KENNA Security

KENNASECURITY.COM

Kenna Security Implementation Success Guide

Get up & running in under an hour

Table of Contents

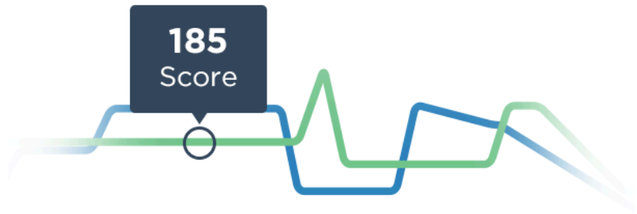
Success Guide

Welcome to Kenna!

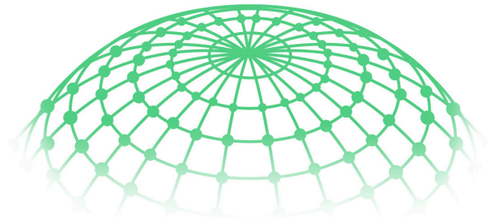
A Risk & Vulnerability Intelligence platform used by leading organizations to automate and enhance their vulnerability management efforts. The primary benefits of Kenna are to:

Automate the tedious process of prioritization vulnerabilities and putting hours back in your team's day—ensuring that they are identifying critical vulns with real-time context, rather than static CVSS scores or other methods

Gain a way to report on risk that's easy yet clearly communicable to the entire team—from security professionals to IT ops all the way to the executive suite



To enhance the efficacy of the entire security team by ensuring that they place their efforts on managing and reducing risk



This document is intended to help you embark on the implementation process, giving you valuable insights into how to use Kenna as well as creating a checklist for you to assess your efforts and the success of the platform.

But remember—you always have access to us in-person. Contact the Sales Engineer assigned to your account, or email support@kennasecurity at any time.

We look forward to helping make you successful!

Plan your Approach

Define Your Risk

How does your organization measure risk? With Kenna, you are able to create logical groups of assets and vulnerabilities on those assets. Each asset has a risk rating from 0 - 1000 based on the contextual threat data Kenna is constantly refreshing from many different threat sources. For each group you create, a Risk Meter becomes a way to understand and measure the risk posed to your networks based on the identified vulnerabilities, and how those vulnerabilities compare to current attacks, ease of exploit, and even potential zero days.

Risk Meter as a Foundation

Risk Meters provide the basis for measuring risk within the Kenna Platform. When planning for implementation, you should consider how you would group your assets to get the most benefit in the test environment.

How does your company work through the Vulnerability Management Lifecycle today? Are the teams who remediate all of your vulnerabilities divided up by business unit? By geography? By application stack? By technology?

When you initially create Risk Meters, it is helpful to consider how you communicate remediation information throughout your company and who consumes and takes action on that data.

Communicating Remediation

Once your groups are created you'll be sending prioritized fixes to your teams. For the scope of the implementation, do you have a test team ready to accept and use that list of prioritized patches? What does your current patch cycle look like? Would you be able to work through a cycle in 15 days? 30 days? Where would you like to improve?

Reporting

During implementation, you'll have the ability to review trending reports. The reports can both work to drive remediation, and to outline progress to management. In order to best take advantage of reporting, you should consider a few factors. First, especially if you are using file based connectors, you should plan to upload data at least twice, if not weekly. Second, if you are planning a management level presentation, the Risk Meters and trend reporting are key methods of communicating progress. Your Account Executive and Sales Engineer are also happy to assist with that presentation, just let them know.

Sync Your Data

Connectors

Kenna supports over 20 different vulnerability scanners today. You can sync both network and application scan data using our API based and File based connectors. Select **Connectors**, and then **+ Add Connector** to begin. Specific information for each connector is available in the application, and here is a brief description of each different category of connector:

View our Full List of Connectors here:
www.kennasecurity.com/connectors

API Connectors

An API connector can be scheduled to facilitate data sync within Kenna. Key considerations in scheduling the API sync are how often you scan, and which asset groups or IP ranges would be a good test environment. Scheduling of the Kenna API can then follow each scan, to pull back the results for analysis in the Kenna platform.

File Based Connectors

File based connectors are created/named; then manually run. For each supported file type, the overall process is similar. While specific detail about each file type is available in the application, key considerations with a file based connector would be having that file output synced at least twice during the implementation process. Then, the Kenna trend reports would be able to track changes over time and produce meaningful sample reports.

ServiceNow Connector

If your company is using ServiceNow as part of the remediation process, or you would like to test that functionality with Kenna, you will also configure a ServiceNow Connector on the Connectors page. You can choose to use the Kenna default ticket layout, or use one of your own incident templates. Your Sales Engineer can assist in this configuration - the ServiceNow connector requires the ITIL role.

Kenna's REST API

You may also be able to sync meaningful data to the platform using the Kenna REST API. While this can be a part of implementation, more often data from other systems like a CMDB system or GRC application is uploaded directly into the platform. Please work with your Sales team directly if you have data that you would like to sync during the process.

The Virtual Tunnel

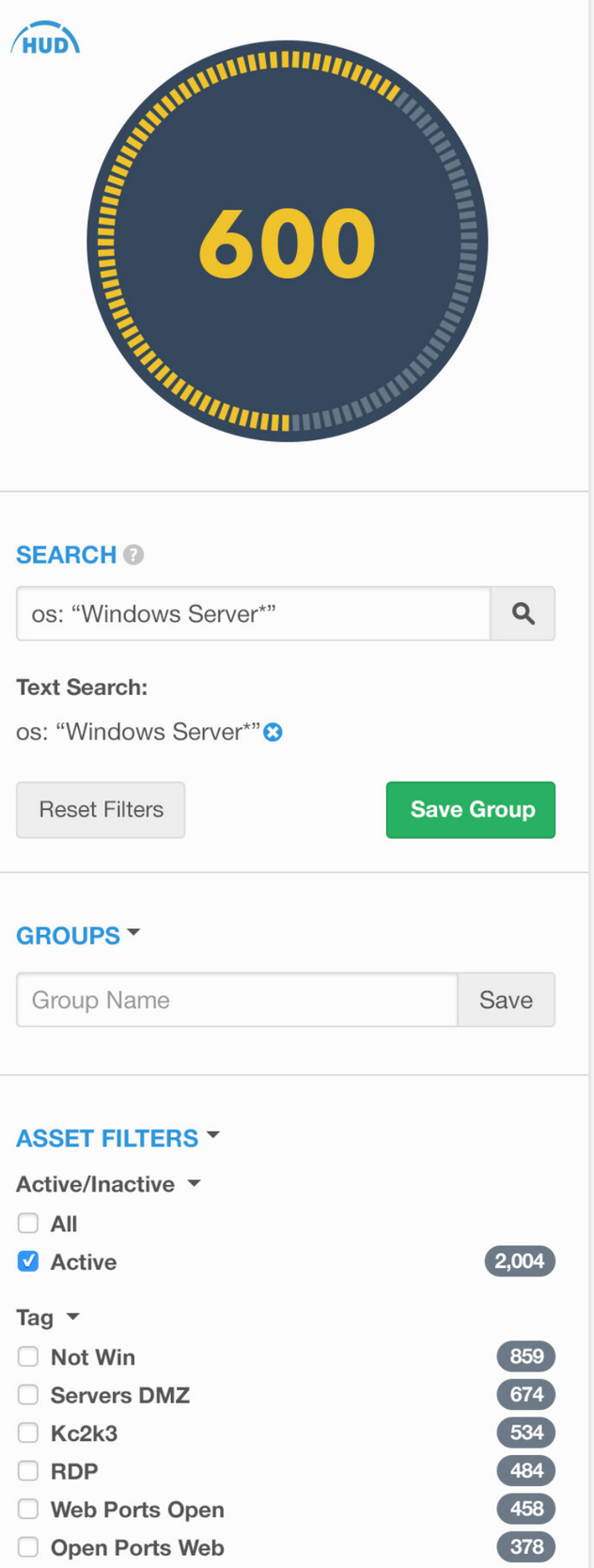
To allow API connections to internal (non-routable) systems, Kenna has a solution which creates a VPN tunnel to facilitate the connection. You may work with your SE to utilize this option if needed.

Build Risk Meters

After your vulnerability and asset data is synced into the platform, you begin the process of organizing that data into meaningful groups to measure risk in your organization. While there are multiple ways to group your data, only you know the most meaningful groups to create. Here are a few methods typically used to create those Risk Meter groups.

Tags

On the **Home** page, you may use existing tags to group assets – and you can search or filter for those tags using the area on the right side of the home page. Today Kenna will auto-tag assets imported from Qualys, Nexpose, Veracode, WhiteHat and HP Foritfy.



Build Risk Meters

Searches

On the **Home** page, you may use existing tags to group assets, and you can search or filter for those tags using the sidebar on the right side of the Home page. Today Kenna will auto-tag assets imported from Qualys, Nexpose, Veracode, WhiteHat and HP Foritfy.

Once the group is defined by search results, tags, or filters, select Save Group and give it a name. You have just created a Risk Meter.

Syntax Examples

Kenna offers many powerful ways to search your assets and vulnerabilities. Here are a few examples you might find useful. You can learn more about searching and other power tips by visiting: **https://help.kennasecurity.com**

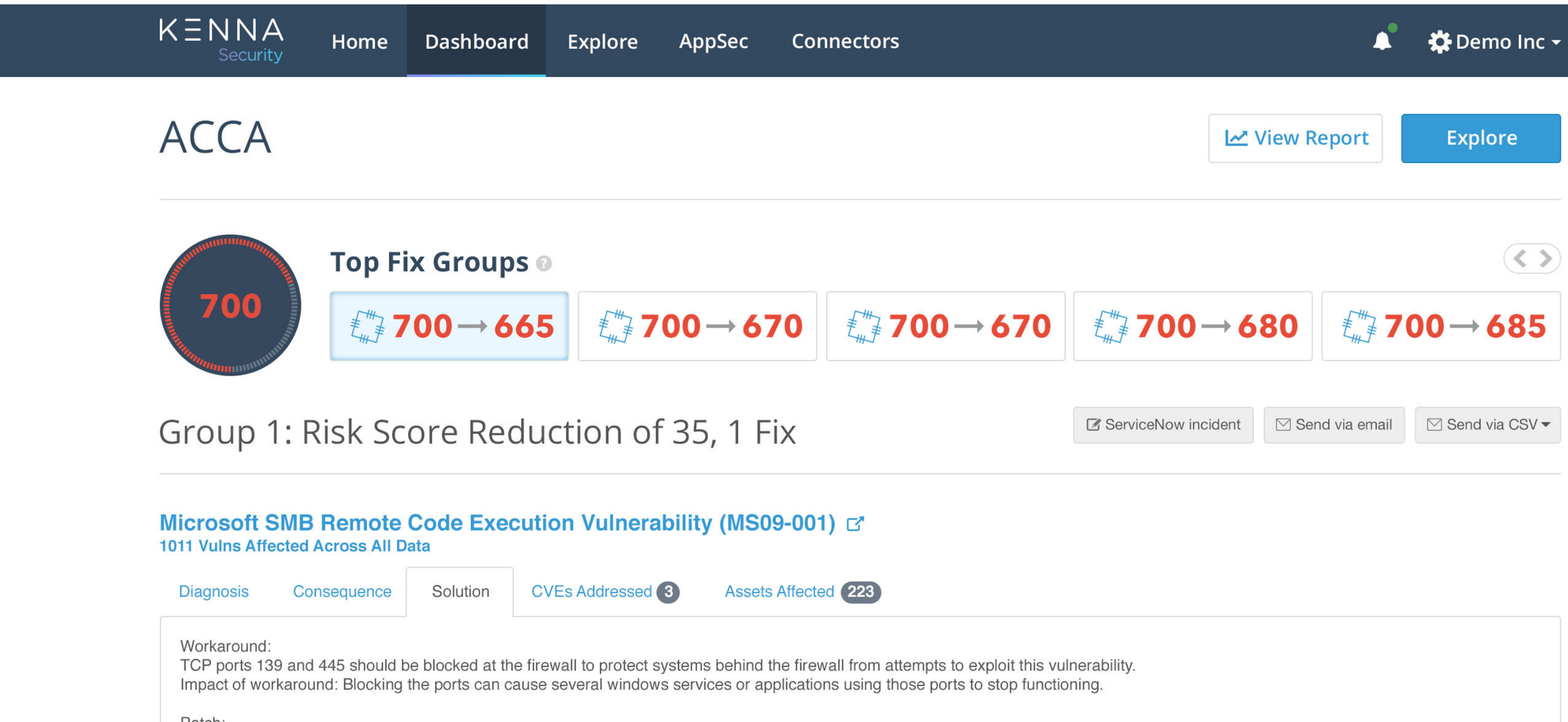
Syntax		Meaning
os: "Windows Server"		Search Windows assets
tag: "Chicago*"		Search asset tags using wildcard
ip:192.168.36.12		Search assets by IP address range
ip:[192.168.36.0 TO 192.168.36.255]		Search assets by IP address range Search
hostname:"internal.foo.com" Other ways to search assets include: **url**, **mac_address**, **netbios**, **fqdn**, and **file**		Search assets by hostname
asset_score:>=700	(0-1000 scale)	Search by asset risk scores of 700 or higher
vulnerability_score:<50	(0-100 scale)	Search vulnerabilities with risk scores below 50
cve:2014-0160		Search vulnerabilities using the Heartbleed CVE
cve_description:"shellshock"		Search by vulnerability description, useful for returning vulnerabilities by specific technology (eg "adobe" or "java") or by management-friendly name (eg "ShellShock")
wasc:WASC-13		Search vulnerabilities by WASC ID

