FIREMON

Improve Security Operations
Improve Security Outcomes

Automation at play: How automation elevates your network security posture

Dawid Kowalski– Sr Technical Director EMEA

Improve Security Operations. Improve Security Outcomes.

Would you agree?

You've spent a lot of money on….

Consequences of Ignoring Security Policies

*Through 2023, "**99% of firewall breaches will be caused by misconfigurations, not firewalls.**"*

Gartner®

Exposed breach avenues and vulnerabilities from policy misconfigurations

Run the risk of unplanned outages due to configuration errors in firewall policies

Increased staffing costs to keep up with manual change processes and compliance reporting

Incur fines and risk lawsuits from compliance violations caused by firewall changes

Assigner: Fortinet

Published: 2022-10-18 **Updated:** 2022-10-19

An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

Product Status

Vendor & Product	Affected
Fortinet Fortinet FortiOS, FortiProxy, FortiSwitchManager	FortiOS 7.2.1, 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0; FortiProxy 7.2.0, 7.0.6, 7.0.5, 7.0.4, 7.0.3, 7.0.2, 7.0.1, 7.0.0; FortiSwitchManager 7.2.0, 7.0.0

References

- **https://fortiguard.com/psirt/FG-IR-22-377**
- **http://packetstormsecurity.com/files/169431/Fortinet-FortiOS-FortiProxy-FortiSwitc Authentication-Bypass.html**

View additional information about **CVE-2022-40684** on NVD.

(Note: The NVD is not operated by the CVE Program)

https://www.cve.org/CVERecord?id=CVE-2022-40684

https://www.fortinet.com/blog/psirt-blogs/update-regarding-cve-2022-40684

```
# show user local
edit "fortigate-tech-support"
  set accprofile "super_admin"set vdom "root"
  set password ENC [...]
next
```

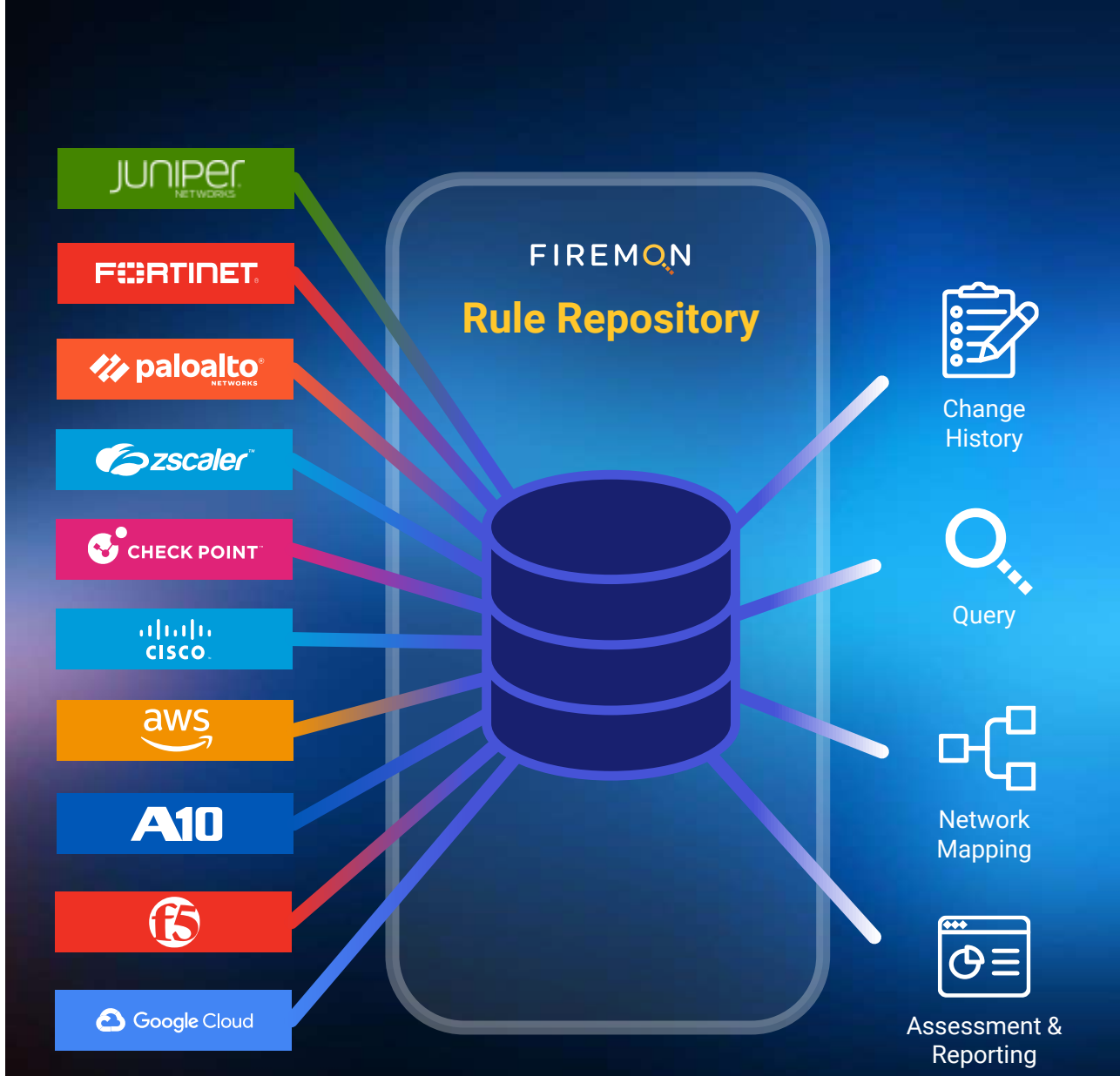
Fortinet recommends that customers validate their configuration to ensure that no unauthorized changes have been implemented by a malicious third party, regardless of whether they have upgraded.

