

April 2026 Release Notes

The Command Platform release notes include information about [what's new](#), which are updated monthly, and [improvements and fixes](#), which are updated weekly.



Last updated: April 13, 2026

What's New

Learn about new features across the Command Platform. These features were released over the past month and are available now:

- [Attack surface: Attack Surface Management \(Surface Command\), Exposure Command](#)
- [Risk: Exposure Command, Vulnerability Management \(InsightVM\), Application Security \(InsightAppSec\)](#)
- [Threat: SIEM \(InsightIDR\), Incident Command](#)
- [Administration: Command Platform](#)
- [Attack surface](#)
 - [Automate external attack surface discovery with dynamic seed queries](#)
- [Risk](#)
 - [See asset protection and patching coverage in Remediation Hub](#)
 - [Gain more coverage with the Web & App Framework Vulnerability Detection Module](#)
 - [Export scan policy data with Bulk Export API](#)
 - [New AlmaLinux Vulnerability Coverage](#)
- [Threat](#)
 - [Improve identity investigations with enhanced group membership visibility](#)
 - [Strengthen identity context in Incident Command with user-to-identity mapping](#)
 - [Maintain investigation context with persistent search tabs](#)
 - [Increase in custom detection rule limits](#)
 - [r7_hostid in endpoint-related events](#)

- [Administration](#)
 - [Export user access data for audit and compliance](#)
 - [Access all tenants with a single multi-tenant API key](#)
-

Attack surface

Your attack surface is comprised of all of the potential entry points that attackers could exploit across your systems, applications, and networks. Developing knowledge of your attack surface is a key goal in improving your company's security posture.

- [Automate external attack surface discovery with dynamic seed queries](#)

Automate external attack surface discovery with dynamic seed queries

Automate external attack surface discovery using data from Rapid7 and third-party Attack Surface Management (Surface Command) connector seed queries. These seed queries provide domain and IP network data to drive discovery. You can enable supported connectors as EASM seed sources to continuously inform your external attack surface inventory. Initial support includes 12 connectors, such as:

- Markmonitor for registered domain data
- NetBox for public network ranges
- Rapid7 Application Security (InsightAppSec) for configured target domains

With this capability from **Command Platform > Assets & Identities > Discovery Seeds**, you can:

- Use domain and network data from integrated tools to power external asset discovery.
- Automatically update discovery inputs as assets are provisioned or decommissioned.
- Reduce reliance on manually maintained domain and IP seed lists.

[Top of page](#)

Risk

Risk is the potential for loss or damage to your assets, operations, or reputation, due to vulnerabilities being exploited by a bad actor.

- [See asset protection and patching coverage in Remediation Hub](#)
- [Gain more coverage with the Web & App Framework Vulnerability Detection Module](#)
- [Export scan policy data with Bulk Export API](#)

See asset protection and patching coverage in Remediation Hub

Security teams often lack the context to answer key questions, such as whether an asset is protected or why a vulnerability persists after patching. Remediation Hub now provides expanded asset-level visibility so you can understand how assets are protected and patched across your environment. These details are available in remediation details, filters, and exports.

With this capability from **Command Platform > Response & Remediation > Remediation Hub**, you can:

- View the endpoint protection applied to each asset.
- Identify which patch management tool is responsible for updates.
- Determine whether a reboot is required after patching.

[Top of page](#)

Gain more coverage with the Web & App Framework Vulnerability Detection Module

Application Security (InsightAppSec) now has coverage for known vulnerabilities in Drupal and WordPress Core, allowing you to measure risk on your current software

versions. Understand the technologies in use, such as frameworks, CMSs, and libraries, while seeing if they're vulnerable.

With this new Attack Module in **Scan Configuration > Passive Attack Modules**, you can:

- Gain context-aware scanning, automatically identifying technologies and running targeted checks.
- Consolidate coverage within Application Security (InsightAppSec), reducing the need for supplementary tools.
- Improve scan accuracy and streamline testing.

[Top of page](#)

Export scan policy data with Bulk Export API

You can now export scan policy data alongside the existing Rapid7 Agent (Insight Agent) policy data using the Bulk Export functionality. This improvement has been incorporated into the existing policy request, meaning you can receive this additional data using the same workflows you use today.

