Ransomware Prevention: Quick Start Guide

We're thrilled to partner with you as you take command of your attack surface.

Refer to this Quick Start Guide for instructions on deploying the Ransomware Prevention add-on to your Managed Detection and Response or Managed Threat Complete service. For help with deployment, contact your Customer Advisor or Customer Advisor team, if needed.

Table of contents

What is Ransomware Prevention? 2
Prerequisites 3
Deployment options 4
- Verify that Ransomware Prevention is deployed 4
- Installation services and folders 5

Configure Ransomware Prevention 6
- Organize assets in prevention groups 6
- Monitor initial deployment with activation mode 6

Prevention engines, detection rules, and alerts 7
- View Endpoint Prevention detection rules in InsightIDR 7
- View Endpoint Prevention alerts in InsightIDR 8
  - Alert structure 9
- How prevention engines block ransomware techniques 10
  - Memory injection 10
  - Living off the land 11
  - Malicious document protection 12
  - OS credential dumping 13
  - File and process manipulation 14
  - Data encryption 15

Manage exclusions 16
- Appy exclusions 16
- Exclusion types 16

Protect your assets using tamper and password protection 18
Switch to active prevention mode 19

RAPID7

What is Ransomware Prevention?

Ransomware Prevention is an additional layer of protection on the endpoint, which coexists alongside Next-Generation Antivirus (NGAV), Endpoint Detection and Response (EDR), and Endpoint Protection Platform (EPP) solutions. It's focused on disrupting the evasive behaviors that ransomware and other forms of malware leverage, preventing both known and unknown (or zero-day) attacks before they start.

Ransomware Prevention mitigates the risk associated with ransomware using proprietary Data Encryption detection and response technology. Instead of looking for patterns and analyzing processes and behavior on runtime or post-execution, Ransomware Prevention focuses on the inner techniques that malicious and evasive attacks employ and embed in processes, manipulating their logic so that they refrain from execution.

Prerequisites

The Insight Agent serves as the vehicle through which Ransomware Prevention is delivered. Your assets, network, and software stack must meet several requirements for each of your Insight Agents, and ultimately, Ransomware Prevention, to function properly.

Complete these tasks first:

- **Verify your operating systems**. While the Insight Agent broadly supports installations on a range of Windows, Linux, and Mac operating systems, only specific Windows operating systems are eligible for use with Ransomware Prevention. Ransomware Prevention is currently compatible with Windows 11, Windows 10, Windows Server 2022, Windows Server 2019, and Windows Server 2016.
- **Install the Insight Agent**. Since Ransomware Prevention is deployed as a component of the Insight Agent, the Insight Agent must be installed on your endpoints.
- **Confirm network traffic and connectivity requirements**. Installed Insight Agents must be allowed to communicate with the Insight Platform in order to power your Insight products and services, including Ransomware Prevention. Refer to the Network traffic and connectivity requirements for Endpoint Prevention for information about Insight Platform-related endpoints where connectivity requirements apply and to understand common network security scenarios that might affect Insight Agent data in transit.

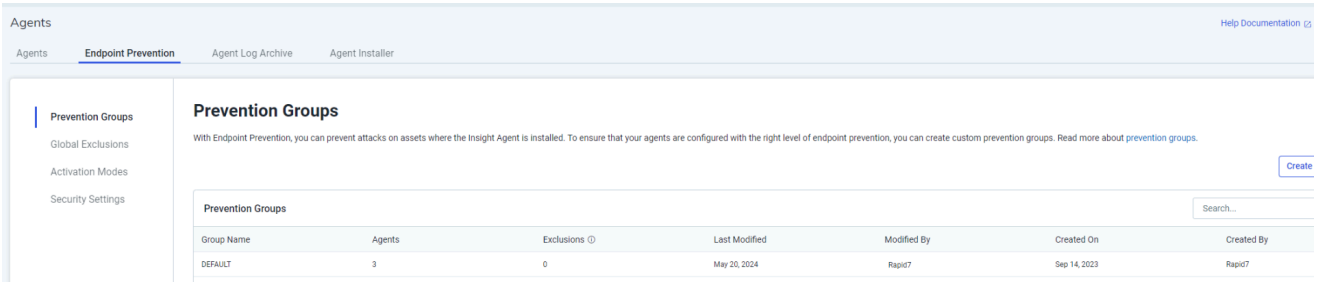
Deployment options

There are two deployment options available for Ransomware Prevention:

- **Deploy using auto-updates**. If you have auto-updates enabled for your organization, Rapid7 can deploy Ransomware Prevention for you, eliminating the need for user intervention. To request that Rapid7 deploy Ransomware Prevention, create a support ticket for your Customer Advisor.
- **Deploy using an installation package**. If auto-updates are not enabled, you can deploy Ransomware Prevention using a dedicated installation package. To get access to the package, create a support ticket for your Customer Advisor to send you the package and installation instructions.