Three steps to improve Network Security Posture Management

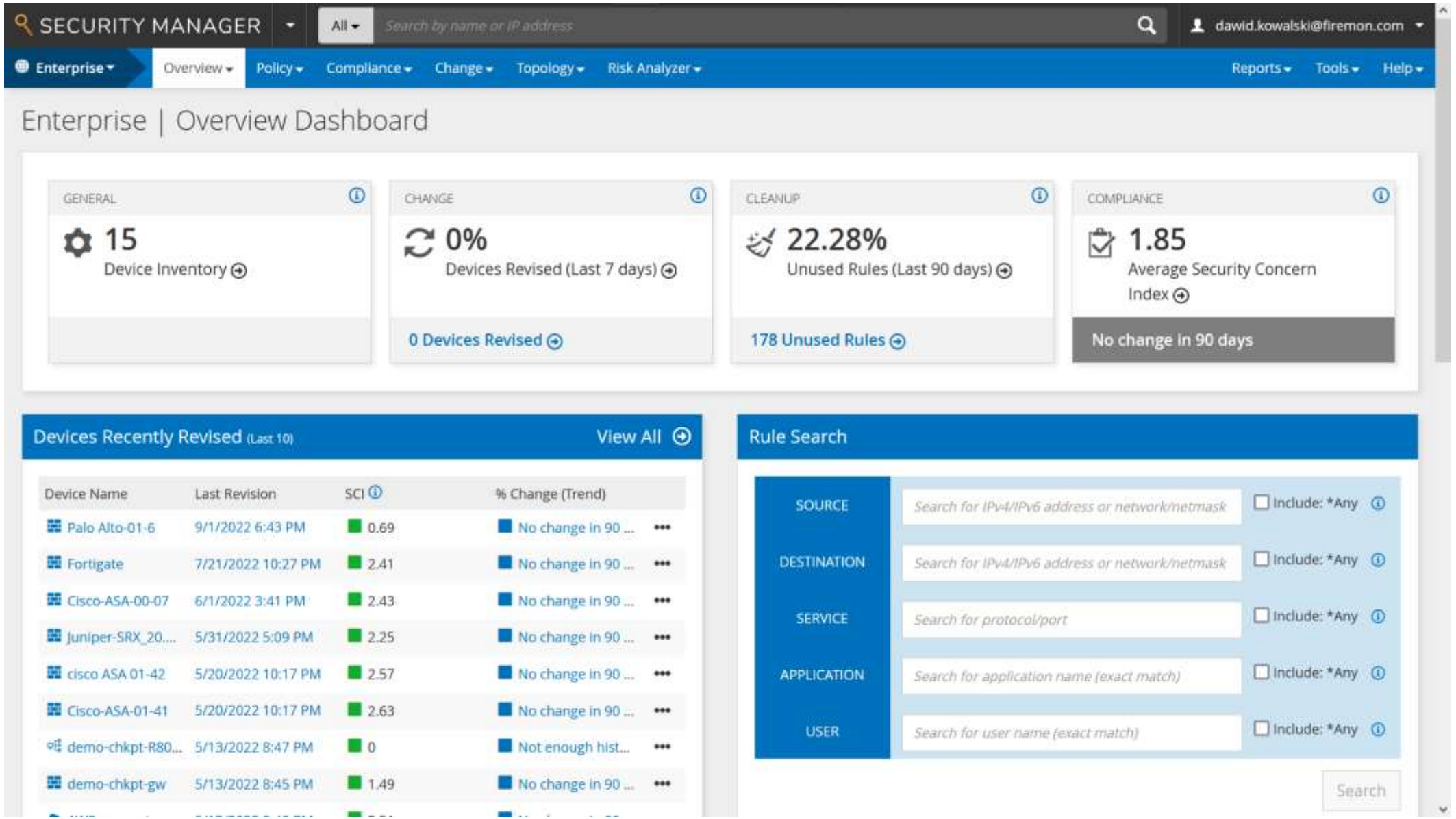
A Real-Time Inventory of Devices and Rules

- Gathers devices and policies across the entire environment
- Translates multi-vendor policies into a consistent, centralized rule database
- Full visibility and control for reporting, audit tracking, and policy management
- Realtime change detection and analysis