With this capability from the **Bulk Export API**, you can:

- Access all your policy data within one export.
- Streamline your policy management processes.
- Gain an enriched data export using the same requests you use already.

New AlmaLinux Vulnerability Coverage

We have released a vulnerability coverage update that will impact AlmaLinux assets. This update improves visibility into vulnerabilities that may already exist in your environment.

With this update in **Vulnerability Management (InsightVM) and Nexpose**, you may:

- See an increase in vulnerabilities detected on AlmaLinux assets.
- See vulnerabilities associated with older CVEs that remain unpatched. However, the “first found” date will appear recent because it reflects when detection became available.
- See an increase in risk score. This is an indication of improved coverage, not an increase of actual risk.

No action is required to receive this vulnerability coverage, as it will be included in your next automatic or scheduled update.

[Top of page](#)

Threat

A threat is any potential event or action that could exploit vulnerabilities in a system, causing harm to assets, data, or operations.

- [Improve identity investigations with enhanced group membership visibility](#)
- [Strengthen identity context in Incident Command with user-to-identity mapping](#)
- [Maintain investigation context with persistent search tabs](#)
- [Increase in custom detection rule limits](#)
- [r7_hostid in endpoint-related events](#)

Improve identity investigations with enhanced group membership visibility

You can now view group membership details for Okta and Microsoft Entra ID users directly in the User Details page.

With this capability from **Users and Accounts**, you can:

- View admin and user group memberships across Active Directory, Okta, and Entra ID in one place.
- Investigate alerts faster with richer identity context.

- Reduce blind spots in privilege and access analysis.
- Strengthen attack surface awareness across hybrid identity environments.

[Top of page](#)

Strengthen identity context in Incident Command with user-to-identity mapping

You can now map SIEM (InsightIDR) users to their corresponding ASM identity profiles in Incident Command.

With this capability from **Users and Accounts**, you can:

- Pivot seamlessly from a SIEM (InsightIDR) user to the corresponding identity profile in ASM.
- View identity posture instantly, including MFA status, account risk, and group memberships.
- Improve triage efficiency by eliminating manual user correlation.
- Gain a unified view of your identity attack surface.

[Top of page](#)

Maintain investigation context with persistent search tabs

Log Search now preserves open tabs, queries, and context across sessions.

With this capability from **Log Search**, you can:

- Resume investigations without rebuilding queries or context.
- Reduce workflow disruption when switching between tasks.
- Maintain continuity across SOC and MSSP workflows.
- Improve operational efficiency and reduce mean time to respond (MTTR).
- Copy the link to share your open tabs with colleagues.

[Top of page](#)

Increase in custom detection rule limits

You can now create more custom detection rules, giving you greater flexibility.

With these updated limits, you can:

- Create and manage more custom detection rules.
- Expand detection coverage across your environment.
- Scale your detection strategy as your organization grows.

Role-Based Access Control

r7_hostid in endpoint-related events

With this update, a new optional field `r7_hostid` is included in the JSON payload for supported event sources.

This update applies to:

- Active Directory Admin Activity - Endpoint Agents
- Endpoint Activity - Local Account Creation
- Endpoint Activity - Local Service Creation
- Endpoint Activity - NetBIOS Poisoning

[Top of page](#)

Administration

Administration focuses on refining platform controls, improving integrations, and streamlining configuration.

- [Export user access data for audit and compliance](#)
- [Access all tenants with a single multi-tenant API key](#)

Export user access data for audit and compliance

Platform administrators can now export a comprehensive view of user access data in CSV format.

With this capability from **Command Platform > Users > Export User List**, you can:

- Export a complete list of platform users and their access details.
- Review user groups, product access, and assigned roles in one place.
- Validate access policies and support compliance reporting.
- Generate downloadable reports for audit requests.

[Top of page](#)

Access all tenants with a single multi-tenant API key

Access tenant data programmatically across all managed tenants using a single multi-tenant API key.

With this capability from **Command Platform > Administration > API Key Management**, you can:

- Use a single multi-tenant API key to access data across all tenants.
- Avoid managing separate credentials.
- Simplify integrations.
- Improve operational efficiency and visibility.

[Top of page](#)

Keep track of improvements and fixes to core technology.