Verify that Ransomware Prevention is deployed

After Ransomware Prevention is successfully deployed, the Endpoint Prevention tab displays in the Insight Platform, under Data Collection > Agents. Go to **Data Collection > Agents** to verify that Ransomware Prevention is deployed.



Installation services and folders

On your endpoints, Ransomware Prevention is installed as a service, named Rapid7 Endpoint Prevention. Ransomware Prevention runs as two services on a 64-bit OS and as a single service on a 32-bit OS.

The Ransomware Prevention installation folder is located in **C:\Program files\rapid7\Insight Agent\components\armor\common\armor**. Refer to the Insight Agent documentation for more information.

Configure Ransomware Prevention

Get started with Ransomware Prevention by understanding key configuration options.

Organize assets in prevention groups

Assets that have Ransomware Prevention deployed are managed using prevention groups, which help you logically organize your assets, defining the protection settings and policy enforcement that should be applied for them. Ransomware Prevention settings and policies are managed in Agent Management on the Endpoint Prevention tab.

Assets with Ransomware Prevention deployed for the first time are assigned to the **default prevention group**. This prevention group cannot be deleted, and its initial settings cannot be modified.

After an asset is assigned to the default prevention group, you can move it to other groups, which you create. You can apply different settings to the prevention groups you create, making it efficient to control and manage various assets. An asset cannot be assigned to multiple groups at once.

Keep in mind that assets are managed in groups, rather than individually, so any settings that you specify apply to the whole group. For example, if you need to test new policies on only a few endpoints, you can create a group and apply exclusions that are relevant to those specific endpoints.

Monitor initial deployment with activation mode

Ransomware Prevention has an organization setting, called activation mode, which overrides prevention groups. To efficiently onboard Ransomware Prevention on your endpoints, the default activation mode is set to **Monitor Only**.

When activation mode is set to **Monitor Only**, Ransomware Prevention actively monitors your assets, but doesn't interfere with suspicious activity, even if the prevention group settings are set to **Block**. In this mode, Ransomware Prevention also still generates alerts in InsightIDR, allowing you to learn how the product interacts with existing business workflows and applications, so an appropriate exclusion can be applied, if necessary.

Prevention engines, detection rules, and alerts

Malware and ransomware often operate using evasive techniques. With evasive techniques, malware and ransomware can send inquiries, allowing them to assess the likelihood of being detected, as well as the ability to move laterally, exploit vulnerabilities, unpack arbitrary code in memory, gain credentials, and more. Often, these methods are hidden in legitimate applications, which are otherwise unlikely to be used.