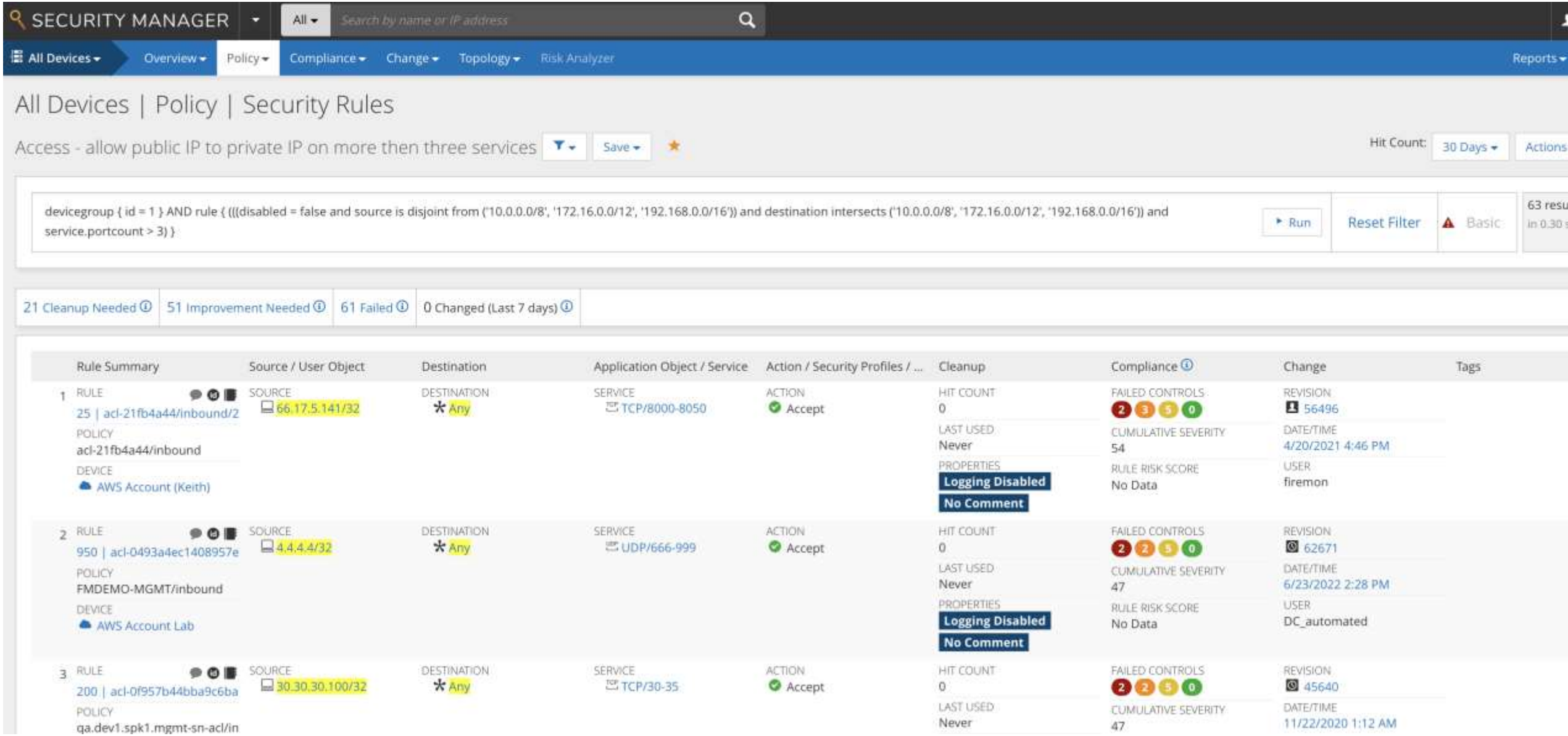
Out-of-the-box support for 80+ vendors and versions