Application Security (InsightAppSec) and AppSpider

No updates released at this time.

[Top of page](#)

Attack Surface Management (Surface Command)

- [Version 1.0.904](#)

Version 1.0.904

Software release date: April 7, 2026 | **Release notes published:** April 13, 2026

Improved:

- Improved asset query performance by enabling indexing for equality operator (=) on indexed correlation properties.
- Updated the dashboard widget override modal to include an **Edit Original** button for direct editing and improved copy and button placement for better usability.
- Added Data Reset support to the Import Feed Connector Profile, allowing removal of imported data using a UI button and deletion of connector profiles after clearing all fields.
- Improved Import Feed Logs performance by reducing data volume per request and displaying entries in reverse chronological order.

Fixed:

- Numeric widget color picker defaults to the initial color selection when creating or editing widgets.
- Trend Bars without dimensions render correctly in the UI.
- Widget sidebar layout maintains consistent vertical spacing when numeric widgets occupy two lines.
- Workspace query for `Case` assets executes without error.

Connectors

The following connectors were updated in the [Extension Library](#) [↗] since the previous release. Connector updates are published independently and may have been available before this release date.

Updated Connectors

- [AWS_EC2](#): Update dependencies
- [AWS_IAM](#): Update dependencies
- [AWS_Route53](#): Update dependencies
- [AWS_S3](#): Update dependencies
- [Amazon Inspector](#): Update dependencies
- [Anthropic](#): Remove Beta label
- [Aqua_CSPM](#): Remove Beta label
- [Aqua_Enterprise](#):
 - Classify AquaEnterpriseContainerRisk records with a derived exposure type
 - Remove Beta label
- [Asimily_Risk_Management](#): Remove Beta label
- [Atlassian_Bitbucket_Data_Center](#): Remove Beta label
- [Atlassian_Compass](#): Remove Beta label
- [BeyondTrust_BeyondInsight_and_Password_Safe](#): Remove Beta label
- [BeyondTrust_Endpoint_Privilege_Management_\(EPM\)](#): Remove Beta label
- [Broadcom_CCS](#): Remove Beta label
- [Cisco_Intersight](#): Remove Beta label
- [Cribl](#): Add Correlation with Attack Surface Management (Surface Command) types using CloudInstanceId
- [CyberArk_Privileged_Access_Manager](#): Remove Beta label
- [Delinea_Secret_Server](#): Remove Beta label
- [DocuSnap365](#): Remove Beta label
- [Druva](#): Remove Beta label
- [EZO_AssetSonar](#): Remove Beta label
- [Elastic_Defend](#): Remove Beta label
- [Elastic_Fleet_Agents](#): Remove Beta label

- **[Hardenize](#)**: Remove Beta label
- **[IGEL UMS](#)**: Remove Beta label
- **[Kaseya VSA 9](#)**: Remove Beta label
- **[Keycloak Identity Management](#)**: Remove Beta label
- **[Lansweeper Classic](#)**: Remove Beta label
- **[Microsoft Intune](#)**:
 - Add support for filtering out devices by last sync date
 - MicrosoftIntuneDevice: declare additional properties for queriability
- **[Mimecast](#)**: Remove Beta label
- **[Nautobot](#)**: Remove Beta label
- **[OneLogin](#)**: Remove Beta label
- **[OpenAI](#)**: Remove Beta label
- **[Phosphorus](#)**: Remove Beta label
- **[Proactivanet](#)**: Remove Beta label
- **[Qualys VMDR](#)**: QualysHost: IP_INTERFACES.IP validation fix
- **[Remediant SecureONE](#)**: Remove Beta label
- **[Snow Atlas](#)**: Remove Beta label
- **[SolarWinds IT Asset Management](#)**:
 - Remove Beta label
 - Updated SolarWinds ITAM User type with missing schema fields
- **[Sumo Logic](#)**: Remove Beta label
- **[Veracode](#)**: Remove Beta label

[Top of page](#)

Cloud Security (InsightCloudSec)

- [Version 26.4.14](#)
- [Mimics Infrastructure as Code \(IaC\) Scanning Tool](#)

› Release availability for self-hosted users

Version 26.4.14

Software release date: April 14, 2026 | **Release notes published:** April 13, 2026

Upcoming Changes to OCI Vault and Secret Resource Identification

Planned for version 26.5.5, updates to `resource_id` generation for the Vault and Secret resource types in Oracle Cloud Infrastructure (OCI) environments will ensure global uniqueness and correct parent-child relationships. The updated format incorporates the Vault OCID.