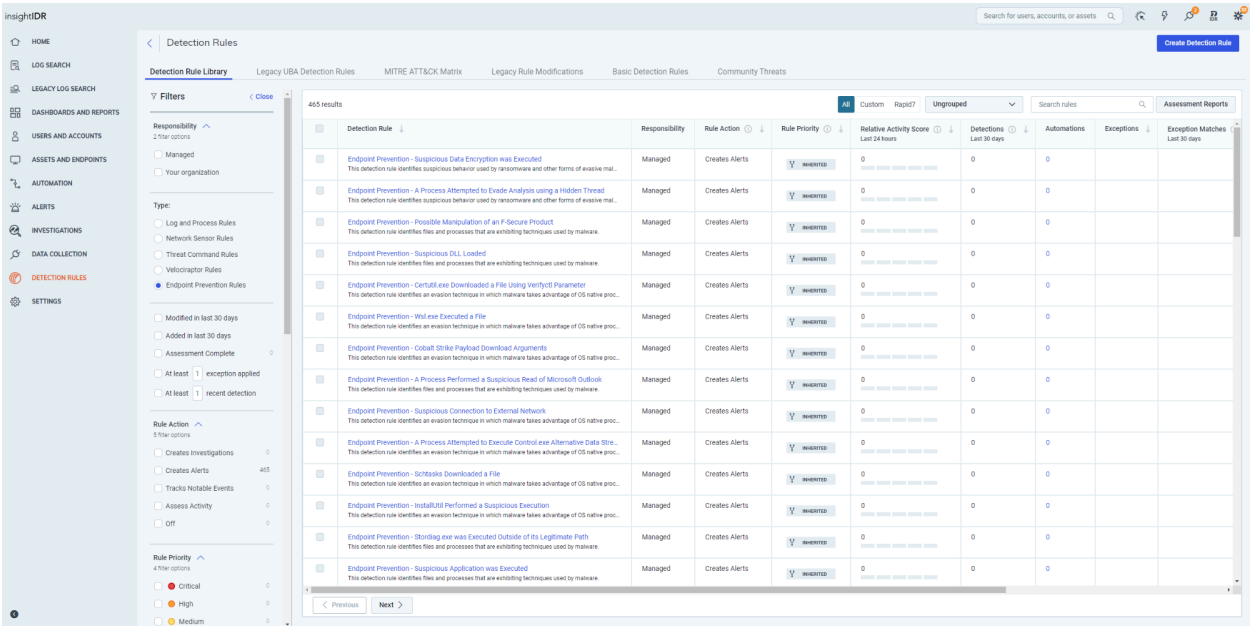
Ransomware Prevention manipulates callback responses for evasive processes, rendering their techniques ineffective and forcing them to refrain from execution or crash, before damage can be done and without impacting end-users' work.

View Endpoint Prevention detection rules in InsightIDR

In InsightIDR, you can view the detection rules that generate Endpoint Prevention alerts, which are also used for Ransomware Prevention.

To view Endpoint Prevention detection rules in Insight IDR:

1. In InsightIDR, select **Detection Rules** in the left menu.
2. Select the **Endpoint Prevention Rules** filter to narrow the list.



View Endpoint Prevention alerts in Managed IDR

By default, all Endpoint Prevention detection rules automatically generate both an alert and an investigation in InsightIDR. These alerts and investigations are also created for Ransomware Prevention.

Currently, only Managed Detection and Response (MDR) customers have access to the Alerts menu item in InsightIDR.

To view Endpoint Prevention alerts in InsightIDR (MDR customers only):

1. In InsightIDR, select **Alerts** in the left menu.
2. In the search field above the table, query for alert titles that include the phrase **endpoint prevention**. All Endpoint Prevention alerts include this phrase in the title.
3. To view details for an alert, click its **Alert Details** icon.

Alert structure

Endpoint Prevention alerts—which also apply to Ransomware Prevention—contain some unique fields, which can be helpful for gaining context about the alert and taking action on it. Alert details might vary based on the alert type, but this structure and raw data is fundamental to each one:

- **Agent action** - The action taken on the reported process or threat, based on the prevention group that the endpoint was assigned to during the time of the event.
- **Process full path** - The full path of the file that triggered the alert.
- **Command line** - The full command line of the process that triggered the alert.
- **Event type** - The category of the rule name, corresponding to the prevention engine.
- **File hash** - The SHA-256 hash of the file that triggered the alert.
- **Host name** - The host name of the endpoint that reported the alert.
- **Certificate information** - The certificate information of the file that triggered the alert, which is applicable for signed processes.
- **PID** - The process ID of the file that triggered the alert.
- **PPID** - The process ID of the parent process for the process that triggered the alert.
- **Parent process full path** - The full path of the parent process for the process that triggered the alert.
- **Armor version** - The underlying component version of Endpoint Prevention, referred to as Armor.
- **Rule name** - The name of the Endpoint Prevention rule responsible for the alert.
- **User name** - The user that executed the process, which triggered the alert.
- **Prevention Group** - The name of the prevention group that the endpoint triggering the alert is assigned to.
- **Local IP** - The local IP of the endpoint reporting the event.
- **Repeat Counter** - The number of similar events received in the last 24 hours.
- **First received time** - The server time when the first similar event was received.

- **Additional info** - Additional information regarding the endpoint action in the alert. Depending on the event type, different details display.
- **Alert type specific details** - Additional forensic information about the alert.
- **Process Hierarchy** - All parent processes' information about the triggered process, including PID, time created, hash, command line, and the user that created the process.

How prevention engines block ransomware techniques

Ransomware Prevention uses various prevention engines to protect your assets from ransomware and other forms of malware that use common types of techniques.