Remediate with Top Fixes

Once you have created Risk Meter groups, it's time to get that fix information into the right hands. We've collected the best individual fixes and grouped them to make your remediation workflow easier. Use Top Fix Groups to maximize impact with the least amount of effort.

Top Fix groups are available for any of the Risk Meter groups you have created - choose "View Reports" from the dashboard for any risk meter, and select Top Fixes from the top of the reporting view.

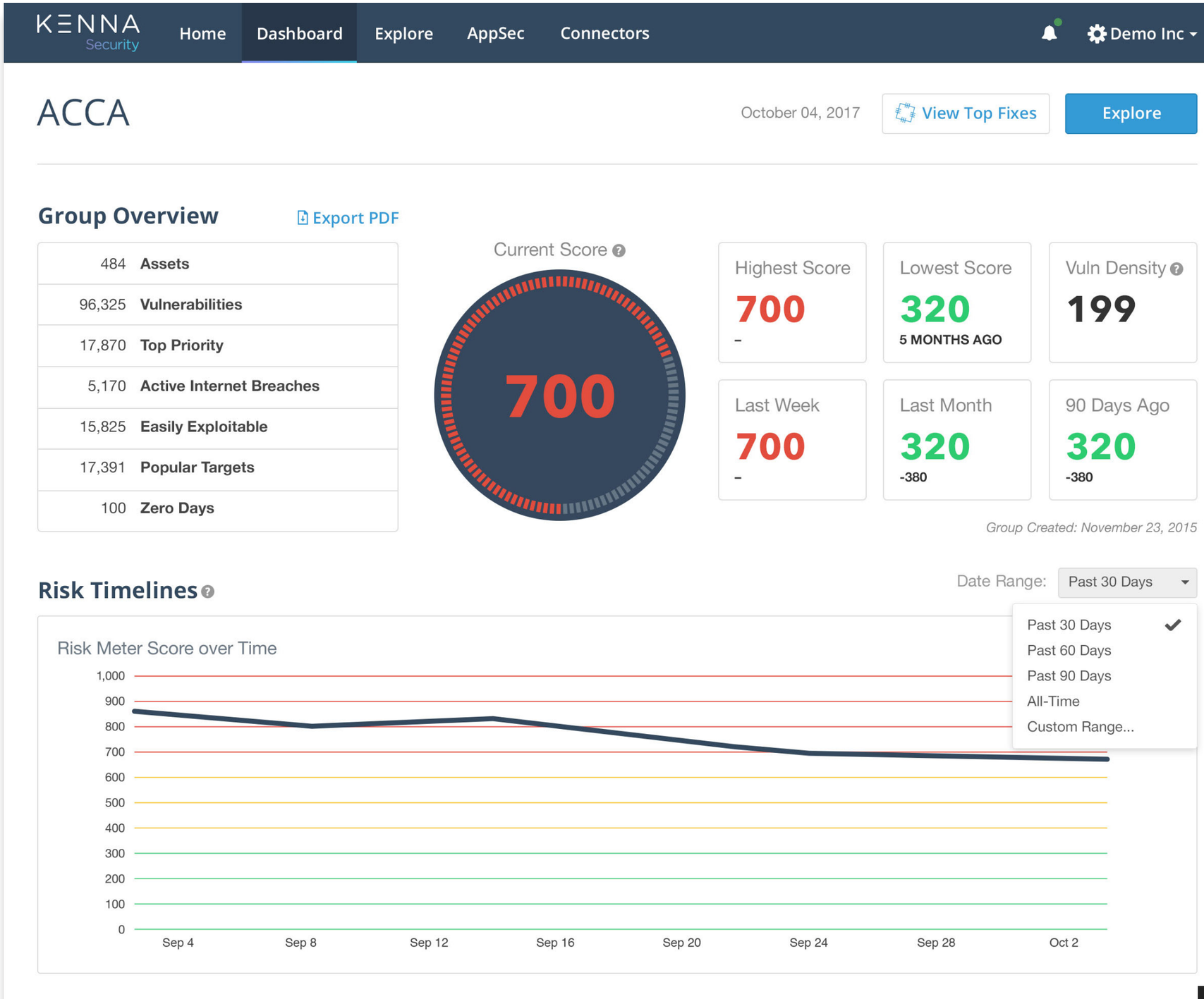
To send the remediation information to the right team, you can either send via email or download as a CSV. (If you have a ServiceNow connector configured, that is also an option for you to open tickets directly) Another approach would be to set up each system admin or business unit manager within Kenna and let them drive the remediation directly from the platform.



Report Trends

Finally, show management your great work.

Once you've synced, prioritized, patched, and synced again, you are ready to report on the progress. Choose "View Report" from the Dashboard for any Risk Meter – you'll see a collection of trending reports and KPIs specific to that group of assets.

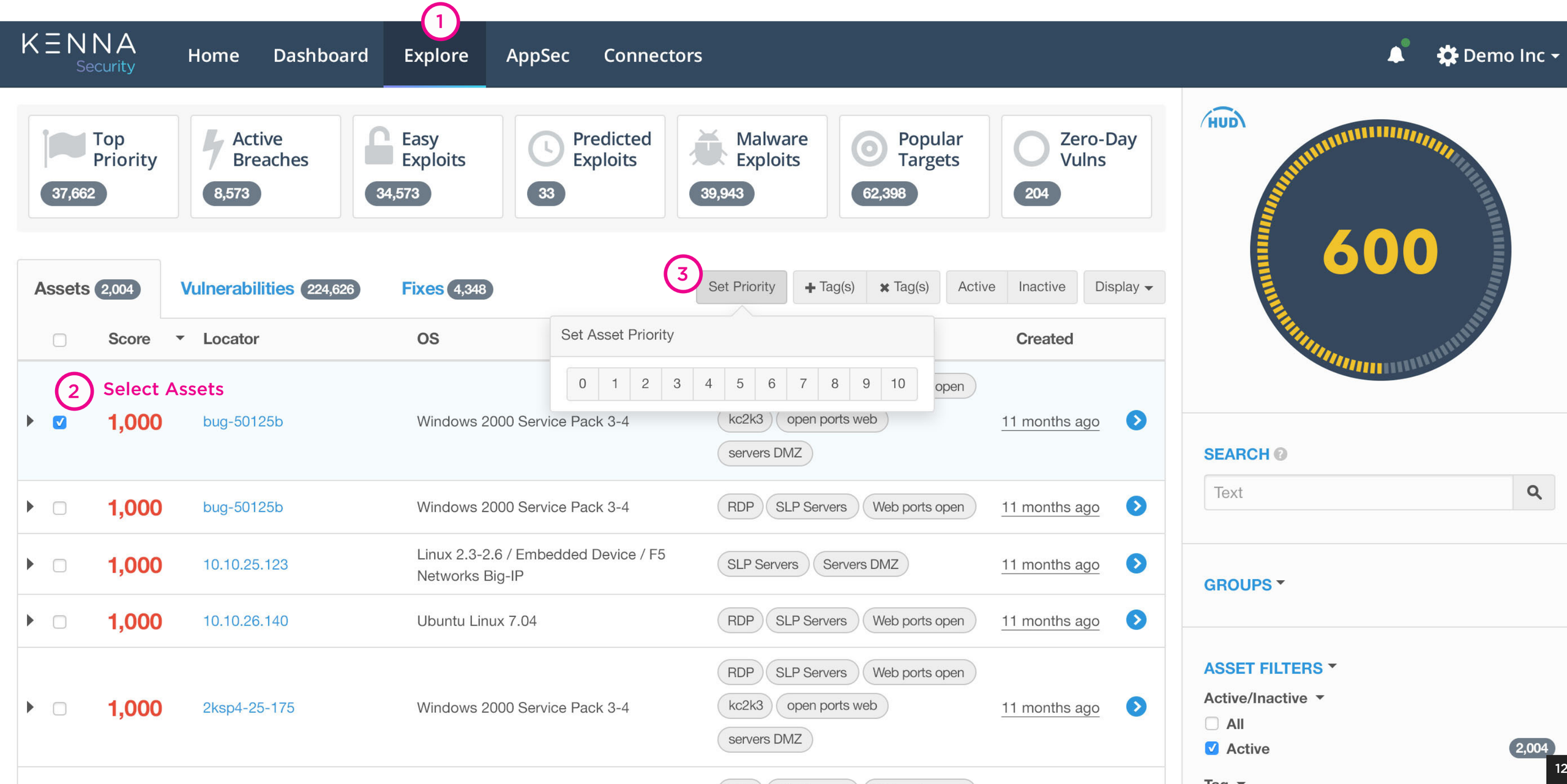


Test Plan

Asset Management

Prioritize assets based on environmental factors (asset criticality, mitigating / compensating controls)

Asset priority values are used in calculating overall asset risk scores (highest vulnerability risk * asset priority = asset risk score)