- Impact:
 - Existing Vaults and Secrets will be re-identified as new resources on the first harvest after this update
 - Bots, alerts, or integrations may be triggered if configured to act on newly discovered resource types
- Reason for this change:
 - Previous `resource_id` generation relied on non-unique display names
 - This could cause referential integrity issues and failed secret harvesting
 - Incorporating the Vault OCID ensures unique and consistent identification across compartments

Improved

- Consolidated billable resource calculations for improved accuracy and performance.
- Updated opt-in Layered Context columns default sort to descending order.
- Renamed the **Visibility** column title to **Harvest Visibility** in the Cloud Accounts table for clarity.
- Updated finding name to “Compromised IAM Credentials Detected” for AWS GuardDuty finding `CredentialAccess:IAMUser/CompromisedCredentials`.
- Added filtering for bots with invalid instructions on the Bot Factory listing page.
- Updated Content Security Policy (CSP) to allow `data:` sources for loading fonts.
- Updated the Cloud List page to now display with an icon and details when an AWS account has been onboarded with an IAM permission boundary attached to the role.

- Added error context modal for harvesters and background jobs to assist with troubleshooting failed jobs.
- Standardized dropdown selects to use in-product tooltip styling for improved readability and consistency.
- Updated DMS EDH re-harvest schedule to 20 minutes and added `instance_type` and `storage_size` fields for change detection.
- Removed redundant retention field from Diagnostic Settings query filters.

New Resources

- Added support for `NetAppFilesAccount` resource type with new harvester `NetAppFilesAccountHarvester`:
 - Action for `NetAppFilesAccountHarvester`: “add tags”
 - New permissions required: `Microsoft.NetApp/netAppAccounts/read`
- Added support for `ContainerAppJob` resource type with new harvester `ContainerAppJobHarvester`:
 - Action for `ContainerAppJobHarvester`: “add tags”
 - New permissions required: `Microsoft.App/jobs/read`

New Insights

- **Azure File Share with NFS Not Configured as Root Squash**: Identifies Azure File Shares with NFS that lack root squash configuration.
- **Storage Container Without Locked Immutability Policy**: Identifies Storage Containers that do not have a locked immutability policy configured.
- **NetApp Files Account Encryption Key Source Set to Platform-Managed**: Identifies NetApp Files accounts using platform-managed encryption keys.
- **Recovery Services Vault With Cross Subscription Restore Enabled**: Identifies Recovery Services Vaults that have cross subscription restore enabled. Maps to CIS Azure Storage Services Benchmark v1.0.0 Recommendation 5.2.7.
- **Recovery Services Vault With Public Network Access Enabled**: Identifies Recovery Services Vaults that have public network access set to `Allow from all networks`. Maps to CIS Azure Storage Services Benchmark v1.0.0 Recommendation 5.2.5.
- **Recovery Services Vault Without Infrastructure Encryption Enabled**: Identifies Recovery Services Vaults that use Customer-Managed Key (CMK)

encryption but do not have infrastructure encryption enabled. Maps to CIS Azure Storage Services Benchmark v1.0.0 Recommendation 5.2.4.

- **Azure Backup Vault Without Infrastructure Encryption Enabled:** Identifies backup vaults without infrastructure encryption.

New Query Filters

- **Azure File Share with NFS Not Configured as Root Squash:** Filters for Azure File Shares lacking root squash configuration.
- **Verify NetApp Files Account Encryption Key Source:** Filters NetApp Files accounts by encryption key source.
- **Recovery Services Vault Cross Subscription Restore State:** Filters vaults by cross-subscription restore configuration.
- **Recovery Services Vault Public Network Access:** Filters vaults by public network access settings.
- **Recovery Services Vault Infrastructure Encryption:** Filters vaults by infrastructure encryption status.
- **Azure Backup Vaults Infrastructure Encryption:** Filters backup vaults by infrastructure encryption configuration.

