Quickly protect your organization against ransomware attacks

Article • 10/13/2024

Ransomware is a cyber attack type that cybercriminals use to extort organizations large and small.

Understanding how to protect against ransomware attacks and minimized damage is an important part of safeguarding your company. This article gives you practical guidance for how to quickly configure ransomware protection.

The guidance is organized into steps, starting with the most urgent actions to take.

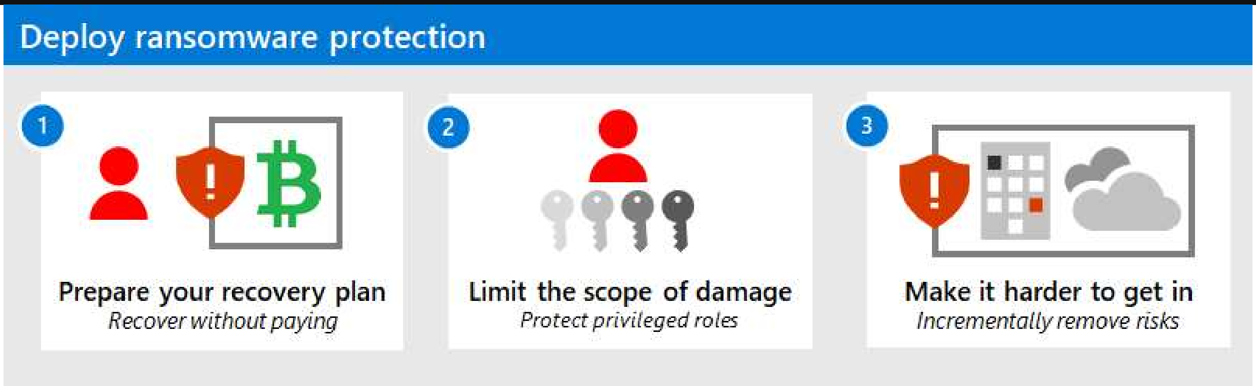
Bookmark this page as your starting point for the steps.

> Important
>
> **Read the ransomware prevention series, and make your organization hard to cyber attack.**
>
> - Have a recovery plan
> - A plan to limit the harm done
> - Make it hard to get in

> Note
>
> What is ransomware? See the ransomware definition here.

Important information about this article

> Note
>
> The order of these steps is designed to ensure you reduce risk *as fast as possible*, and built on an assumption of great urgency that overrides normal security and IT priorities, in order to avoid or mitigate devastating attacks.


Deploy ransomware protection
1
Prepare your recovery plan
Recover without paying
2
Limit the scope of damage
Protect privileged roles
3
Make it harder to get in
Incrementally remove risks

It is important to note this ransomware prevention guidance is structured as steps you should follow in the order shown. To best adapt this guidance to your situation:

1. **Stick with the recommended priorities**

   Use the steps as a starting plan for what to do first, next, and later, so you get the most impactful elements first. These recommendations are prioritized using the Zero Trust principle of *assuming a breach*. This forces you to focus on minimizing business risk by assuming the attackers can successfully gain access to your environment through one or more methods.

2. **Be proactive and flexible (but *don't skip important tasks*)**

   Scan through the implementation checklists for all sections of all three steps to see if there are any areas and tasks that you can quickly *complete earlier*. In other words, things you can do faster because you already have access to a cloud service that hasn't been used but could be quickly and easily configured. As you look over the whole plan, be careful that *these later areas and tasks don't delay completion* of critically important areas like backups and privileged access!

3. **Do some items in parallel**

   Trying to do everything at once can be overwhelming, but some items can naturally be done in parallel. Staff on different teams can be working on tasks at the same time (for example, backup team, endpoint team, identity team), while also driving for completion of the steps in priority order.

The items in the implementation checklists are in the recommended order of prioritization, not a technical dependency order.

Use the checklists to confirm and modify your existing configuration as needed and in a way that works in your organization. For example, in the most important backup element, you back up some systems, but they might not be offline or immutable, you might not test the full enterprise restore procedures, or you might not have backups of critical business systems or critical IT systems like Active Directory Domain Services (AD DS) domain controllers.

> **Note**
>
> See the 3 steps to prevent and recover from ransomware (September 2021) Microsoft security blog post for an additional summary of this process.

Set up your system to prevent ransomware right now

The steps are:

Step 1. Prepare your ransomware recovery plan

This step is designed to minimize the monetary incentive from ransomware attackers by making it:

- Much harder to access and disrupt systems or encrypt or damage key organization data.
- Easier for your organization to recover from an attack without paying the ransom.