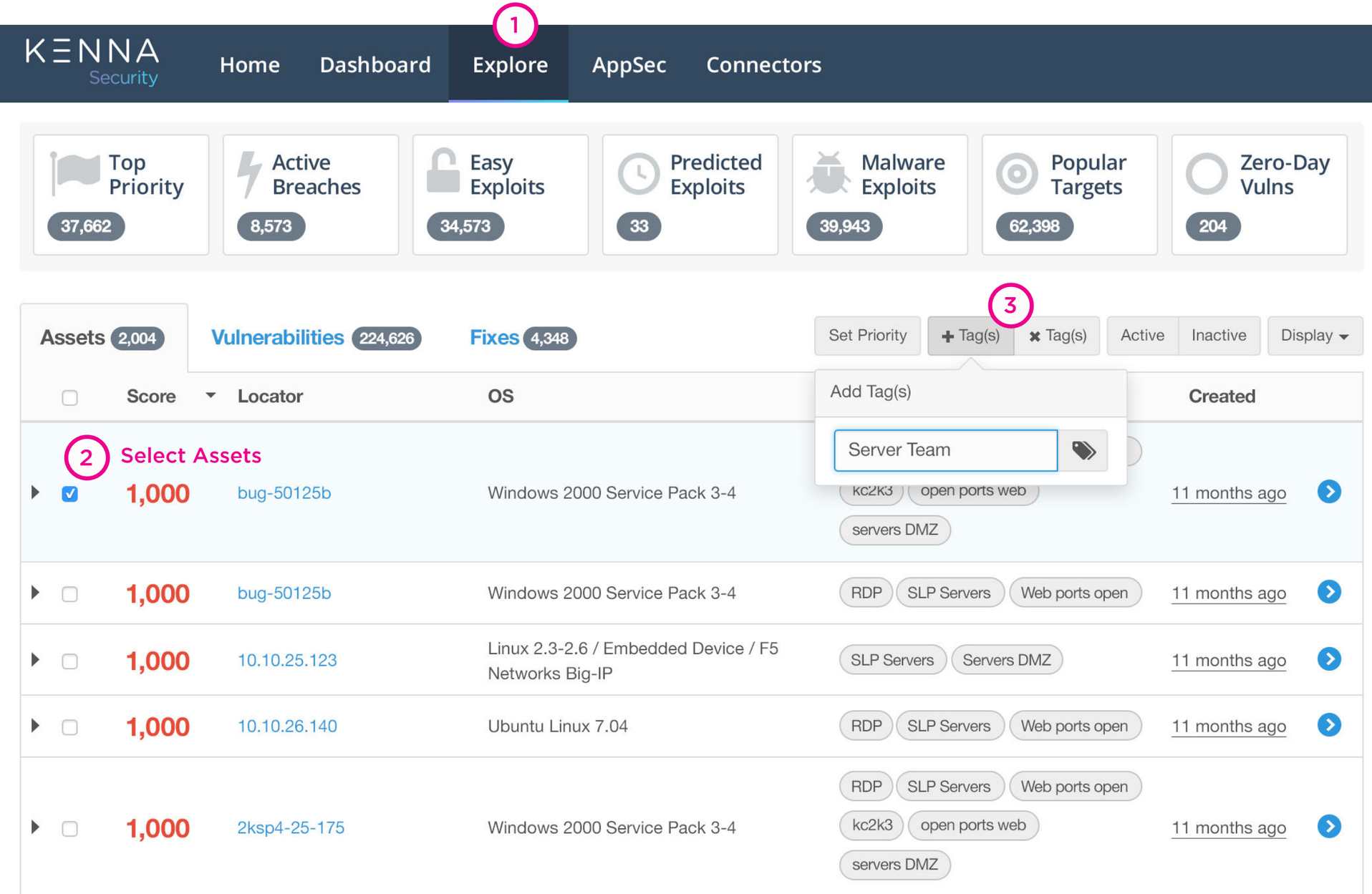


Tags

Organize assets by adding contextual tags (i.e. Asset Owner, Application, IT support organization)

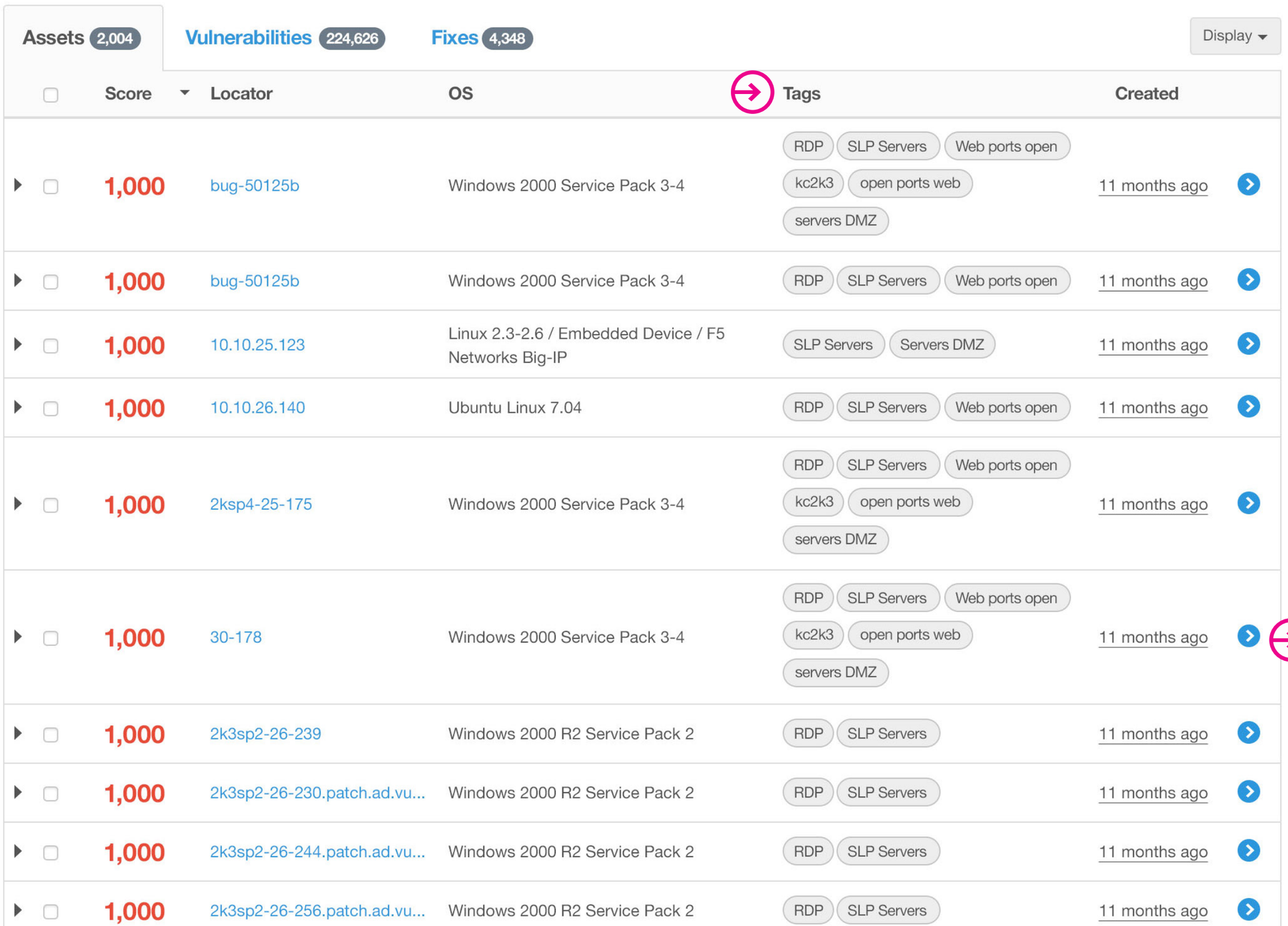
Asset tags from vulnerability scanners will persist in Kenna. (i.e. Qualys Assets groups and tags, Nexpose Site Names and tags, etc). Asset tags are searchable with elastic search and may be leveraged to create Kenna Risk Meter groups.

TEST: Tags to be added for testing: (unit), P1 vs P2, BISO, ITRL, region, IT support org, asset owner, platform technology



Tags

Tags are displayed in the asset view and in the navigation side bar on the right:

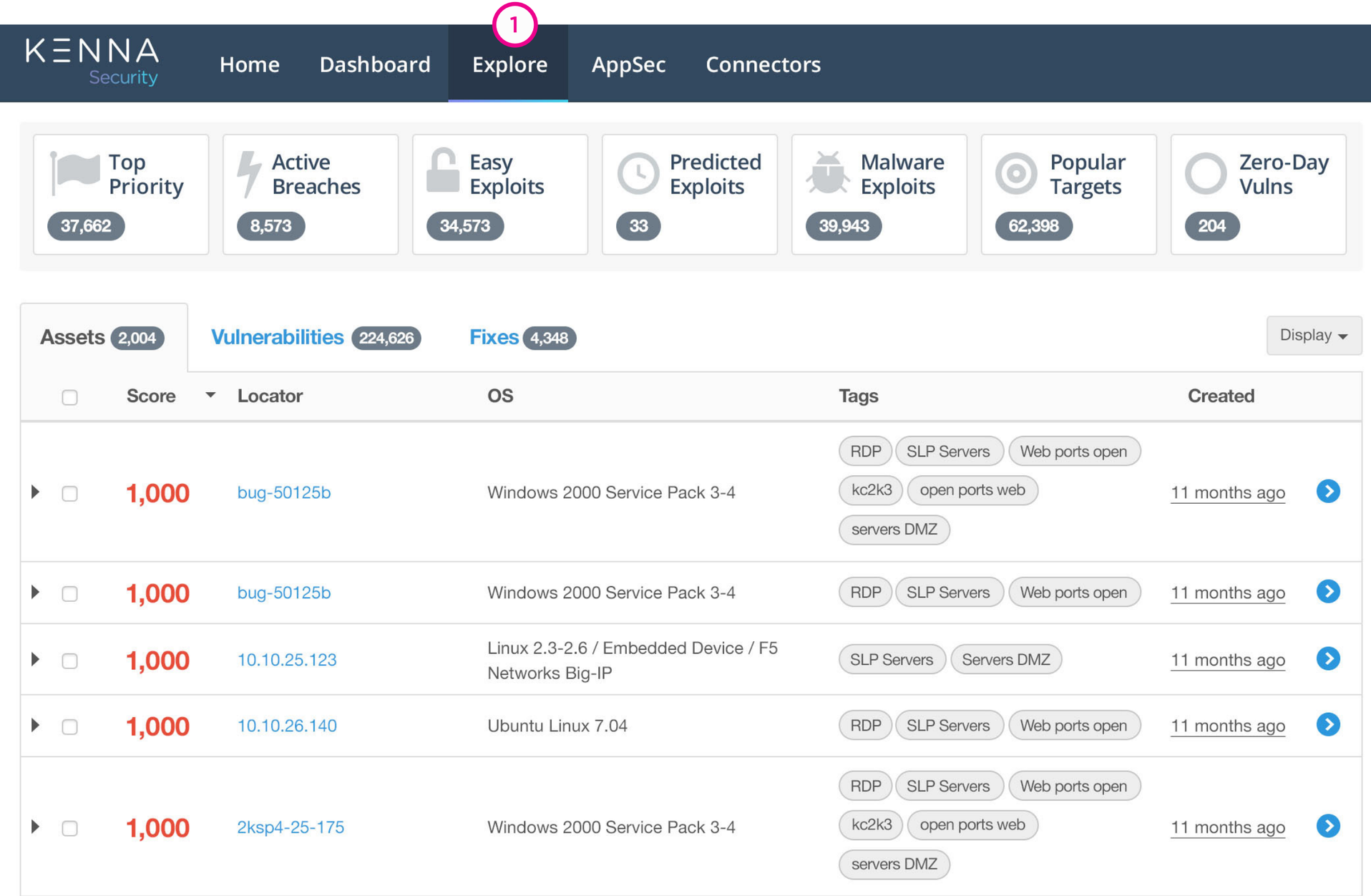


Risk Meter Creation

Organize, track, prioritize and report assets and vulnerabilities by business context

Risk meters may be grouped based on P1 vs P2 application, BISO, ITRL, device location (network segment), platform technology, etc