New Compliance Packs

- Added the **CIS Microsoft Azure Compute Services Benchmark 2.0.0** compliance pack.

Fixed

- Fixed a bug where applying tags to S3 Buckets failed if the bucket contained AWS-managed tags.
- Enhanced throttling protection for Bot Tagging action operations to resolve throttling errors when a bot matches against a high volume of resources.
- Fixed an issue where delete actions for Azure Logic Apps triggered via ICS failed with errors for both Consumption and Standard plans. Delete operations now complete successfully across Logic App plan types.
- Fixed an issue with unnamed series data in Compliance Overview Reporting graphs.
- Fixed an issue where `log_group_name` for build projects was set to None if using default CloudWatch log group.

- Fixed an issue where AliCloud NetworkHarvester did not collect tags for AliCloud VPC network resources, resulting in missing tags in ICS and the ResourceTags table.
- Fixed an issue with `AWSVolumeHarvesterRedux` where the app column in an AWS volume ResourceTags table entry was not updated correctly if the value of the application tag key changed.
- Added optional `minimum_severity` parameter to the `get_insights` method of resource objects for filtering matched insights to only include higher severity ones.
- Updated Query Filters page so links to bots associated with a specific query filter properly filter the bot listing page.

Release of Kubernetes Scanner v5.0.2

- Released with vulnerability fixes. Internal components and their versions are available in the chart value file.
 - View data using: `helm show values <chart name> | grep -E 'Name:|Version:'`
 - Update using `helm upgrade --install` command referenced in Kubernetes Scanner documentation

[Top of page](#)

Mimics Infrastructure as Code (IaC) Scanning Tool

No updates released at this time.

[Top of page](#)

SIEM (InsightIDR)

Improved:

- Alert rendering performance optimized to reduce latency.
- Investigation's Endpoint Queries and Alert Payload information UI modernized.
- User details now include associated admin groups across Identity Providers.

[Top of page](#)

Vulnerability Management (InsightVM)

- [8.43.0](#)
- [8.42.0](#)
- [8.41.0](#)

Version 8.43.0

Software release date: Apr 20, 2026 | **Release notes published:** Apr 16, 2026

Improved:

- Improved access control logic to ensure non-admin users only see sites they have permission to access across both the Assets page and the Scan History tab, providing a more secure and consistent user experience.

Fixed:

- Resolved an issue affecting the accuracy of Cisco IOS XE fingerprinting, ensuring correct device identification.
- Fixed an issue that caused false positives for certain VMware environments, including Cisco APIC devices, improving detection accuracy.
- Addressed an issue where some AWS Discovery Connections failed and prevented configuration metadata from loading. Connections now load correctly and can be used as expected.
- Resolved an issue impacting access to multi-silo consoles, restoring expected user access.
- Fixed an issue where updates to custom scan templates via API did not persist to the underlying XML configuration files. Updates are now applied correctly.

Version 8.42.0

Software release date: Apr 13, 2026 | **Release notes published:** Apr 9, 2026

New:

- **New Policy Content:** Support has been added for the following versions of CIS and DISA STIG benchmarks to enable organizations to adhere to the latest security best practices:
 - DISA STIG F5 Big-IP TMOS VPN V1R1
 - DISA STIG Builtin Support for SUSE Linux Enterprise Server (SLES) 15 V2R7
 - DISA STIG Builtin Support for Google Chrome Browser for Windows V2R1
 - DISA STIG Builtin Support for Oracle Linux 9 V1R2
 - DISA STIG Red Hat Enterprise Linux 9 V2R7
 - CIS Benchmark - Add Builtin Support for Apple macOS 14.0 Sonoma Benchmark V3.0.0
 - CIS Benchmark Palo Alto firewalls 10 v1.3.0

Improved:

- **Policy Proof Readability (Dark Theme).** Enhanced the display of policy proof details in dark mode to improve contrast and readability.
- **User Management Search Enhancements.** Improved user search functionality to support lookup by first name or last name, making it easier to locate users in large environments.