> **Note**
>
> While restoring many or all enterprise systems is a difficult endeavor, the alternative of paying an attacker for a recovery key they might not deliver, and using tools written by the attackers to try to recover systems and data.

Step 2. Limit the scope of ransomware damage

Make the attackers work a lot harder to gain access to multiple business critical systems through privileged access roles. Limiting the attacker's ability to get privileged access makes it much harder to profit off of an attack on your organization, making it more likely they'll give up and go elsewhere.

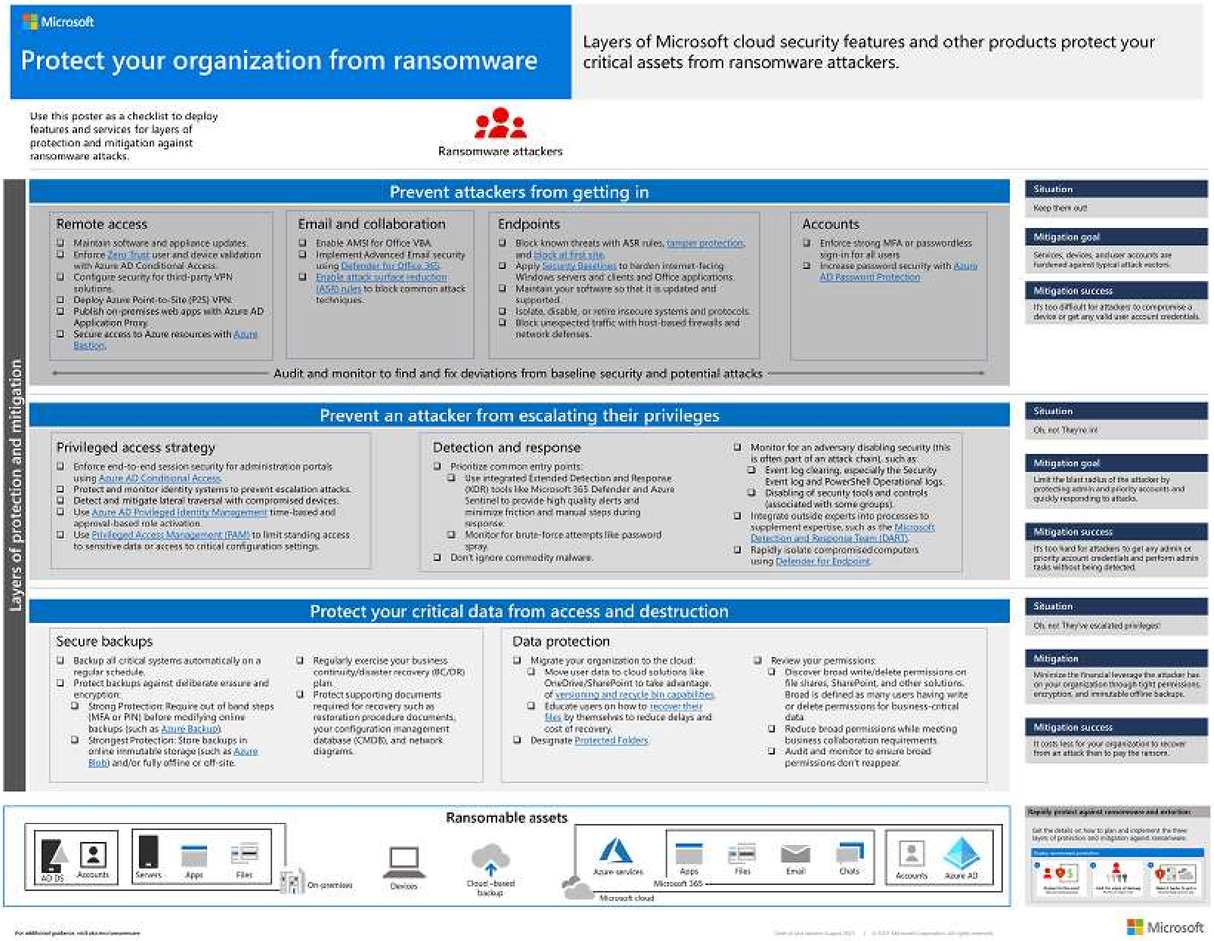
Step 3. Make it hard for cybercriminals to get in

This last set of tasks is important to raise friction for entry but will take time to complete as part of a larger security journey. The goal of this step is to make the attackers' work *much* harder as they try to obtain access to your on-premises or cloud infrastructures at the various common points of entry. There are many tasks, so it's important to prioritize your work here based on how fast you can accomplish these with your current resources.

While many of these will be familiar and easy to quickly accomplish, it's critically important that ***your work on step 3 should not slow down your progress on steps 1 and 2***.