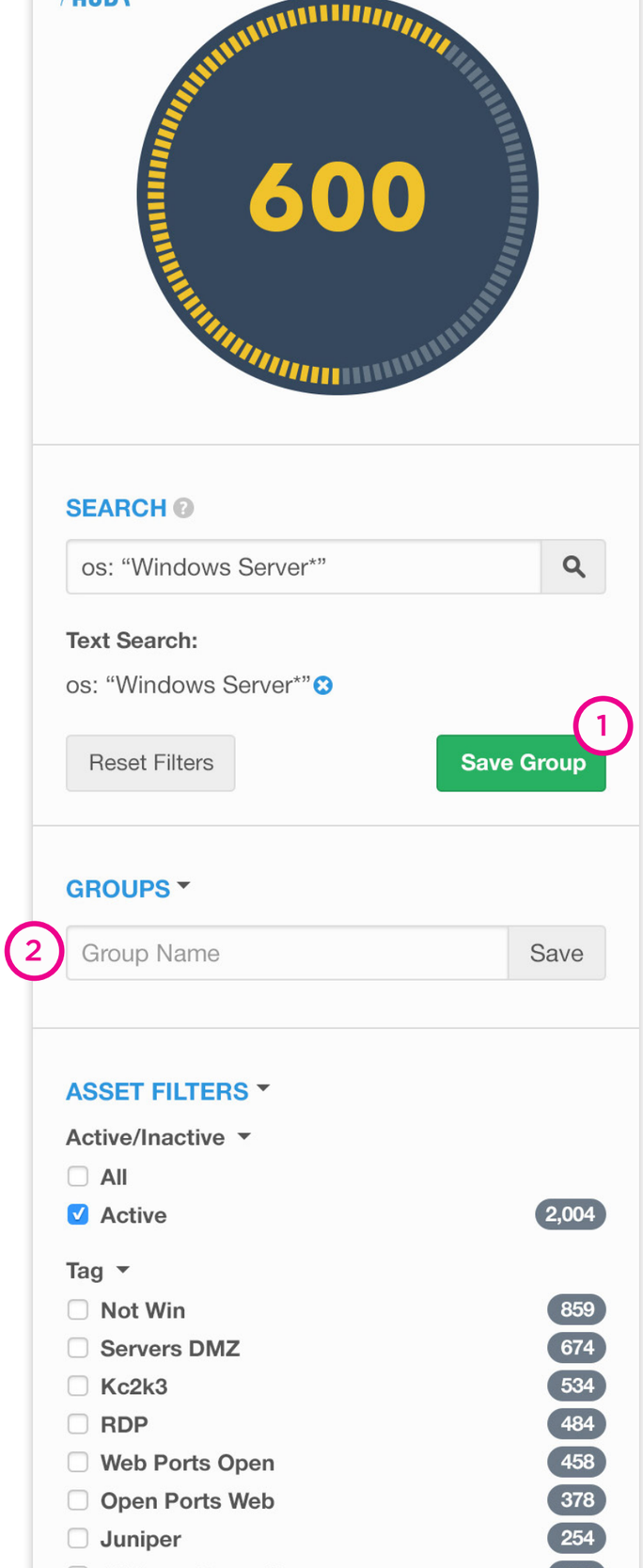
TEST: Create Risk Meter group based on Platform Operating System: Windows Servers:
1) Enter the following query in the search dialog box: **os:"Windows Server*"**



Risk Meter Creation

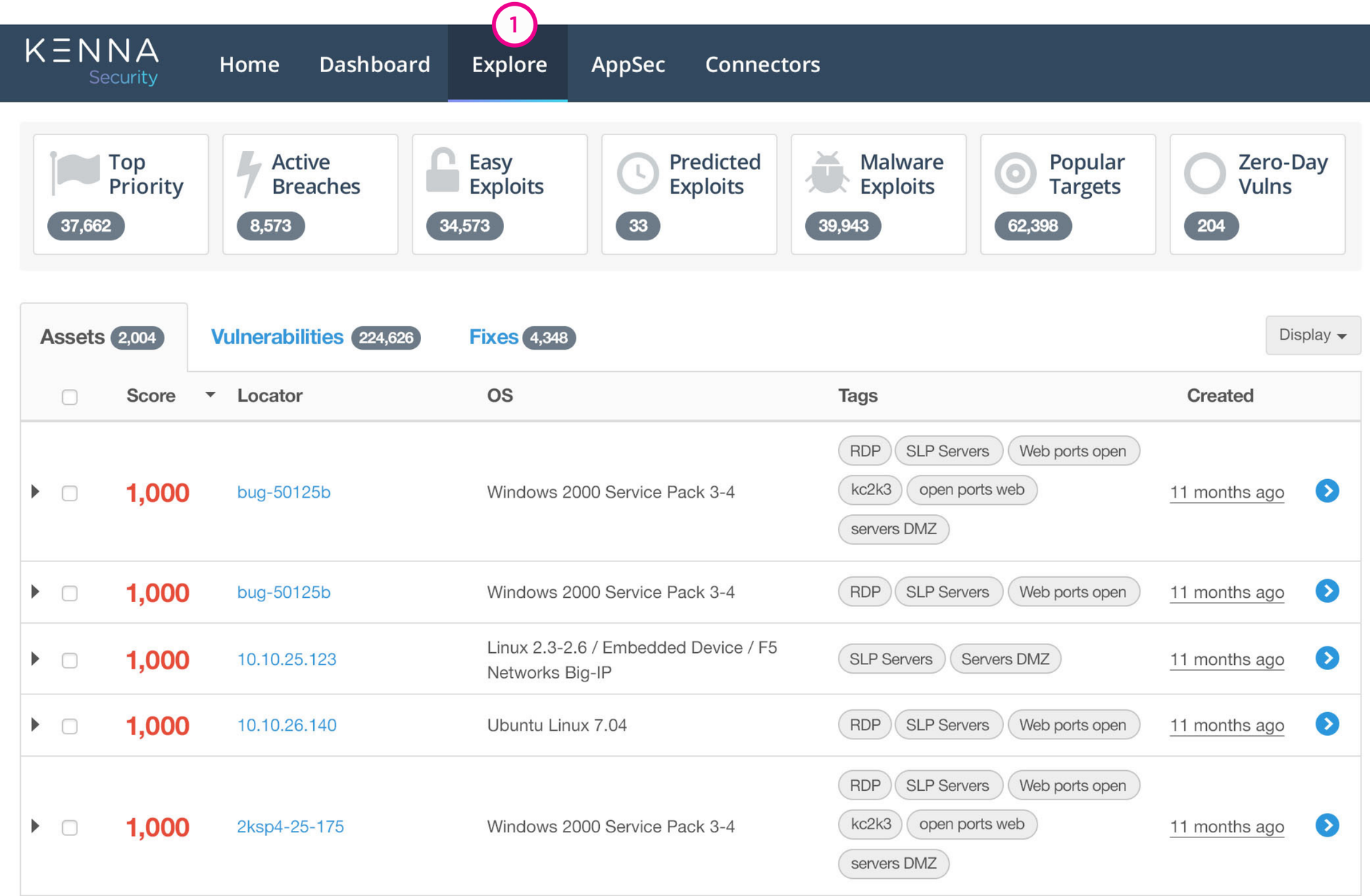
2) Save the Group and provide a name: **Windows Servers**

Provide Name & Save (2)



Risk Meter Creation

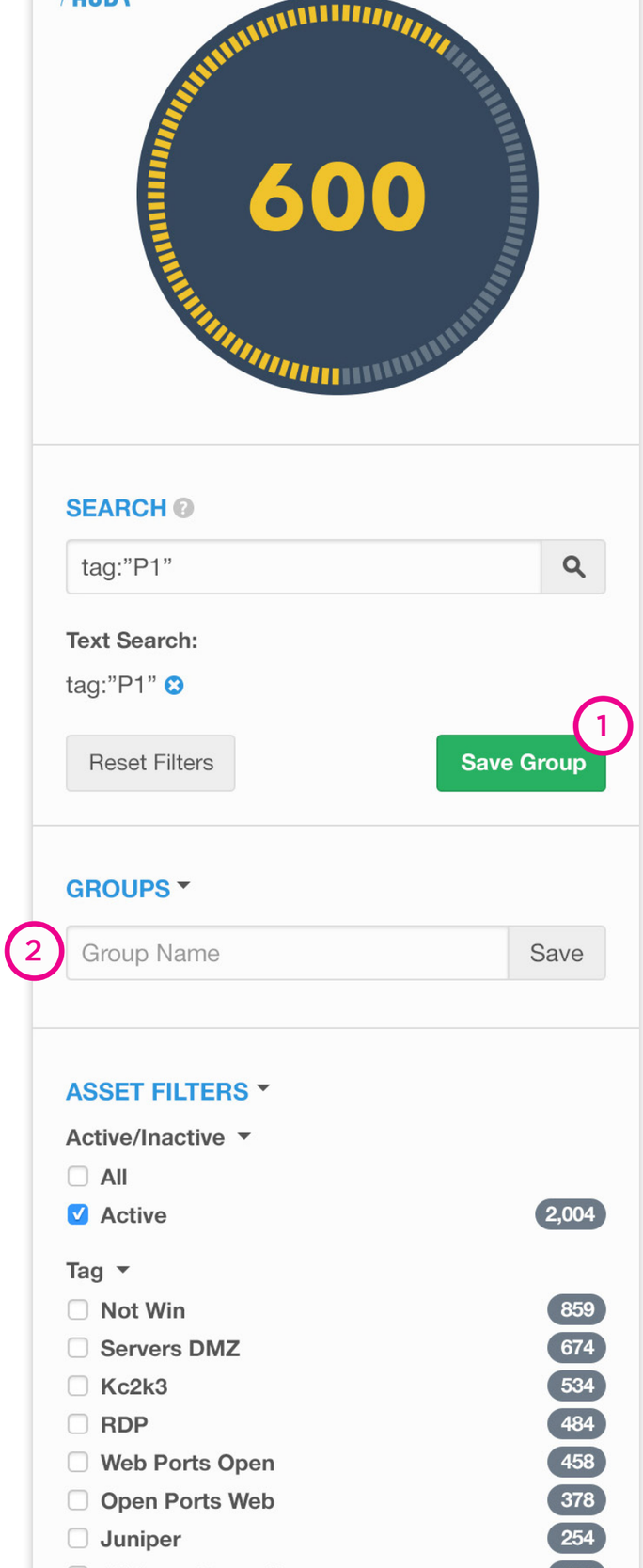
TEST: Create Risk Meter group based on P1 Applications:
1) Enter the following query in the search dialog box: **tag:”P1”**



