Release Notes

Published

2024-03-25

Juniper Secure Edge CASB and DLP Release 23.3

Engineering
Simplicity

Copyright and Disclaimer

The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This document may provide access to, or information on content, products and services from third parties. Lookout, Inc. and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Lookout, Inc. and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

Introduction

Juniper Secure Edge provides Firewall as a Service (FWaaS) in a single-stack software architecture managed by Juniper Security Director Cloud.

Juniper Secure Edge empowers organizations to secure their workforce wherever they are. With consistent security policies that follow the user, device, and application without having to copy over or re-create rule sets, Juniper Secure Edge makes it easy to deploy cloud-delivered application control, intrusion prevention content and Web filtering and effective threat prevention without breaking the visibility or security enforcement.

These release notes describe new and changed features and known and resolved problems in the software.

For details about working with product features, refer to the *Juniper Secure Edge CASB and DLP Administration Guide*.

What's New

- You can now configure Quarantine as a policy action, enable Quarantine review, and release workflow for Salesforce API mode protection. You now have a choice to disable file downloads until DLP and Malware scan is complete.
- For Salesforce applications, the onboarding workflow now provides an additional prompt that enables you to specify restrictions for file downloads. The Block Downloads for security scan prompt includes two options: 1) Never, and 2) Until scan is complete. A text box is also available to provide information about any file not available for download.
- With this update, we perform Luhn check validation for Credit Card Regex patterns, even when the rule is not combined with a keyword dictionary.
- When a Google Drive label sync action fails more than twice, further sync actions stop, and administrators receive a system-generated email.

What's Changed

- We made these improvements to the User Directory sync capability using Ping Identity:
  - The platform now has an API connector for Ping Identity to facilitate the User Directory sync action. After successful integration, the platform syncs the User Directory from Ping Identity periodically.
  - The platform also supports SCIM functionality for Ping Identity, enabling automated user provisioning to prevent delays in user sync when you add, delete, or modify a user.

- We revamped these reports to offer enhanced data, providing deeper insights into data security.
  - Anomaly Reports: These reports focus on User and Entity Behavioral Analysis (UEBA) capability provided by the platform. They show anomalous user and content activity, which can indicate insider threats or potential malware or ransomware.
  - Compliance Reports: These reports help you gain insights into your organization's compliance status and adherence to security policies. They show findings from observations of policy violations, users and applications involved, and remediation steps to address noncompliance issues.

Resolved Issues

None for this release.

Known Issues

None for this release.

Upgrade and Downgrade Instructions

None for this release.