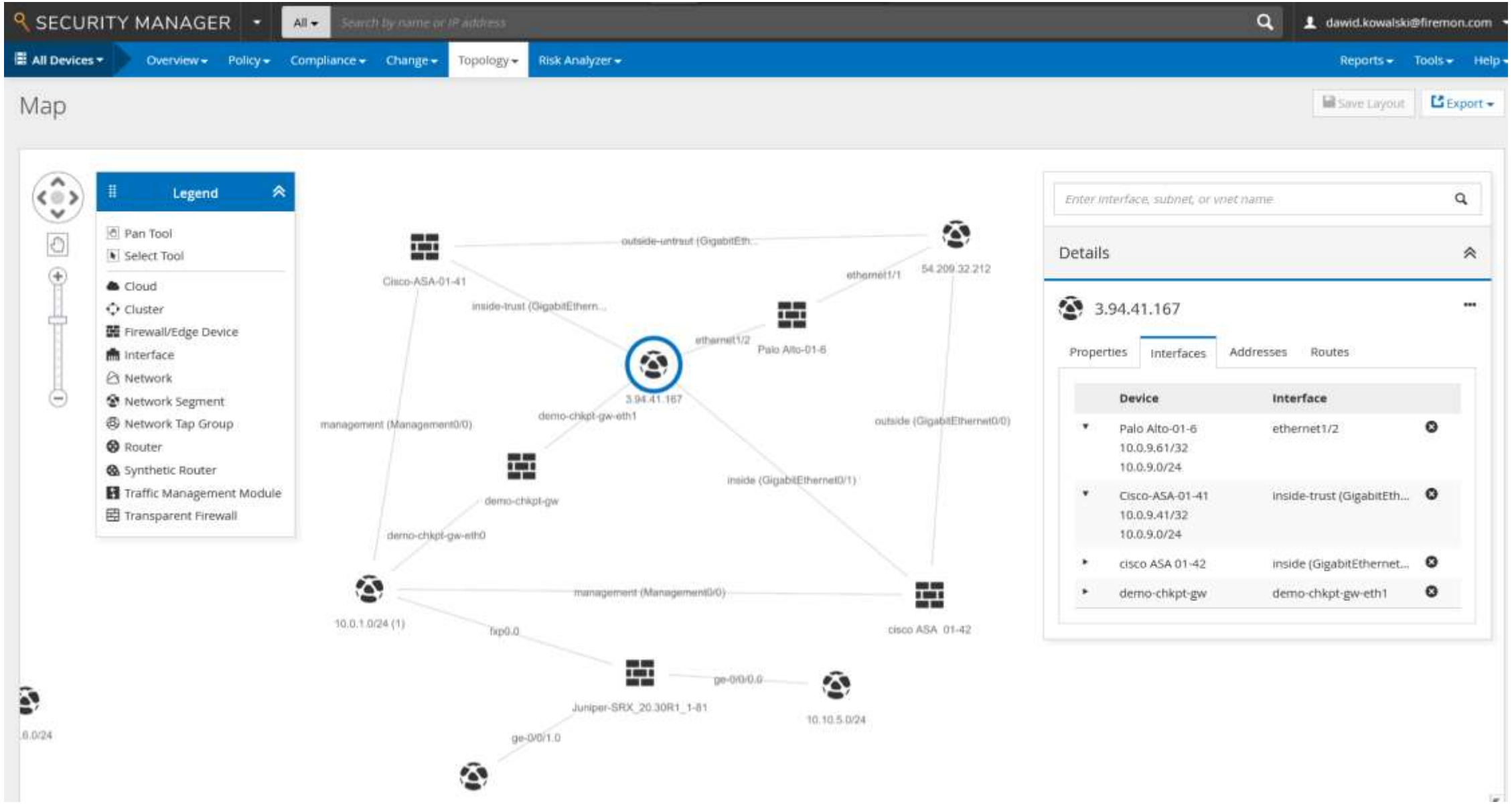
1 Visibility



1 Visibility



1 Visibility



Consolidated Compliance and Risk Assessments

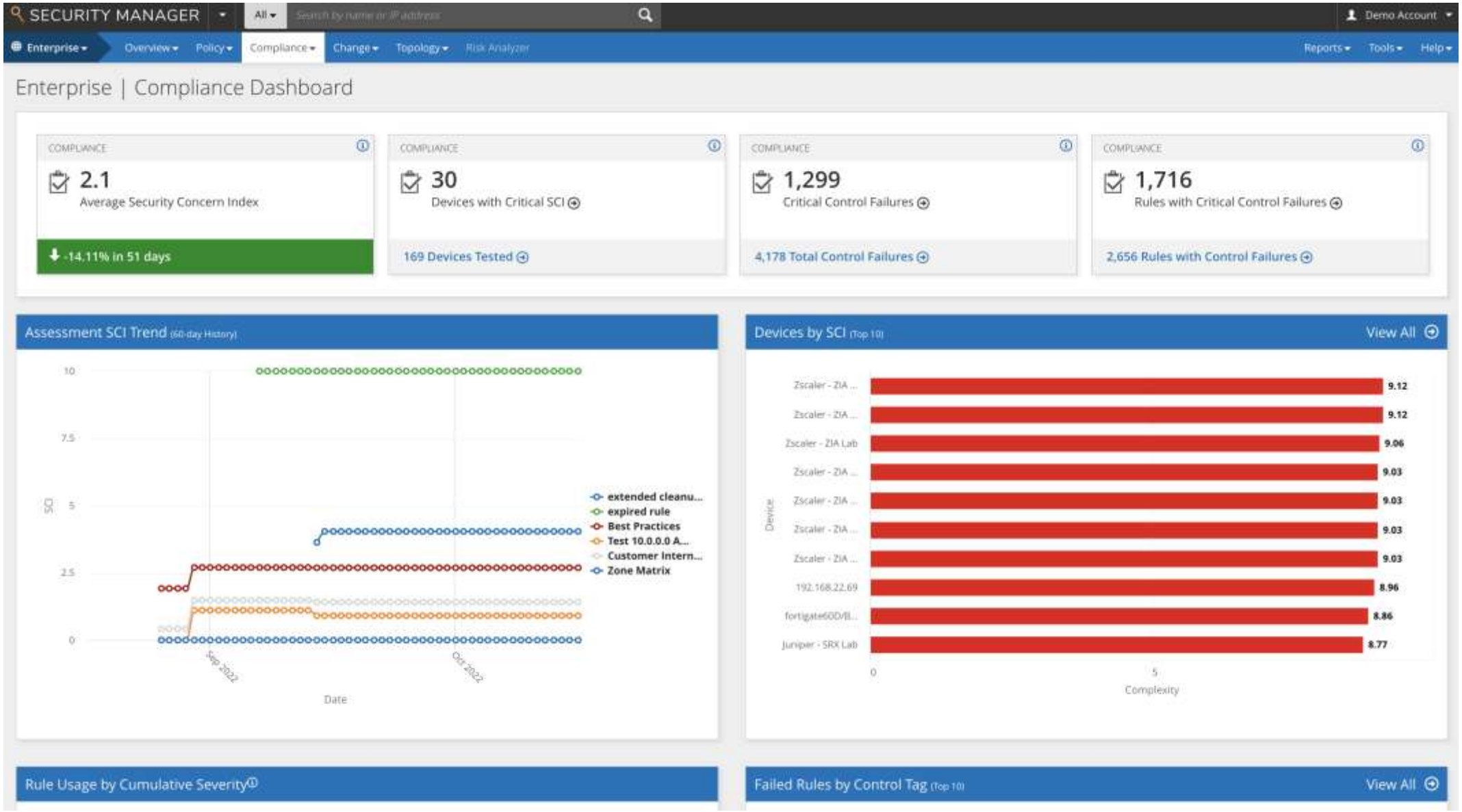
- Over 20 preconfigured reports
- Customizable reporting and alerts using over 500 included controls
- Add custom controls with SiQL search
- Unified dashboard with real-time Security Concern Index (SCI)
- Access path analysis and “what if” attack assessments
- Qualys, Rapid7, and Tenable integrations enrich rules with vulnerability data

Out-of-the-Box Reports Include:

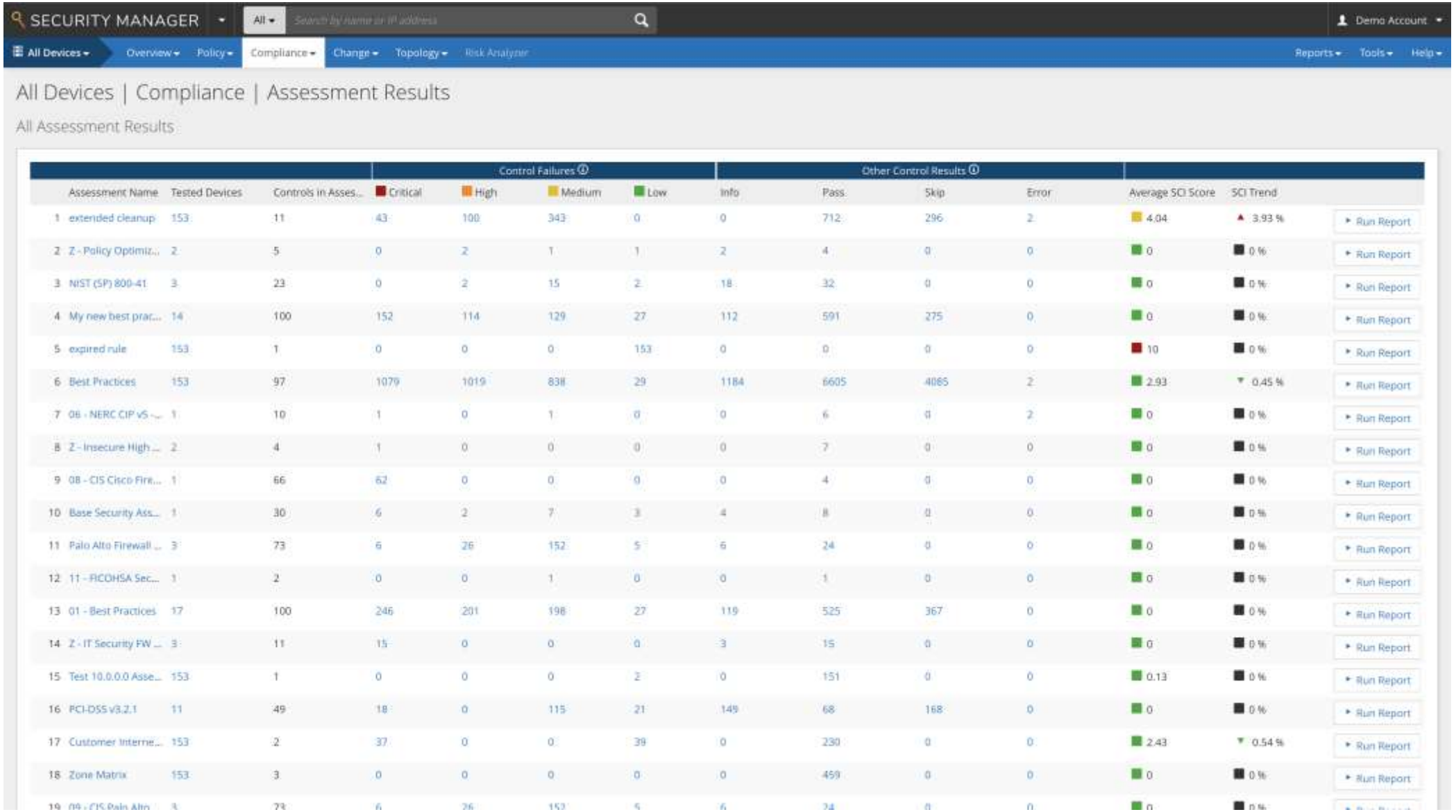
Compliance
- PCI-DSS
- NERC-CIP
- NIST
- HIPAA
- GDPR
- ISO/IEC 27001
- Sarbanes-Oxley

Assessments
- Asset exposure analysis
- Insecure services
- App outage protection
- Rules allowing bad actors
- Overly Permissive access