Risk Meter Creation

2) Save the Group and provide a name: **P1 Application**

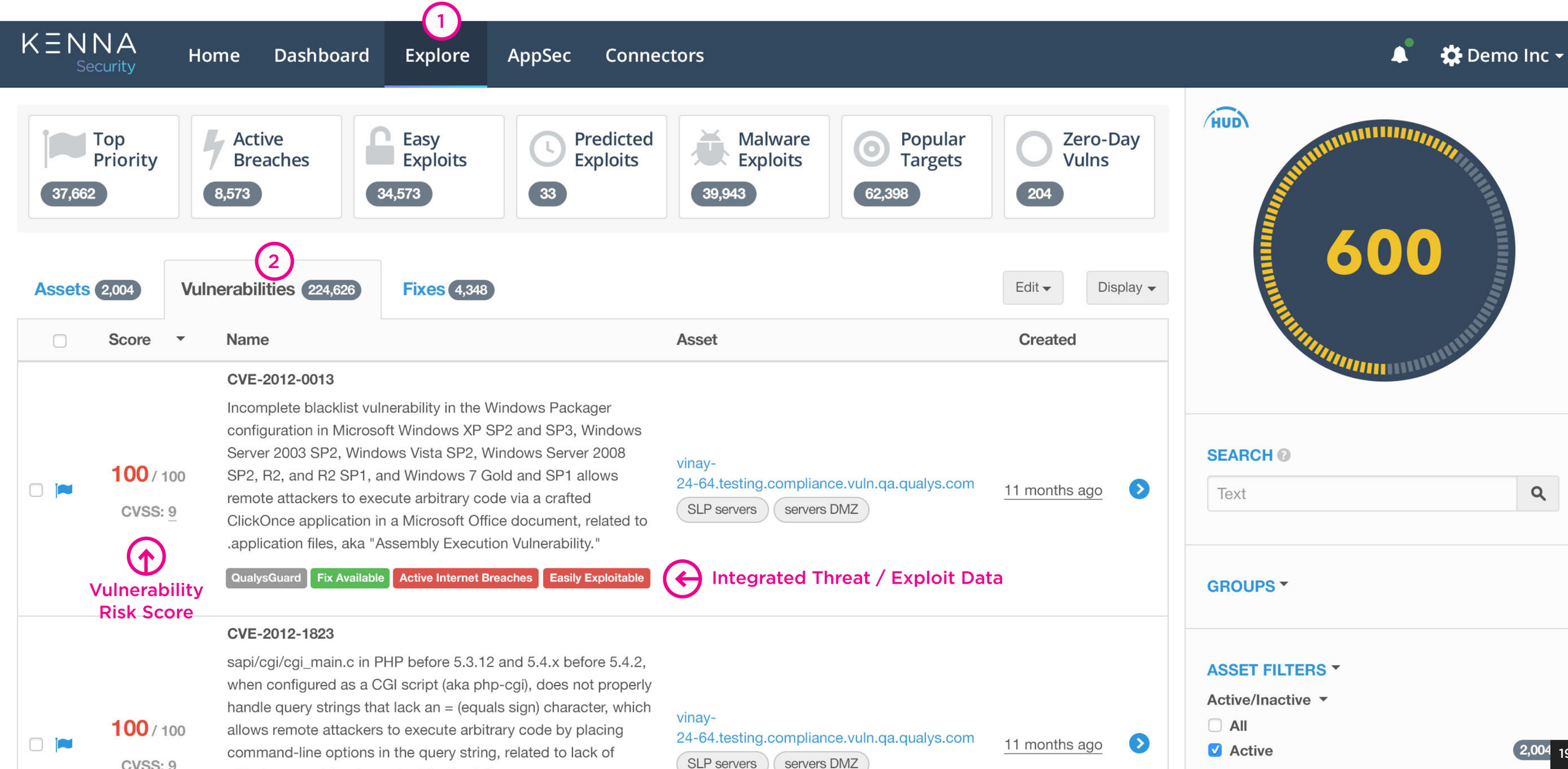
Provide Name & Save (2)



Vulnerability Management

Calculate vulnerability risk using integrated threat / exploit context

Vulnerability risk scores are calculated using data feeds from the NIST NVD, scanning vendor KBs, Dell CTU, AlientVault OTX, Metasploit, ExploitDB, Shodan, Exodus Security and many others. Please see the following link for a comprehensive list: **www.kennasecurity.com/partners**



Vulnerability Management

Threat / Exploit filters may be used to prioritize high risk vulnerabilities:

KENNA Security | Home | Dashboard | 1 Explore | AppSec | Connectors | Demo Inc

Top Priority 37,662 | Active Breaches 8,573 | Easy Exploits 34,573 | Predicted Exploits 33 | Malware Exploits 39,943 | Popular Targets 62,398 | Zero-Day Vulns 204

3 Apply Both Facets to view High Risk Vulnerabilities

2

Assets 2,004 | Vulnerabilities 224,626 | Fixes 4,348 | Edit | Display

Score	Name	Asset	Created
100 / 100 CVSS: 9	**CVE-2012-0013** Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability." QualysGuard Fix Available Active Internet Breaches Easily Exploitable	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago
100 / 100 CVSS: 9	**CVE-2012-1823** sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of	vinay-24-64.testing.compliance.vuln.qa.qualys.com SLP servers servers DMZ	11 months ago

HUD

600

SEARCH

Text

GROUPS

ASSET FILTERS

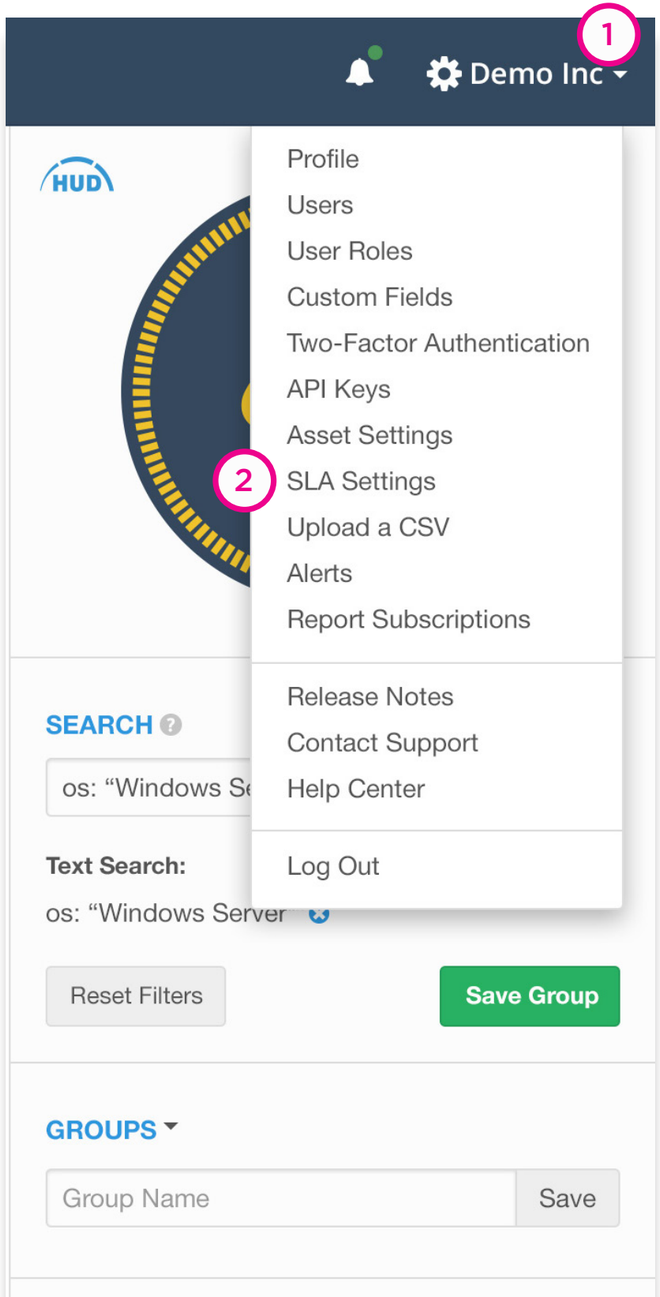
Active/Inactive

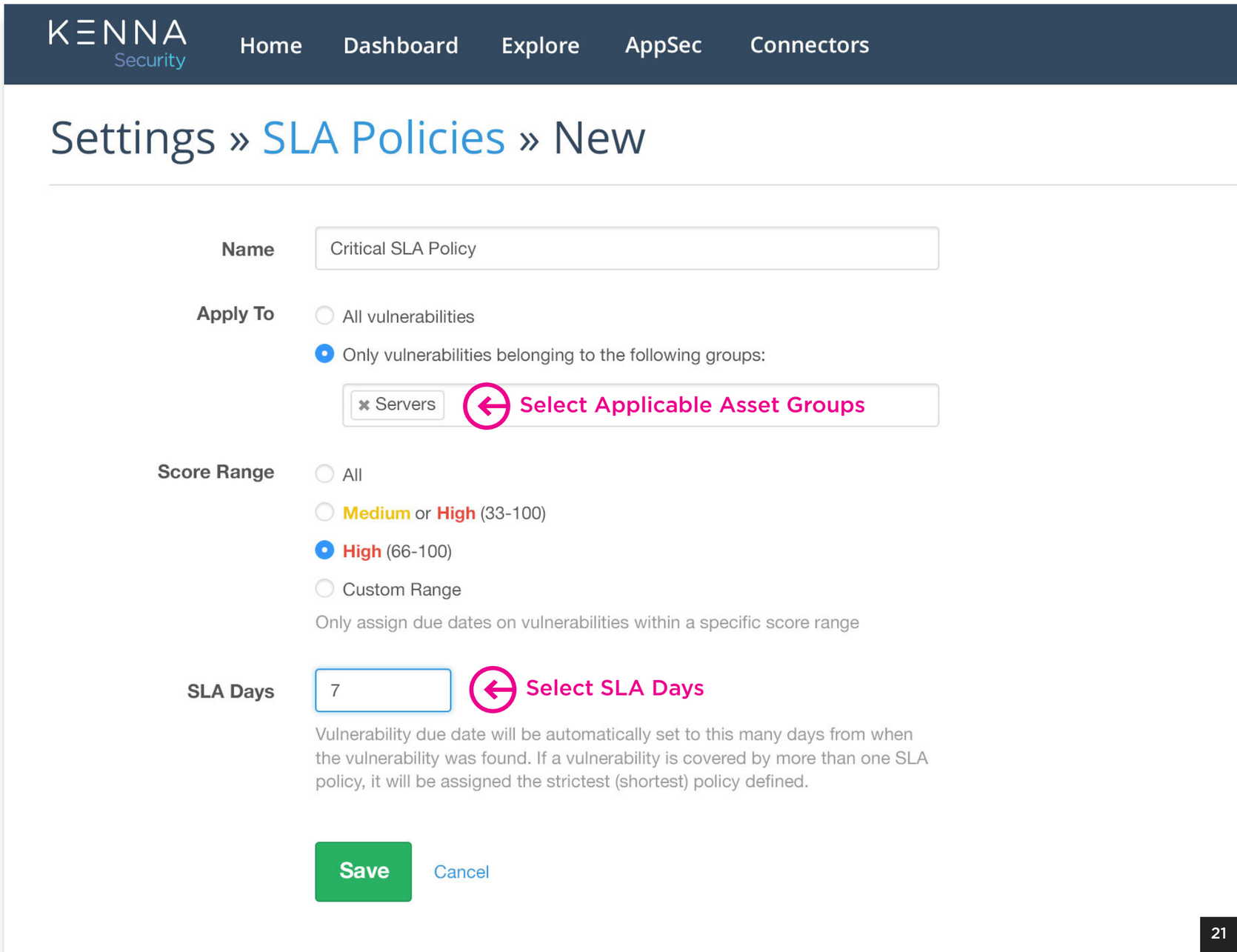
- [ ] All
- [x] Active 2,004

Manage & Track Vulnerability SLA Due Dates

Vulnerability due dates may be set automatically or manually defined in the UI.