Memory injection

Why it's used

Previously, malware attacks typically involved malicious processes, which either carried out the attack or downloaded a file-based payload with malicious code. These processes were found by threat analysts and security software that listed running processes, distinguishing suspicious processes from legitimate ones.

How it's used

Malware authors are now aware of this countermeasure and have created a way to circumvent it, using techniques known as process injection or memory injection.

Process and memory injection make it harder for security tools to detect malicious processes. These techniques run malicious code in the address space–the range of valid addresses in-memory, which are allocated for a particular program or process–of a legitimate process or a sensitive OS process. Sometimes, malware also unpacks malicious code into its own process as a form of self-injection, creating a skeleton process that is already present in memory.

How Endpoint Prevention blocks it

Endpoint Prevention stops fileless and other memory-resident malware from hiding in legitimate processes and evading detection. For example, Ransomware Prevention

deceives the malware about its ability to unpack code solely in a process' memory space without exposing or loading a dynamic link library (DLL) into the process memory, stopping the attack before it does any damage.

Resulting actions

The code injection is blocked from unpacking itself in the destination or targeted process.

Forensic information available in alerts

In addition to the standard details, the resulting alert provides information about the destination process and the malware targeted for injection. It also provides a list of all loaded modules (DLLs) in the process that triggered the alert.

Living off the land

Why it's used

Living off the land (LOTL or LOL) is an evasion technique that takes advantage of trusted system utilities, libraries, tools, and components, which are native to the operating system. The operations that this software performs appear to be legitimate, even though they are performed on behalf of a threat actor.

How it's used

Malware uses LOLbins to perform operations, which appear to be typical. For example, malware can perform lateral movement, download malicious artifacts, and move to another stage of attack without triggering an alert. These operations can use trusted utilities and components, including those that are digitally signed.

How Endpoint Prevention blocks it

Endpoint Prevention stops unwanted process relationship executions by hiding LOLbins. This makes it impossible for attackers to find them and use them to continue their attack.

Resulting actions

Endpoint Prevention blocks processes from spawning LOLbins' executions.

Forensic information available in alerts

In addition to the standard details, the resulting alert provides information about the blocked command, which executed the child process.

Malicious document protection

Why it's used

Threat actors use documents to lure victims through phishing or social engineering attacks, allowing them to deliver malicious code and gain a foothold on a machine. Traditional antivirus (AV) tools and threat analysts typically detect malware by comparing the hash of the document file to the malware hashes in their database.

However, it's more difficult to detect malicious activity in popular software that's used to open these documents, such as Microsoft Office or Adobe. This software is often misused as an evasive technique, carrying out the document's malicious code on its behalf while remaining undetected, since the software is considered legitimate.

How it's used

Malware uses legitimate document software to run macros, open script interpreters, obfuscate malicious code, use add-ons and extensions, download scripts, execute another executable program, and more.

How Endpoint Prevention blocks it

Endpoint Prevention isolates the document in the container software used to open it by preventing interaction with other script interpreters and executables that appear unusual or risky.

Resulting actions

Endpoint Prevention blocks malware from spawning risky child processes' executions.

Forensic information available in alerts

In addition to the standard details, the resulting alert provides information about the blocked command that executed the child process.

OS credential dumping

Why it's used

It takes multiple steps for ransomware to be successful, including shutting down security controls and accessing restricted information to hold for ransom. Spreading through a network requires lateral movement, where attackers can attempt to dump credentials, allowing them to obtain account logins that enable their malware to move laterally.

How it's used

Adversaries might attempt to access credentials stored in the process memory of the Local Security Authority Subsystem Service (LSASS). They can deploy tools that allow them to extract this data, exploit legitimate applications and processes, and use LOLbins to dump sensitive, credential information.

How Endpoint Prevention blocks it

Endpoint Prevention cloaks sensitive files, processes, and other artifacts, preventing attackers or their malware from harvesting credentials or other sensitive data—even if the threat finds a way to run on the system.

Resulting actions

Endpoint Prevention monitors API calls that attempt to access credentials stored in process memory of the LSASS, preventing access to this area and snapshot dumping using an LOLbin.

Forensic information available in alerts

In addition to the standard details, the resulting alert provides information about the sensitive asset where credential harvesting was attempted. It also provides the block command line involved in the attempt.

File and process manipulation

Why it's used

Traditional antivirus (AV) tools and threat analysts typically detect malware by comparing the hash of a file or process with the malware hashes in their database. Additionally, file systems often require dedicated permissions or access controls.