Fixed:

- **Scan Assistant OS Detection.** Addressed an issue impacting Scan Assistant fingerprinting accuracy, ensuring the correct operating system is identified under all conditions.
- **MOVEit Transfer Vulnerability Detection.** Fixed a false positive for CVE-2023-46445 (Progress MOVEit Transfer). Assets are now correctly marked as not vulnerable once mitigation steps are applied.
- **Discovered Assets - Clear All Function.** Resolved an issue affecting the “Clear All” delete function for large Sonar discovery connections. The operation now reliably removes all discovered assets at scale.
- **Dynamic Site Statistics Accuracy.** Fixed an issue where negative VM counts could appear in Dynamic Site Statistics. Counts now accurately reflect targets after exclusions, even in complex configurations.
- **PostgreSQL Policy Scan Errors.** Addressed a fingerprinting issue causing errors during policy scans of PostgreSQL instances hosted on Amazon RDS or Docker.

- Resolved a false positive for rule 4.1.9 in the CIS Red Hat Enterprise Linux 7 Level 2 Server benchmark (v3.1.1).
- Fixed errors in proof details for rules 5.1.5 and 5.1.7 in the CIS Ubuntu Linux 24.04 LTS benchmark, ensuring accurate and complete reporting.

Version 8.41.0

Software release date: Apr 6, 2026 | **Release notes published:** Apr 2, 2026

Improved:

- Upgraded Nmap to version 7.98, delivering improved CPU and memory efficiency during the scanning process. This will leverage previous optimizations to port data ingestion allowing for lighter XML processing, resulting in more efficient scan performance.
 - For more details and recommended actions, read the [Nmap Upgrade documentation](#) [↗].
- Updated APIv3 endpoint `/api/3/scan_engines/{engine_id}/scans` for engine pools to ensure complete scan history results are returned for all participating engines.

Fixed:

- Addressed an OS fingerprinting issue where under certain conditions, a mismatch occurred for operating system details between the Security Console and Exposure Analytics. OS information is now consistent for newly assessed assets and will be corrected for existing affected assets after rescanning.
- Addressed an issue causing failures when running the Perform Diagnostics function within the Security Console. This feature now executes as expected.

[Top of page](#)

Nexpose

- [8.43.0](#)
- [8.42.0](#)
- [8.41.0](#)

Version 8.43.0

Software release date: Apr 20, 2026 | **Release notes published:** Apr 16, 2026

Improved:

- Improved access control logic to ensure non-admin users only see sites they have permission to access across both the Assets page and the Scan History tab, providing a more secure and consistent user experience.

Fixed:

- Resolved an issue affecting the accuracy of Cisco IOS XE fingerprinting, ensuring correct device identification.
- Fixed an issue that caused false positives for certain VMware environments, including Cisco APIC devices, improving detection accuracy.
- Addressed an issue where some AWS Discovery Connections failed and prevented configuration metadata from loading. Connections now load correctly and can be used as expected.
- Resolved an issue impacting access to multi-silo consoles, restoring expected user access.
- Fixed an issue where updates to custom scan templates via API did not persist to the underlying XML configuration files. Updates are now applied correctly.

Version 8.42.0

Software release date: Apr 13, 2026 | **Release notes published:** Apr 9, 2026

New:

- New Policy Content: Support has been added for the following versions of CIS and DISA STIG benchmarks to enable organizations to adhere to the latest security best practices:
 - DISA STIG F5 Big-IP TMOS VPN V1R1
 - DISA STIG Builtin Support for SUSE Linux Enterprise Server (SLES) 15 V2R7
 - DISA STIG Builtin Support for Google Chrome Browser for Windows V2R1
 - DISA STIG Builtin Support for Oracle Linux 9 V1R2

- DISA STIG Red Hat Enterprise Linux 9 V2R7
- CIS Benchmark - Add Builtin Support for Apple macOS 14.0 Sonoma Benchmark V3.0.0
- CIS Benchmark Palo Alto firewalls 10 v1.3.0

Improved:

- Policy Proof Readability (Dark Theme). Enhanced the display of policy proof details in dark mode to improve contrast and readability.
- User Management Search Enhancements. Improved user search functionality to support lookup by first name or last name, making it easier to locate users in large environments.