TEST: Automate SLA due dates based on group and vulnerability severity.
Configure a new due date rule





Manage & Track Vulnerability SLA Due Dates

TEST: Manually set a SLA due date for a vulnerability

KENNA Security | Home | Dashboard | 1 Explore | AppSec | Connectors | Demo Inc

Top Priority 37,662 | Active Breaches 8,573 | Easy Exploits 34,573 | Predicted Exploits 33 | Malware Exploits 39,943 | Popular Targets 62,398 | Zero-Day Vulns 204

Assets 2,004 | 2 Vulnerabilities 224,626 | Fixes 4,348

Set Status | 4 Edit | ServiceNow incident | Display

	Score	Name	Asset
☑	100 / 100 CVSS: 9	**CVE-2012-0013** Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability." QualysGuard · Fix Available · Active Internet Breaches · Easily Exploitable	vinay-24-64.testing.compliance SLP servers servers DM ago
☑	100 / 100 CVSS: 9	**CVE-2012-1823** sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of	vinay-24-64.testing.compliance SLP servers servers DM ago

3 Select Vulnerabilities

4 Edit
- Internal Risk Rating
- Notification Date
- Notes
- Remediation Notes
- Development Team
- Project
- Person
- Priority
- 5 Due Date
- Risk Acceptance Justification
- Business Impact
- Reevaluation Date
- Risk Acc Criteria
- My SLA

HUD 600

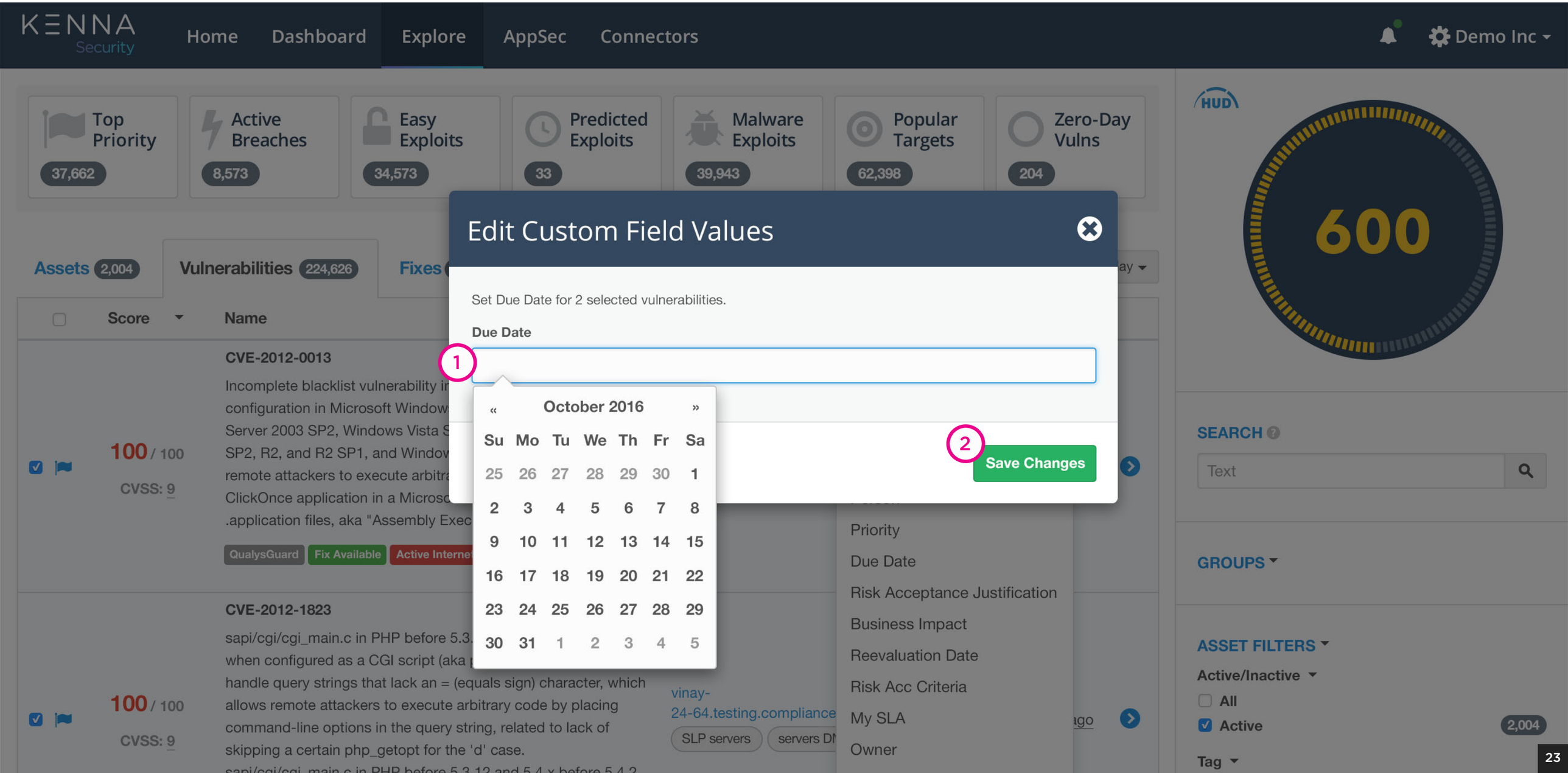
SEARCH
Text

GROUPS

ASSET FILTERS
Active/Inactive
- All
- Active 2,004

Manage & Track Vulnerability SLA Due Dates

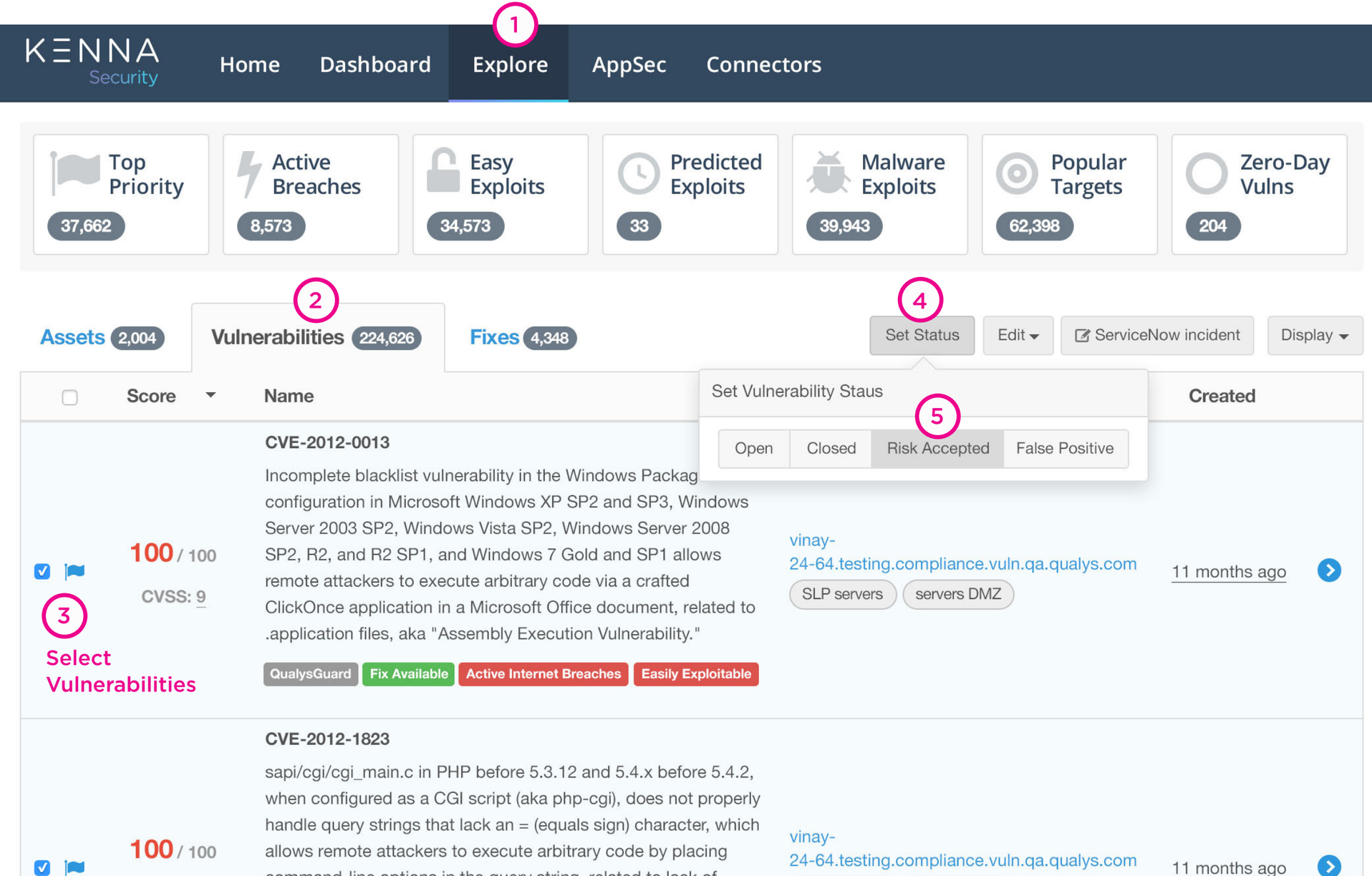
TEST: Select the due date



Track Risk Acceptance & Exceptions

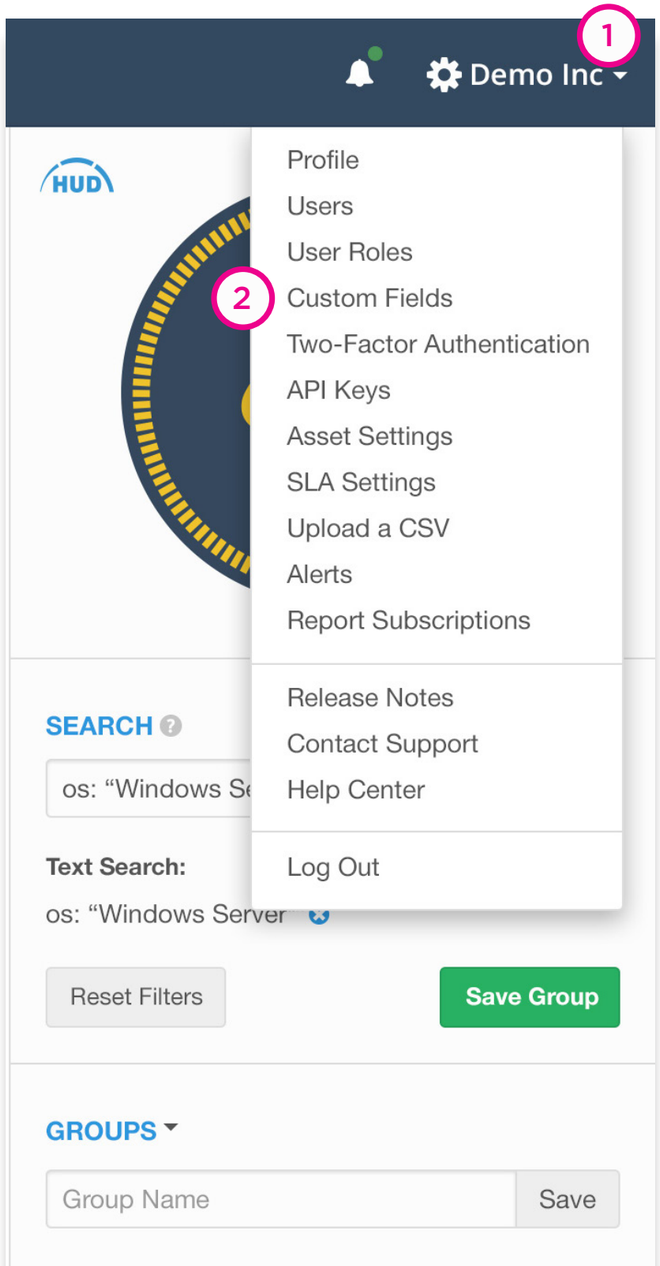
Vulnerabilities may be marked as “Risk Accepted” and custom fields (text, date, number) may be used to capture exception details.