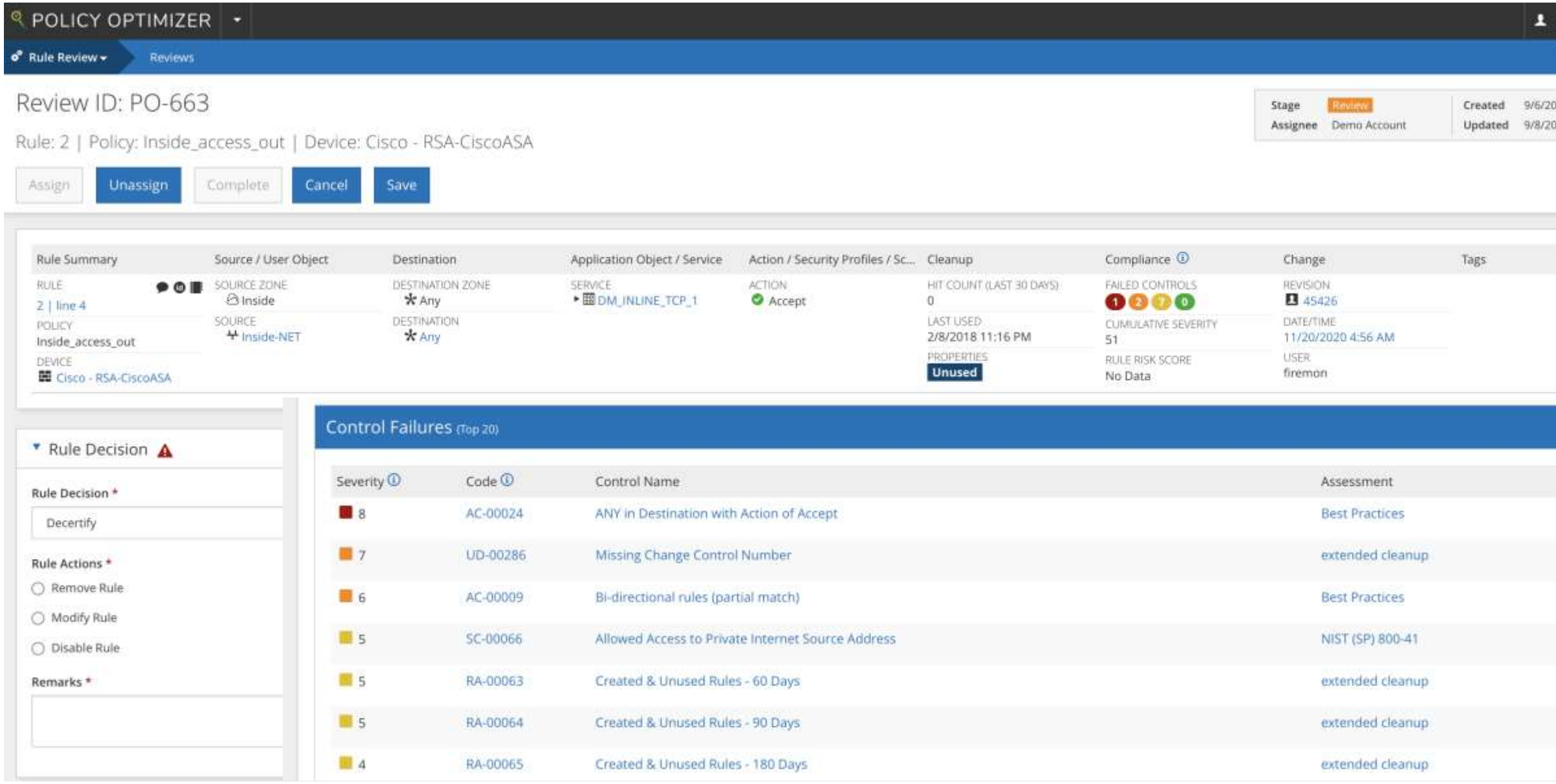
2 Continuous sec posture



2 Continuous sec posture



2 Continuous sec posture

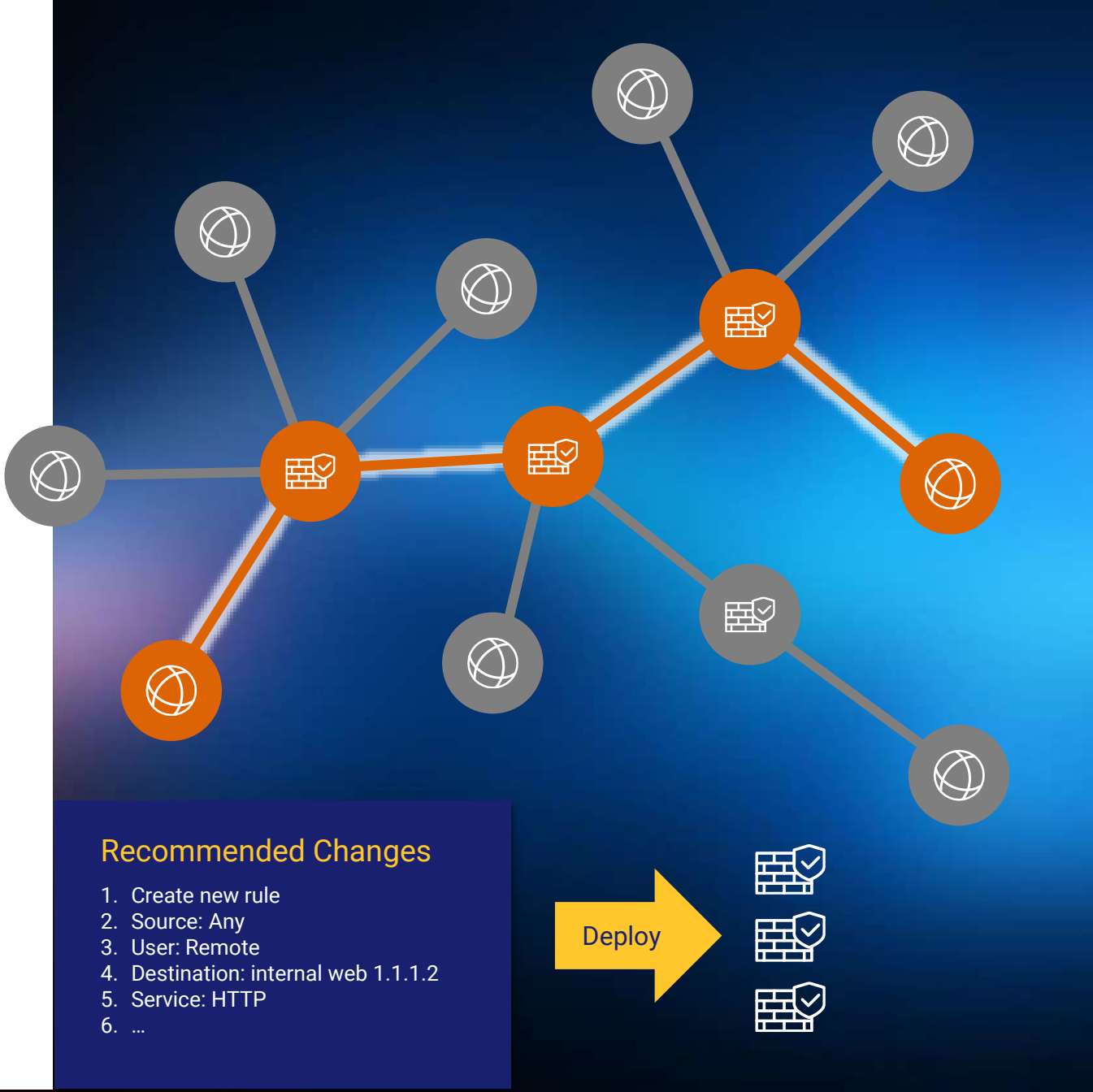


Easily Create and Update Policies

