ransomware Protection for your Microsoft 365 tenant: Deploy ransomware protection for your Microsoft 365 tenant | Microsoft Learn
- Microsoft Security Compliance toolkit: Microsoft Security Compliance Toolkit 1.0 Guide | Microsoft Learn
- Microsoft Secure Score: Assess your security posture through Microsoft Secure Score | Microsoft Learn
- Microsoft Purview Compliance Manager: Microsoft Purview Compliance Manager - Microsoft Purview (compliance) | Microsoft Learn
- Microsoft Zero Trust Architecture: Zero Trust implementation guidance | Microsoft Learn
- Create Separate Administrator accounts from user accounts: Active Directory Accounts | Microsoft Learn
- Remove dormant privileged accounts: Why you should regularly check for and remove inactive user accounts in Active Directory | Microsoft Learn
- Azure AD Password Protection Azure AD Password Protection - Azure Active Directory - Microsoft Entra | Microsoft Learn
- Azure AD Conditional Access What is Conditional Access in Azure Active Directory? - Microsoft Entra | Microsoft Learn
- Passwordless Authentication: Plan a passwordless authentication deployment in Azure Active Directory - Microsoft Entra | Microsoft Learn
- Attack Surface Reduction Rules: Attack surface reduction rules reference | Microsoft Learn
- Controlled Folder Access: Enable controlled folder access | Microsoft Learn
- Microsoft Defender Antivirus email scanning: Configure scanning options for Microsoft Defender Antivirus | Microsoft Learn
- Exchange Online Protection: Exchange Online Protection (EOP) overview - Office 365 | Microsoft Learn
- Security Baselines for Microsoft 365 apps and Edge: Microsoft Security Baselines Blog - Microsoft Community Hub
- Malware and ransomware protection in Microsoft 365: Malware and ransomware protection in Microsoft 365 - Microsoft Service Assurance | Microsoft Learn

Interested in learning more about any of the topics in this Whitepaper or Microsoft Zero Trust?



- Book a call with us at your convenience
- Send us an email
- Follow us on LinkedIn

© 2023 Levacloud LLC. All rights reserved