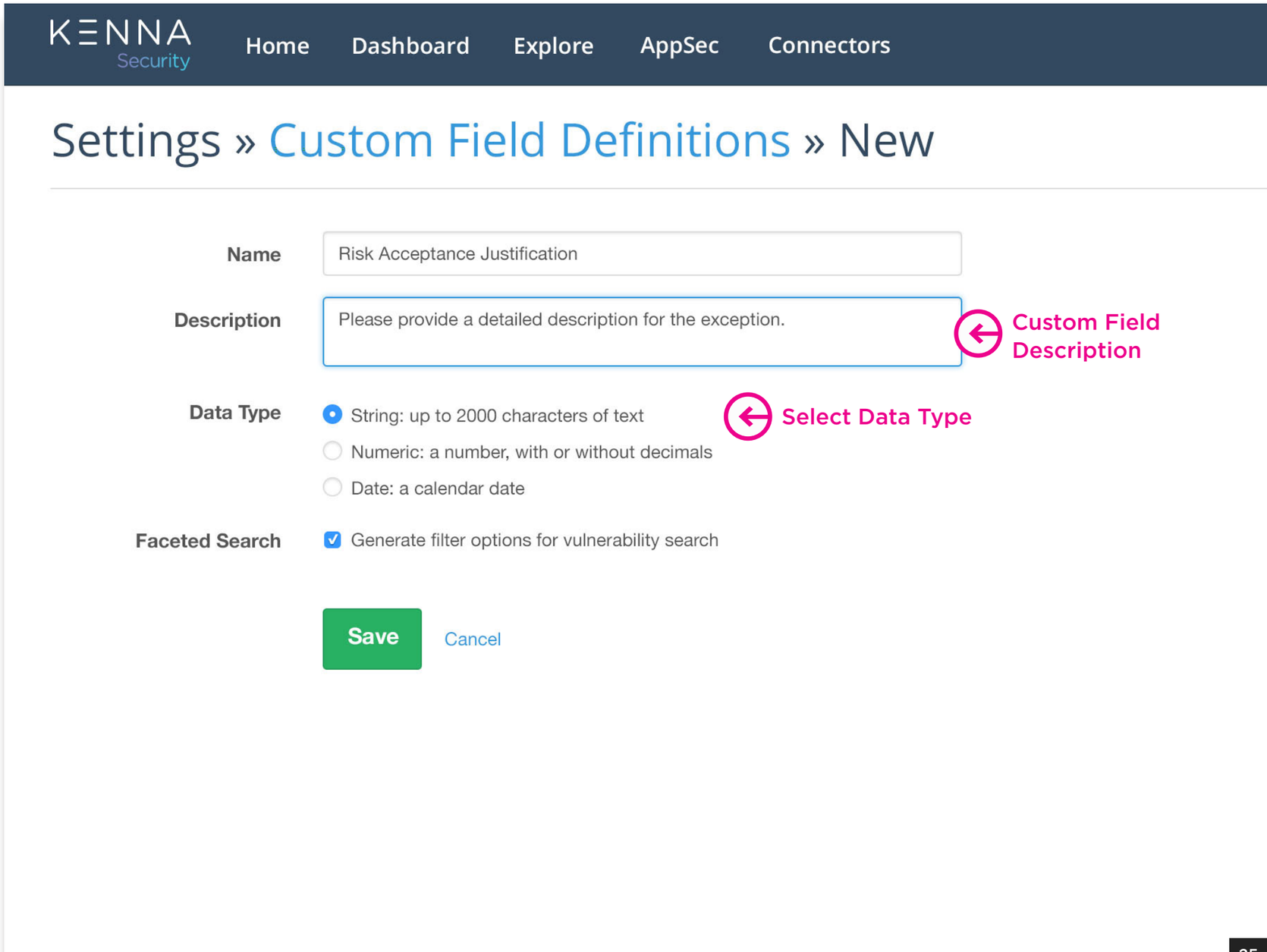
TEST: Mark vulnerabilities as Risk Accepted



Track Risk Acceptance & Exceptions

TEST: Create a custom field to capture Risk Acceptance justification





Track Risk Acceptance & Exceptions

TEST: Add Risk Acceptance justification details to vulnerability

KENNA Security | Home | Dashboard | 1 Explore | AppSec | Connectors | Demo Inc

Top Priority 37,662 | Active Breaches 8,573 | Easy Exploits 34,573 | Predicted Exploits 33 | Malware Exploits 39,943 | Popular Targets 62,398 | Zero-Day Vulns 204

2 Assets 2,004 | Vulnerabilities 224,626 | Fixes 4,348

Set Status | Edit | ServiceNow incident | Display

Score	Name	Asset
100 / 100 CVSS: 9	**CVE-2012-0013** Incomplete blacklist vulnerability in the Windows Packager configuration in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code via a crafted ClickOnce application in a Microsoft Office document, related to .application files, aka "Assembly Execution Vulnerability." QualysGuard Fix Available Active Internet Breaches Easily Exploitable	vinay-24-64.testing.compliance SLP servers servers DM ago
100 / 100 CVSS: 9	**CVE-2012-1823** sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.	vinay-24-64.testing.compliance SLP servers servers DM ago

3 Select Vulnerabilities

4

- Internal Risk Rating
- Notification Date
- Notes
- Remediation Notes
- Development Team
- Project
- Person
- Priority
- Due Date
- Risk Acceptance Justification
- Business Impact
- Reevaluation Date
- Risk Acc Criteria
- My SLA
- Owner

HUD 600

SEARCH

Text

GROUPS

ASSET FILTERS

Active/Inactive

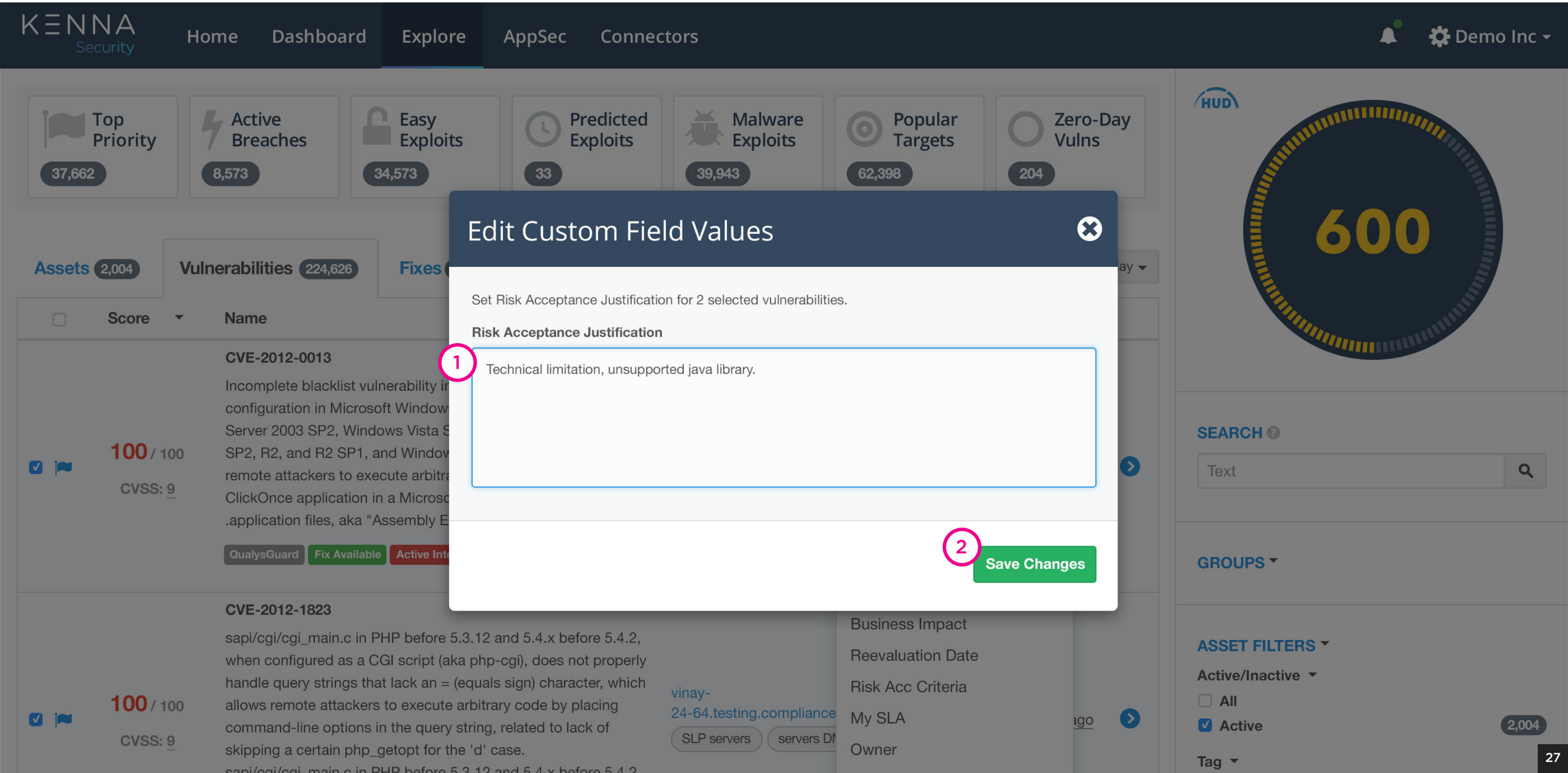
All

Active 2,004

Tag

Track Risk Acceptance & Exceptions

TEST: Add justification details

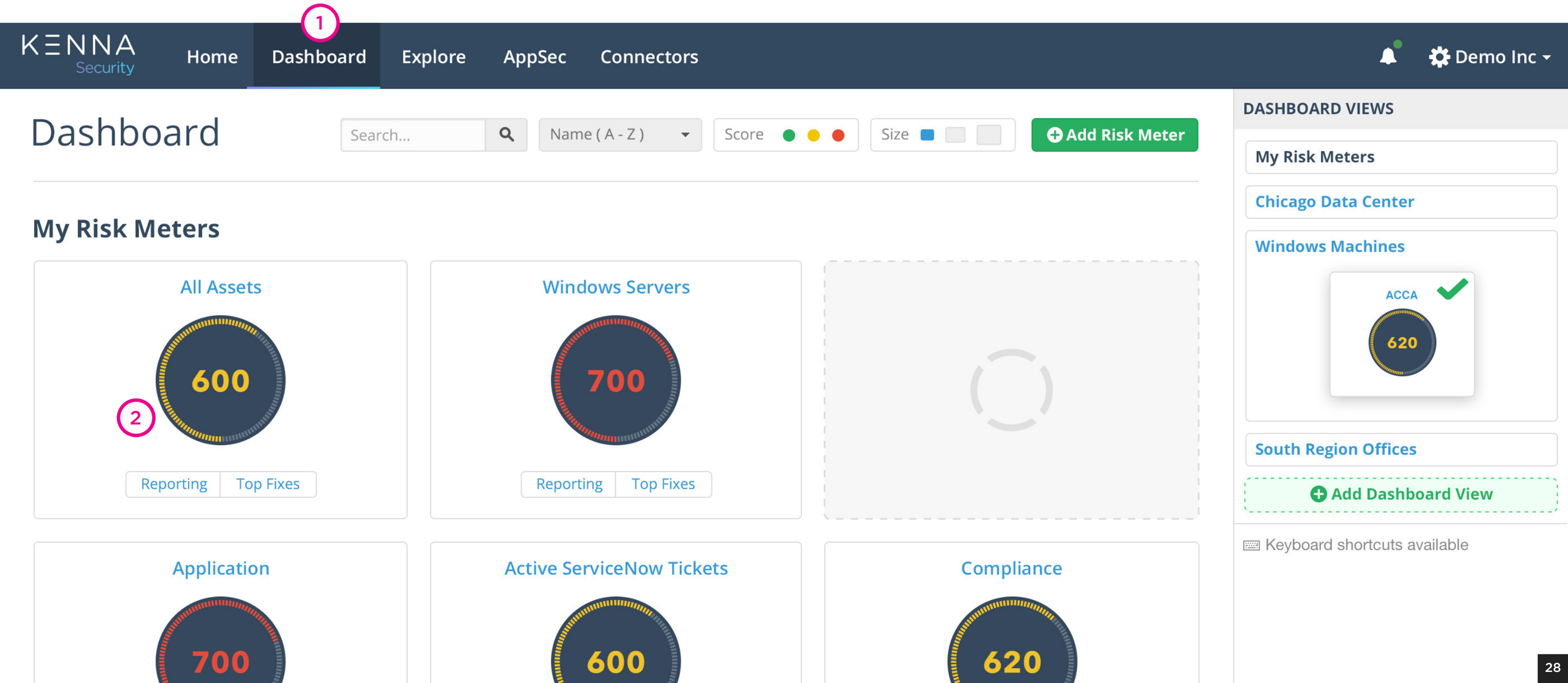


Automatically prioritize vulnerabilities & recommend fixes based on risk

Access the latest information around available patches and receive contextualized remediation for your asset groups (as well as overall assets). These suggestions can be prioritized and sorted to display key remediation insights such as the highest risk reduction, patches containing the most CVEs and the most assets affected. Fixes also responds to any filtering that happens on the dashboard, so you can filter based on remediations for vulnerabilities containing active internet breaches, or those that are easily exploitable.