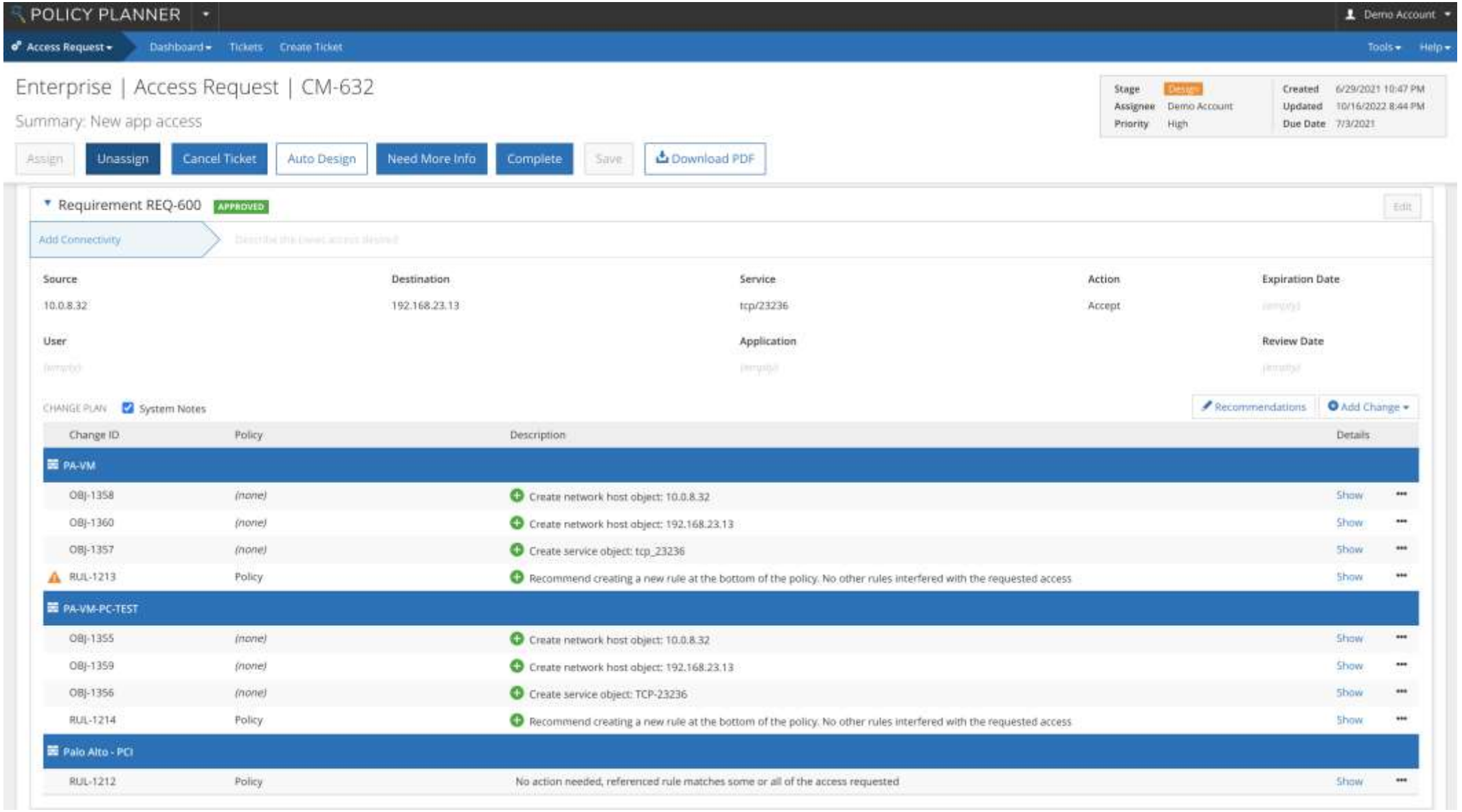
- Rule creation and change workflows
- Intelligent rule design recommendations
- Audit history captured automatically
- Option to automatically deploy changes