Ransomware protection at a glance

You can also see an overview of the steps and their implementation checklists as levels of protection against ransomware attackers with the Protect your organization from ransomware poster.



Microsoft

Protect your organization from ransomware

Layers of Microsoft cloud security features and other products protect your critical assets from ransomware attackers.

Use this poster as a checklist to deploy features and services for layers of protection and mitigation against ransomware attacks.

Ransomware attackers

Layers of protection and mitigation

Prevent attackers from getting in

Remote access

- ❑ Maintain software and appliance updates.
- ❑ Enforce Zero Trust user and device validation with Azure AD Conditional Access.
- ❑ Configure security for third-party VPN solutions.
- ❑ Deploy Azure Point-to-Site (P2S) VPN.
- ❑ Publish on-premises web apps with Azure AD Application Proxy.
- ❑ Secure access to Azure resources with Azure Bastion.

Email and collaboration

- ❑ Enable AMSI for Office VBA.
- ❑ Implement Advanced Email security using Defender for Office 365.
- ❑ Enable attack surface reduction (ASR) rules to block common attack techniques.

Endpoints

- ❑ Block known threats with ASR rules, tamper protection, and block at first site.
- ❑ Apply Security Baselines to harden internet-facing Windows servers and clients and Office applications.
- ❑ Maintain your software so that it is updated and supported.
- ❑ Isolate, disable, or retire insecure systems and protocols.
- ❑ Block unexpected traffic with host-based firewalls and network defenses.

Accounts

- ❑ Enforce strong MFA or passwordless sign-in for all users
- ❑ Increase password security with Azure AD Password Protection.

Audit and monitor to find and fix deviations from baseline security and potential attacks

Situation

Keep them out!

Mitigation goal

Services, devices, and user accounts are hardened against typical attack vectors.

Mitigation success

It's too difficult for attackers to compromise a device or get any valid user account credentials.

Prevent an attacker from escalating their privileges

Privileged access strategy

- ❑ Enforce end-to-end session security for administration portals using Azure AD Conditional Access.
- ❑ Protect and monitor identity systems to prevent escalation attacks.
- ❑ Detect and mitigate lateral traversal with compromised devices.
- ❑ Use Azure AD Privileged Identity Management time-based and approval-based role activation.
- ❑ Use Privileged Access Management (PAM) to limit standing access to sensitive data or access to critical configuration settings.

Detection and response

- ❑ Prioritize common entry points:
  - ❑ Use integrated Extended Detection and Response (XDR) tools like Microsoft 365 Defender and Azure Sentinel to provide high quality alerts and minimize friction and manual steps during response.
  - ❑ Monitor for brute-force attempts like password spray.
- ❑ Don't ignore commodity malware.
- ❑ Monitor for an adversary disabling security (this is often part of an attack chain), such as:
  - ❑ Event log clearing, especially the Security Event log and PowerShell Operational logs.
  - ❑ Disabling of security tools and controls (associated with some groups).
- ❑ Integrate outside experts into processes to supplement expertise, such as the Microsoft Detection and Response Team (DART).
- ❑ Rapidly isolate compromised computers using Defender for Endpoint.

Situation

Oh, no! They're in!

Mitigation goal

Limit the blast radius of the attacker by protecting admin and priority accounts and quickly responding to attacks.

Mitigation success

It's too hard for attackers to get any admin or priority account credentials and perform admin tasks without being detected.

Protect your critical data from access and destruction

Secure backups

- ❑ Backup all critical systems automatically on a regular schedule.
- ❑ Protect backups against deliberate erasure and encryption:
  - ❑ Strong Protection: Require out of band steps (MFA or PIN) before modifying online backups (such as Azure Backup).
  - ❑ Strongest Protection: Store backups in online immutable storage (such as Azure Blob) and/or fully offline or off-site.
- ❑ Regularly exercise your business continuity/disaster recovery (BC/DR) plan.
- ❑ Protect supporting documents required for recovery such as restoration procedure documents, your configuration management database (CMDB), and network diagrams.

Data protection

- ❑ Migrate your organization to the cloud:
  - ❑ Move user data to cloud solutions like OneDrive/SharePoint to take advantage of versioning and recycle bin capabilities.
  - ❑ Educate users on how to recover their files by themselves to reduce delays and cost of recovery.
- ❑ Designate Protected Folders.
- ❑ Review your permissions:
  - ❑ Discover broad write/delete permissions on file shares, SharePoint, and other solutions. Broad is defined as many users having write or delete permissions for business-critical data.
  - ❑ Reduce broad permissions while meeting business collaboration requirements.
  - ❑ Audit and monitor to ensure broad permissions don't reappear.

