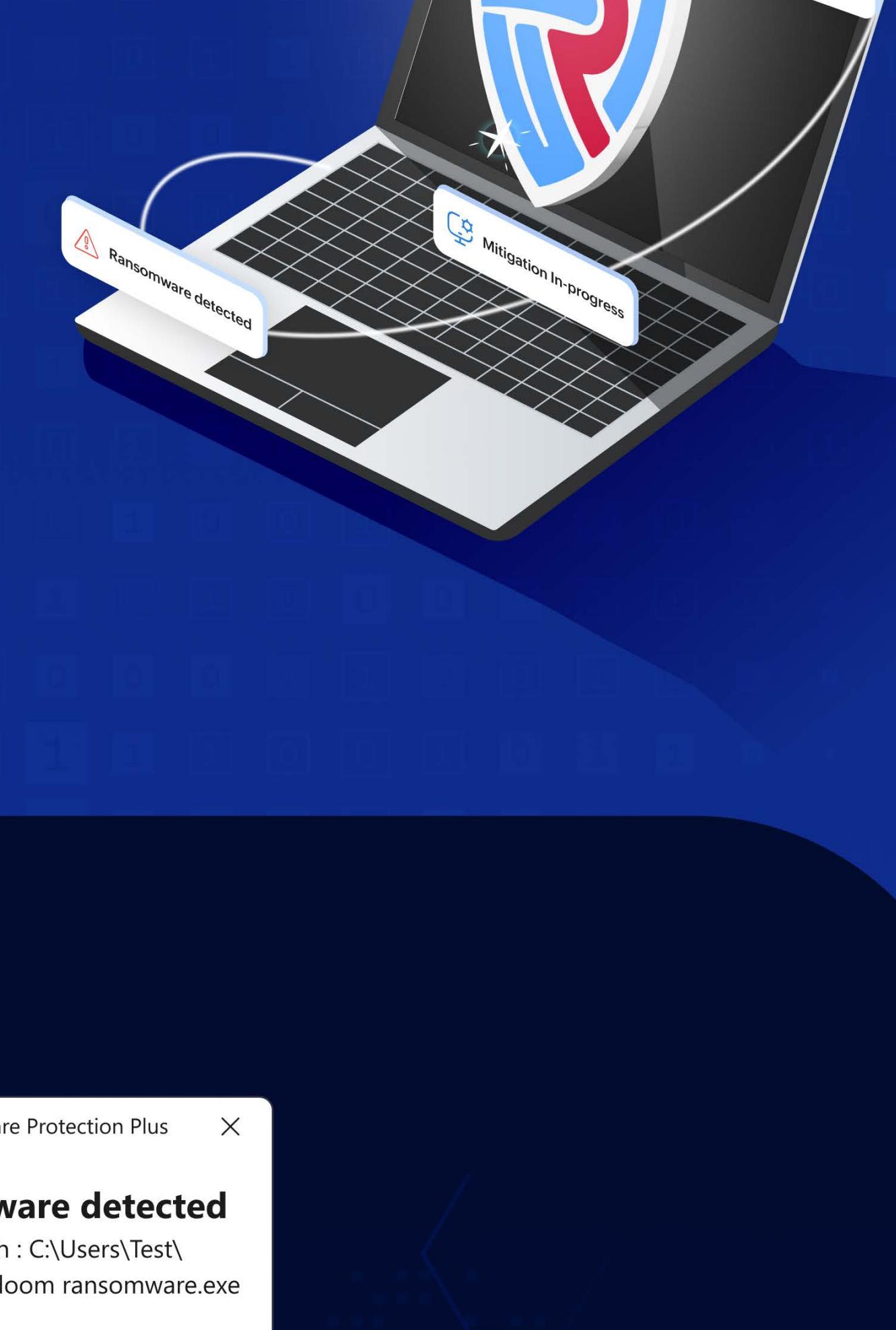


Back to Business Within Minutes

Map out the entire attack chain from robust detection to swift mitigation and recovery, while complementing your incident response, compliance, and overall threat management strategy. Ensure a resilient security posture against evolving ransomware threats with zero downtime.



Detect Ransomware

Identify ransomware-based malicious activity within seconds of reaching a predefined threshold via real-time alerts.

The screenshot displays the following components:

- Ransomware detected:** A modal window showing an exclamation mark icon, the path C:\Users\Test\Desktop\Mydoom ransomware.exe, and a 'Mark as' button.
- Email notification:** An incoming email from 'Administrator_sudhar' with the subject 'Possible Suspicious event detected'. It includes a preview of the attack details and a link to the full alert.
- Attack Details:** A detailed list of attack parameters including detection and reported times, attack status, agent action, and source.
- Endpoint Details:** Information about the infected endpoint, including name, domain, version, and contact details.
- Message:** A note from the administrator.
- Footer:** A disclaimer about auto-generated emails and a link to support.

The screenshot shows a detailed view of a ransomware incident, including:

- Signer:** Signed, Yes.
- SHA256:** 74251D8C7A300C4BDBE4807A1DDH655ACE6303C95DG.
- Virus Total:** EP441965228185A9.
- First Infected Info:** Infected Device Name: Desktop_VP674, Infected Time: Sep 3, 2021 09:54 PM.
- Organization Info:** Company: Microsoft Corporation, Product: Microsoft Windows Operating System, Description: Microsoft Corporation.
- Process Info:** File type: EXE, Original File name: services.exe.mui, Copyrights: Microsoft Corporation. All rights reserved.

Attack Summary

Key details to understand the nature of the ransomware incident, from its source to its scope.

Incident Timeline

Unravel the process chain depicting the sequence of events along with the execution details and malicious intent.

The screenshot shows the 'Alert Story' timeline for the 'Wininit.exe' process, which includes:

- Attack Story: Wininit.exe, Jun 02, 2023 12:24 AM.
- Attack Story: Service.exe, Jun 02, 2023 12:24 AM.
- Attack Story: Svchost.exe, Jun 02, 2023 12:24 AM.
- Attack Story: whomini.exe, Jun 02, 2023 12:24 AM.
- Lockbit.exe:** Alert: Ransomware, Jun 02, 2023 12:24 AM.
- Mitre info:** T1486 - Data Impact.
- Behaviour:** VSS Snapshot Deleted, Jun 02, 2023 12:24 AM.
- Mitre info:** T1243 - Backup Delete, Jun 02, 2023 12:24 AM.

Recovered Data Encrypted by Ransomware

Restore your files swiftly and securely post-attack to ensure zero downtime and zero ransomware payment.

The screenshot shows a summary of incidents and devices:

- Incidents:** Last visit Sep 8, 2021, 04.
- Unresolved Incidents:** 02.
- Out of Protected Devices:** 02.
- Incident Details:** A table showing incident ID, detected time, severity, alerts, and infected device(s) for four incidents.

Affected Devices

Get a report on the list of devices affected due to the impending ransomware attack. Isolate affected devices and control damage.

Resolution Status

Know the security posture of your endpoints across your organization at a glance. Manually intervene to resolve the incident or auto-kill based on your preference.

The screenshot shows the 'Resolve Incident' dialog box with options:

- Mark as:** True Positive (radio button selected).
- Action:** Kill Processes, Clean Up, Rollback.
- Note:** Choosing Rollback will revert the incident to its previous state (True to the threat), kill the threat, and revert all files and system configurations to their previous state.
- Buttons:** Proceed, Cancel.

See Ransomware Protection Plus in action

30-DAY FREE TRIAL

BOOK A DEMO