Making too many changes on a file system can trigger existing endpoint security controls, which block malware activity. However, legitimate programs with direct access can read and write files directly from the drive by analyzing file systems. These programs can access sensitive or vulnerable files in a way that doesn't raise suspicion.

How it's used

To avoid detection, adversaries abuse programs that already have direct access to file systems and can read and write files directly from the drive. These programs can be used to access sensitive files and then read, write, or execute on the malware's behalf. This technique can bypass Windows file access controls and file system monitoring tools.

How Endpoint Prevention blocks it

To prevent the evasive techniques that exploit access to a file system, Endpoint Prevention can control access to the file system, making it inaccessible or unchangeable.

Resulting actions

Endpoint Prevention blocks attempts from the malicious process to access restricted file systems by manipulating the access controls to the file or path.

Forensic information available in alerts

In addition to the standard details, the resulting alert provides information about the blocked path that the process attempted to reach.

Data encryption

Why it's used

Encryption occurs often in a Windows OS and is not necessarily malicious. Many built-in and third-party tools use native OS functions and methods of encryption to meet their functional requirements. These encryption methods, which are usually unmonitored, are often time and resource intensive.

Encryption makes it harder for endpoint security tools and threat analysts to identify ransomware as malicious. However, once the ransomware is detected, a signature is immediately created, preventing further infections.

How it's used

Malware authors are aware of this technical challenge and have created a way to avoid it, using hidden or nested threads that allow them to execute their malicious code quickly while remaining unnoticed.

How Endpoint Prevention blocks it

Endpoint Prevention blocks ransomware's attempts to hide in process threads. Instead of monitoring the encryption method itself, Endpoint Prevention monitors suspicious thread activities, rendering this technique ineffective.

Resulting actions

Endpoint Prevention terminates the process initiating hidden or nested threads.

Forensic information available in alerts

In addition to the standard details, the resulting alert provides information about the process that initiated the attack.

Manage exclusions

You can set Ransomware Prevention to ignore asset behavior that typically triggers a response from the prevention policy. If you receive an alert for prevented activity that is actually legitimate, you can create an exclusion to avoid future alerts on similar activity.

After deploying Ransomware Prevention with activation mode set to **Monitor Only**, you might notice alerts in InsightIDR that show how Ransomware Prevention interacts with your daily processes, applications, and tasks. For activities that you determine are benign, we recommend adding exclusions before switching activation mode to **Active Prevention**.

Appy exclusions

Ransomware Prevention focuses on processes and their behavior. Because of this, you can configure exclusions so that Ransomware Prevention stops monitoring a process completely or stops interfering with the actions taken by a process.

Exclusions are applied to prevention groups, rather than individual assets. If an asset is moved to another prevention group, it receives the exclusions applied to that group and loses exclusions that were applied to the previous group.

Exclusion types

You can choose to exclude a process completely or exclude only specific activities that the process performs.

There are differences between these approaches, which impact how the excluded process interacts with other processes:

- When you exclude a process completely, any child processes that it spawns are also excluded.
- When you exclude activities within a process, the process is still monitored and child processes that it spawns are monitored as well.

Depending on the alert type, process type and other parameters, the Insight Platform provides the applicable exclusion type for you to set. For more details, refer to the exclusion documentation.

Protect your assets using tamper and password protection

Attackers often attempt to tamper with endpoint security solutions, so that they can freely perform malicious activities without being detected.

The Tamper Protection engine contains rules that protect the Ransomware Prevention component of the Insight Agent, therefore protecting your assets continuously. When Tamper Protection is turned on, it prevents malware and bad actors from tampering with the files and functionality of Ransomware Prevention. It also offers the option of turning on password protection.

Using a one-time passcode (OTP) or a fixed password allows you to limit the users who can update, stop, or uninstall the Ransomware Prevention service. You can activate password protection at both the organizational level and for individual prevention groups that require extra security. For more details, refer to the Tamper Protection in documentation.

Switch to active prevention mode

After completing initial deployment, setting policies and exclusions, managing your assets in prevention groups, and enabling password protection, you can switch Ransomware Prevention to active prevention mode.

Depending on the complexity of your organization—for example, the number of systems, applications, and teams—you'll be able to identify alerts, set exclusions for benign alerts, and notice the alert volume decrease and remain stable.