Fixed:

- Scan Assistant OS Detection. Addressed an issue impacting Scan Assistant fingerprinting accuracy, ensuring the correct operating system is identified under all conditions.
- MOVEit Transfer Vulnerability Detection. Fixed a false positive for CVE-2023-46445 (Progress MOVEit Transfer). Assets are now correctly marked as not vulnerable once mitigation steps are applied.
- Discovered Assets - Clear All Function. Resolved an issue affecting the “Clear All” delete function for large Sonar discovery connections. The operation now reliably removes all discovered assets at scale.
- Dynamic Site Statistics Accuracy. Fixed an issue where negative VM counts could appear in Dynamic Site Statistics. Counts now accurately reflect targets after exclusions, even in complex configurations.
- PostgreSQL Policy Scan Errors. Addressed a fingerprinting issue causing errors during policy scans of PostgreSQL instances hosted on Amazon RDS or Docker.
- Resolved a false positive for rule 4.1.9 in the CIS Red Hat Enterprise Linux 7 Level 2 Server benchmark (v3.1.1).
- Fixed errors in proof details for rules 5.1.5 and 5.1.7 in the CIS Ubuntu Linux 24.04 LTS benchmark, ensuring accurate and complete reporting.

Version 8.41.0

Software release date: Apr 6, 2026 | **Release notes published:** Apr 2, 2026

Improved:

- Upgraded Nmap to version 7.98, delivering improved CPU and memory efficiency during the scanning process. This will leverage previous optimizations to port data ingestion allowing for lighter XML processing, resulting in more efficient scan performance.
 - For more details and recommended actions, read the [Nmap Upgrade documentation](#) [↗].
- Updated APIv3 endpoint `/api/3/scan_engines/{engine_id}/scans` for engine pools to ensure complete scan history results are returned for all participating engines.

Fixed:

- Addressed an issue causing failures when running the Perform Diagnostics function within the Security Console. This feature now executes as expected.

[Top of page](#)

Digital Risk Protection (Threat Command)

No updates released at this time.

[Top of page](#)

Rapid7 Agent (Insight Agent)

- [Version 4.1.0.2](#)

Version 4.1.0.2

New:

- **Support for Upcoming On-Demand Vulnerability Scanning:** This release introduces foundational support within the Agent for an upcoming on-demand vulnerability scanning capability. With this update, the Agent is now prepared to support ad-hoc scan requests, enabling real-time vulnerability assessments outside

of the traditional scheduled scanning cadence to enable more flexible and responsive scanning workflows.

Improved:

- Rapid7's in-house `fswalk` command can now search for files with the `.exe` extension, improving coverage during assessments.

Fixed:

- Rapid7 Agent data collection now correctly identifies Google Cloud Compute assets as virtual machines.
- Removed use of the Python `eval()` function in Rapid7 Agent beaconing logic to eliminate potential exposure to remote code execution (CVE-2026-4837). Because the Agent uses mutual TLS (mTLS) to verify commands from the Rapid7 Platform, it is unlikely that the `eval()` function could be exploited remotely. Thanks to John Rodriguez from CyberDagger, LLC for reporting this issue.
- Restricted specific Rapid7 Agent file paths on Windows installations to the `SYSTEM` user to prevent potential unauthorized access to sensitive files (CVE-2026-4482). Thanks to Peter Gabaldon @ [ITRESIT](#) ↗ for reporting this issue.
- Rapid7 Agent no longer attempts to load an OpenSSL file from a non-existent path in non-FIPs installations, preventing the possibility of loading arbitrary files. Thanks to Dell Security Assurance for reporting this issue.
- Updated the Python cryptography library to version 46.0.5 to address CVE-2026-26007.
- Resolved an OpenSSL integration issue with the `applink.c` function that prevented application execution in certain Windows environments.

Updated Operating System Support:

- As of version 4.1.0.2, the Rapid7 Agent (Insight Agent) no longer supports the following operating systems for any architecture:
 - Ubuntu 16.04
 - SUSE Enterprise 15.2/15 SP2

[Top of page](#)

Next-Generation Antivirus

No updates released at this time.

[Top of page](#)

Ransomware Prevention

No updates released at this time.

[Top of page](#)

Velociraptor

No updates released at this time.

[Top of page](#)

© Rapid7

[Legal Terms](#)

[Privacy Policy](#)

[Export Notice](#)

[Trust](#)