Situation

Oh, no! They've escalated privileges!

Mitigation

Minimize the financial leverage the attacker has on your organization through tight permissions, encryption, and immutable offline backups.

Mitigation success

It costs less for your organization to recover from an attack than to pay the ransom.

Ransomable assets

Rapidly protect against ransomware and extortion

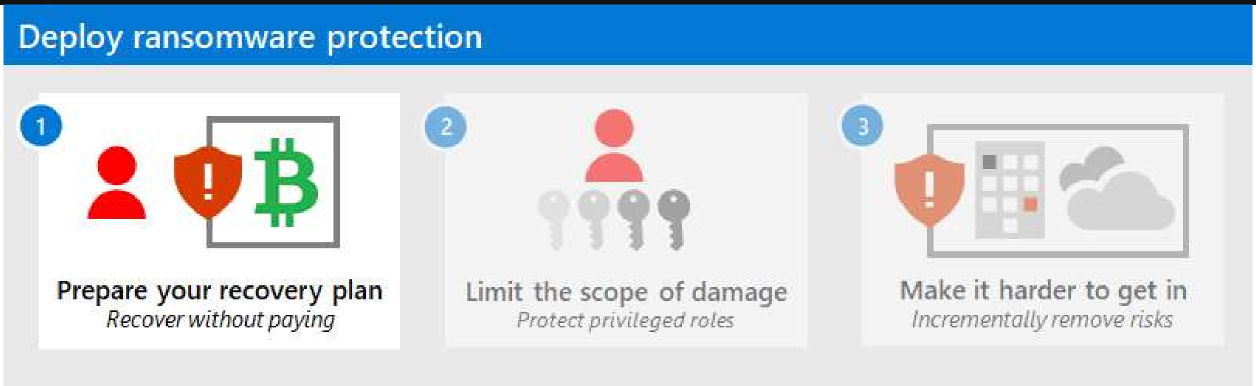
Get the details on how to plan and implement the three layers of protection and mitigation against ransomware.

For additional guidance, visit aka.ms/ransomware

Microsoft

Prioritize ransomware mitigation at the macro level. Configure your organization's environment to protect against ransomware.

Next step


Deploy ransomware protection
1
Prepare your recovery plan
Recover without paying
2
Limit the scope of damage
Protect privileged roles
3
Make it harder to get in
Incrementally remove risks

Start with step 1 to prepare your organization to recover from an attack without having to pay the ransom.

Additional ransomware resources

Key information from Microsoft:

- The growing threat of ransomware, Microsoft On the Issues blog post on July 20, 2021
- Human-operated ransomware
- 2021 Microsoft Digital Defense Report (see pages 10-19)
- Ransomware: A pervasive and ongoing threat threat analytics report in the Microsoft Defender portal
- Microsoft Incident Response team (formerly DART/CRSP) ransomware approach and case study

Microsoft 365:

- Deploy ransomware protection for your Microsoft 365 tenant
- Maximize Ransomware Resiliency with Azure and Microsoft 365
- Recover from a ransomware attack
- Malware and ransomware protection
- Protect your Windows 10 PC from ransomware
- Handling ransomware in SharePoint Online
- Threat analytics reports for ransomware in the Microsoft Defender portal

Microsoft Defender XDR:

- Built in protection against ransomware
- Find ransomware with advanced hunting

Microsoft Azure:

- Azure Defenses for Ransomware Attack

- Maximize Ransomware Resiliency with Azure and Microsoft 365
- Backup and restore plan to protect against ransomware
- Help protect from ransomware with Microsoft Azure Backup (26 minute video)
- Recovering from systemic identity compromise
- Advanced multistage attack detection in Microsoft Sentinel
- Fusion Detection for Ransomware in Microsoft Sentinel

Microsoft Defender for Cloud Apps:

- Create anomaly detection policies in Defender for Cloud Apps

Microsoft Security team blog posts:

- 3 steps to prevent and recover from ransomware (September 2021)
- A guide to combatting human-operated ransomware: Part 1 (September 2021)

  Key steps on how Microsoft Incident Response conducts ransomware incident investigations.

- A guide to combatting human-operated ransomware: Part 2 (September 2021)

  Recommendations and best practices.

- Becoming resilient by understanding cybersecurity risks: Part 4—navigating current threats (May 2021)

  See the **Ransomware** section.

- Human-operated ransomware attacks: A preventable disaster (March 2020)

  Includes attack chain analyses of actual attacks.

- Ransomware response—to pay or not to pay? (December 2019)
- Norsk Hydro responds to ransomware attack with transparency (December 2019)

Feedback

Was this page helpful? Yes No