ITSM Integrations

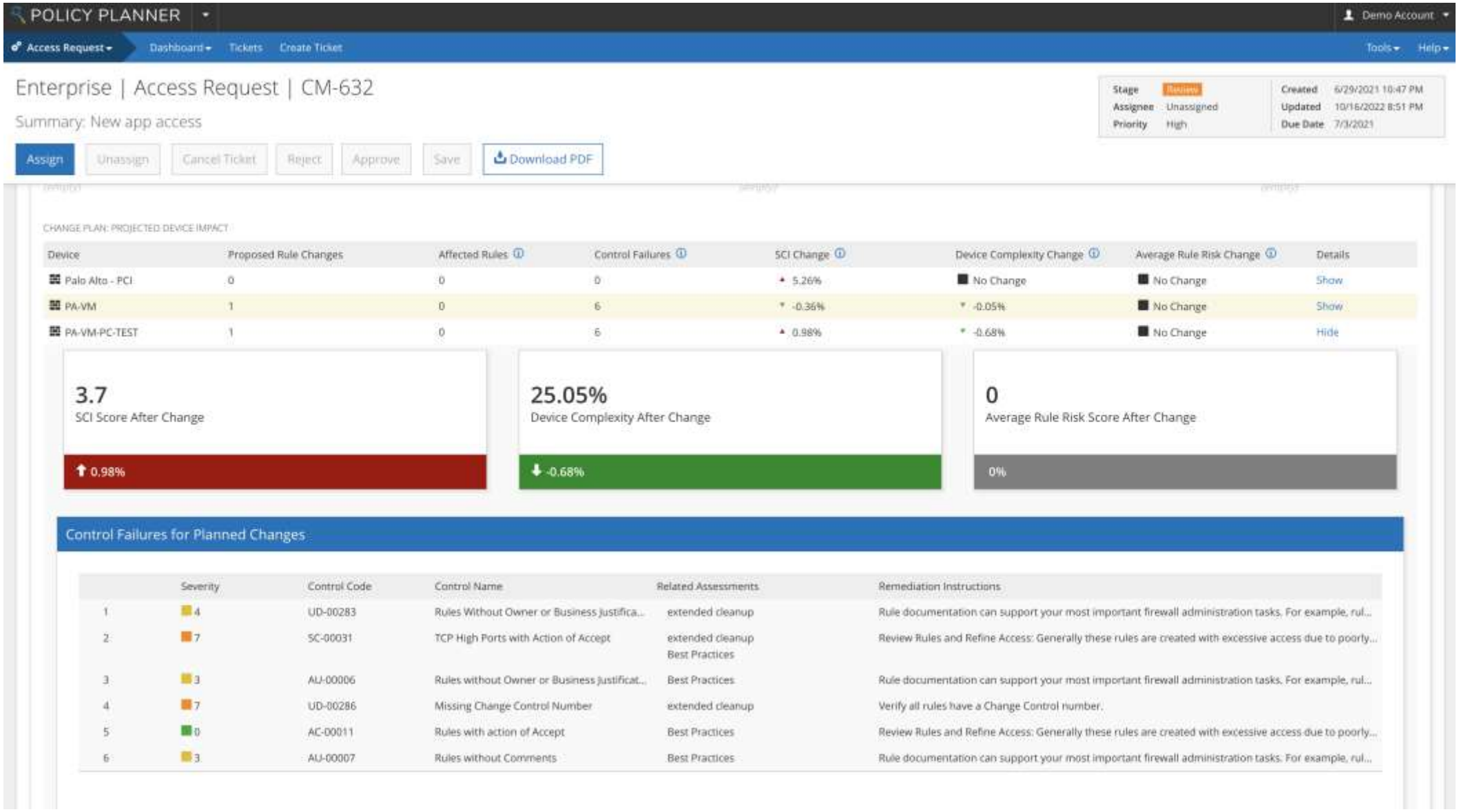
servicenow Jira Software bmc



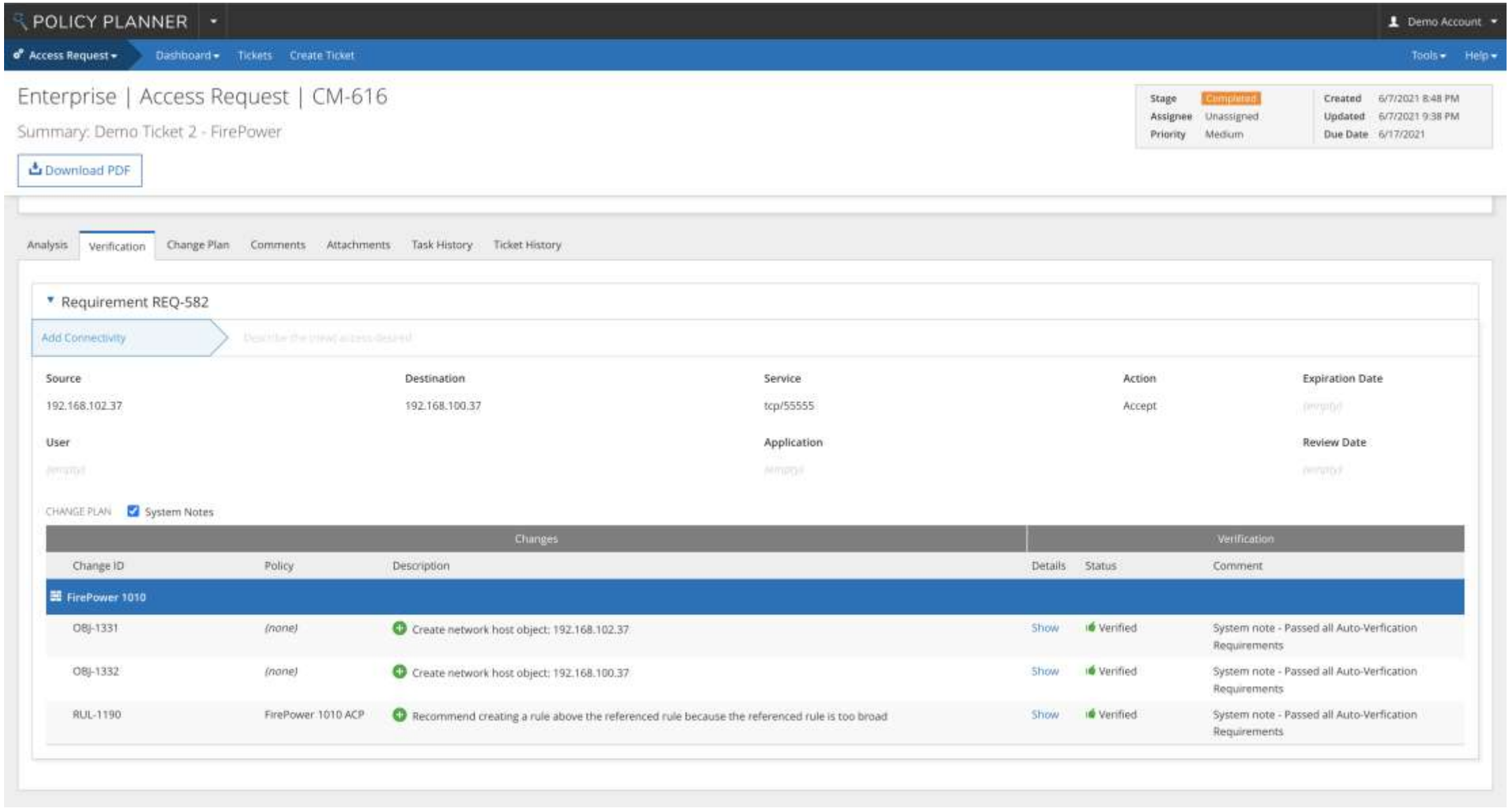
3 Secure the process



3 Secure the process



3 Secure the process



Thank you!

FIREMON

Improve Security Operations. Improve Security Outcomes.

firemon.com

Learn more;
Come see us at

Hall 7, Booth 7-401