You can also preview how much your risk score will be adjusted by applying the patch before actually deploying. This ensures that you are fixing the most critical vulnerabilities first.

TEST: Review patch / fix recommendations for a Risk Meter group



Automatically prioritize vulnerabilities & recommend fixes based on risk

KENNA Security | Home | Dashboard | Explore | AppSec | Connectors | Demo Inc

ACCA

October 04, 2017 | 3 View Top Fixes | Explore

Group Overview

Export PDF

484	**Assets**
96,325	**Vulnerabilities**
17,870	**Top Priority**
5,170	**Active Internet Breaches**
15,825	**Easily Exploitable**
17,391	**Popular Targets**
100	**Zero Days**

Current Score

700

Highest Score	Lowest Score	Vuln Density
700 –	320 5 MONTHS AGO	199

Last Week	Last Month	90 Days Ago
700 –	320 -380	320 -380

Group Created: November 23, 2015

Risk Timelines

Date Range: Past 30 Days

- Past 30 Days ✓
- Past 60 Days
- Past 90 Days
- All-Time
- Custom Range...

Risk Meter Score over Time

1,000
900
800
700

Automatically prioritize vulnerabilities & recommend fixes based on risk

KENNA Security | Home | Dashboard | Explore | AppSec | Connectors | Demo Inc

ACCA

View Report | Explore

700

Top Fix Groups

Risk Reduction Scores

700 → 665 | 700 → 670 | 700 → 670 | 700 → 680 | 700 → 685

Group 1: Risk Score Reduction of 35, 1 Fix

ServiceNow incident | Send via email | Send via CSV

Microsoft SMB Remote Code Execution Vulnerability (MS09-001)

1011 Vulns Affected Across All Data

Vulnerability Rollup

Diagnosis | Consequence | Solution | CVEs Addressed 3 | Assets Affected 223

Assets Requiring Patch/Fix

Vendor Security Advisory

Workaround:
TCP ports 139 and 445 should be blocked at the firewall to protect systems behind the firewall from attempts to exploit this vulnerability.
Impact of workaround: Blocking the ports can cause several windows services or applications using those ports to stop functioning.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

MS09-001: Microsoft Windows 2000 Service Pack 4

MS09-001: Windows XP Service Pack 2 and Windows XP Service Pack 3

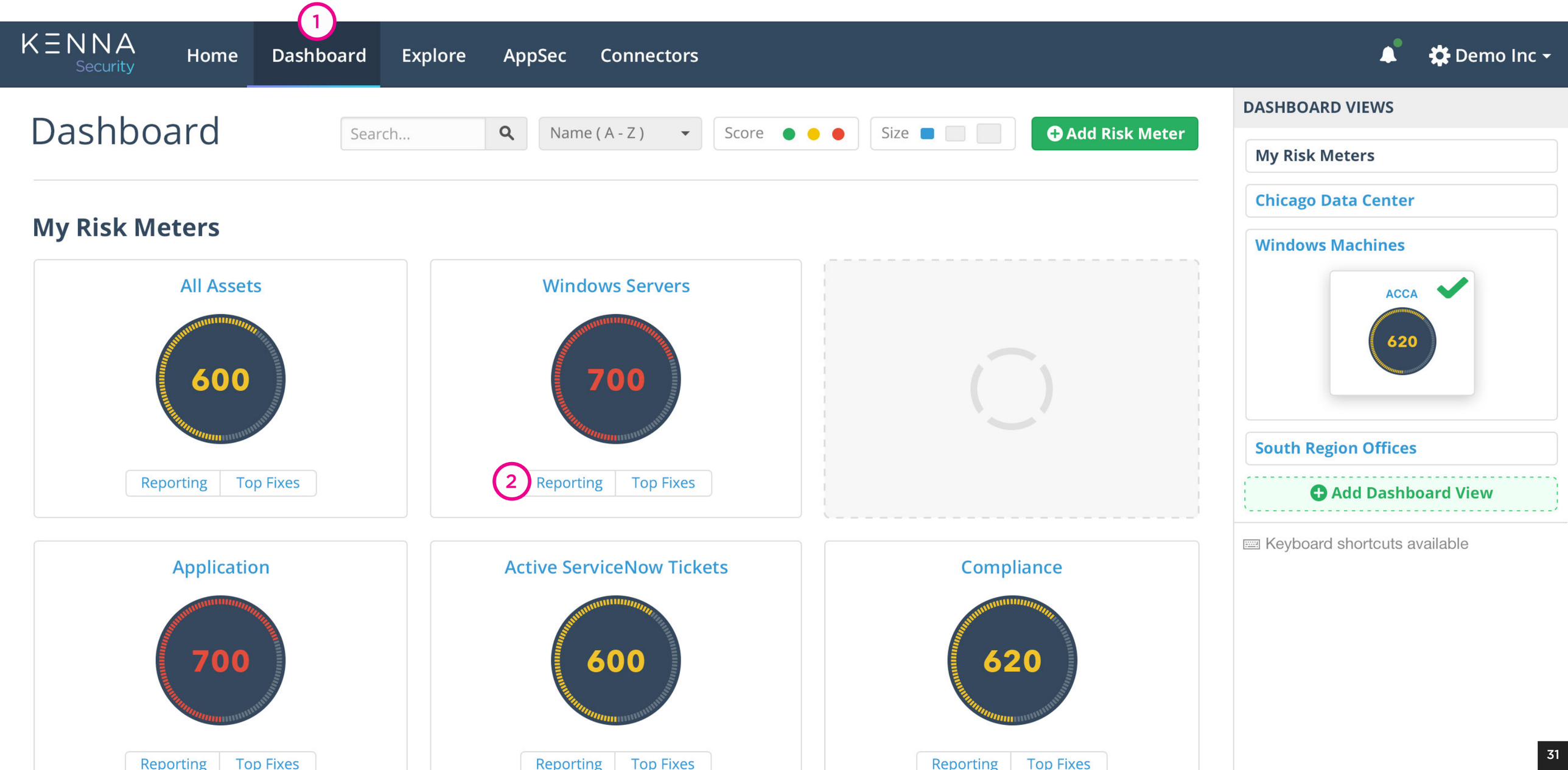
MS09-001: Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

MS09-001: Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Reporting

Track / report vulnerability and asset risk scores over time

Detailed security metric and historical trending reports are available for each Risk Meter on the **Dashboard** page.



Reporting

Risk Meter group summary and score over time are tracked with historical trend.

Group Overview

Export PDF

484	**Assets**
96,325	**Vulnerabilities**
17,870	**Top Priority**
5,170	**Active Internet Breaches**
15,825	**Easily Exploitable**
17,391	**Popular Targets**
100	**Zero Days**

Current Score

Highest Score	Lowest Score	Vuln Density
700	320	199
–	5 MONTHS AGO	
Last Week	**Last Month**	**90 Days Ago**
700	320	320
–	-380	-380

Group Created: November 23, 2015

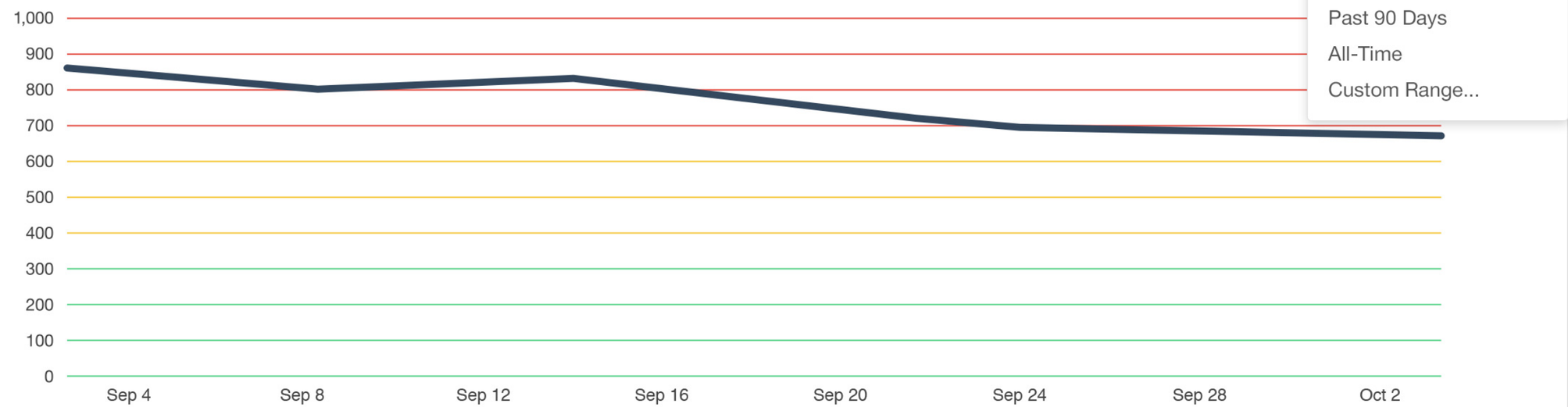
Risk Timelines

Select Desired Date Range (2)

Date Range: Past 30 Days

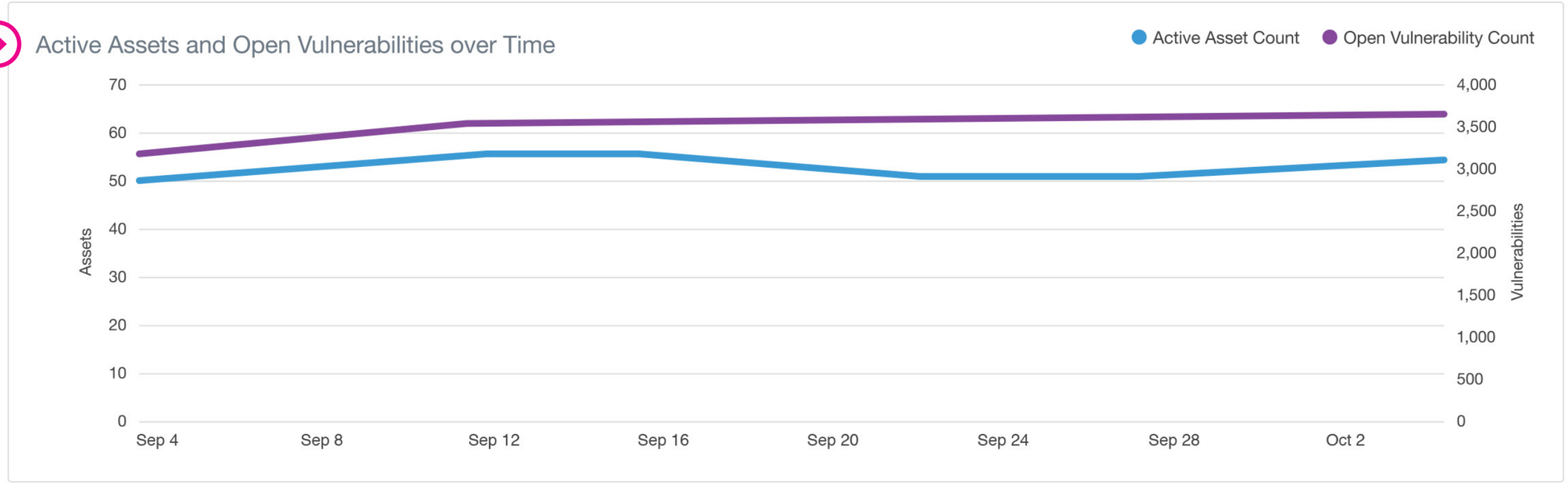
- Past 30 Days ✓
- Past 60 Days
- Past 90 Days
- All-Time
- Custom Range...

(1) Risk Meter Score over Time



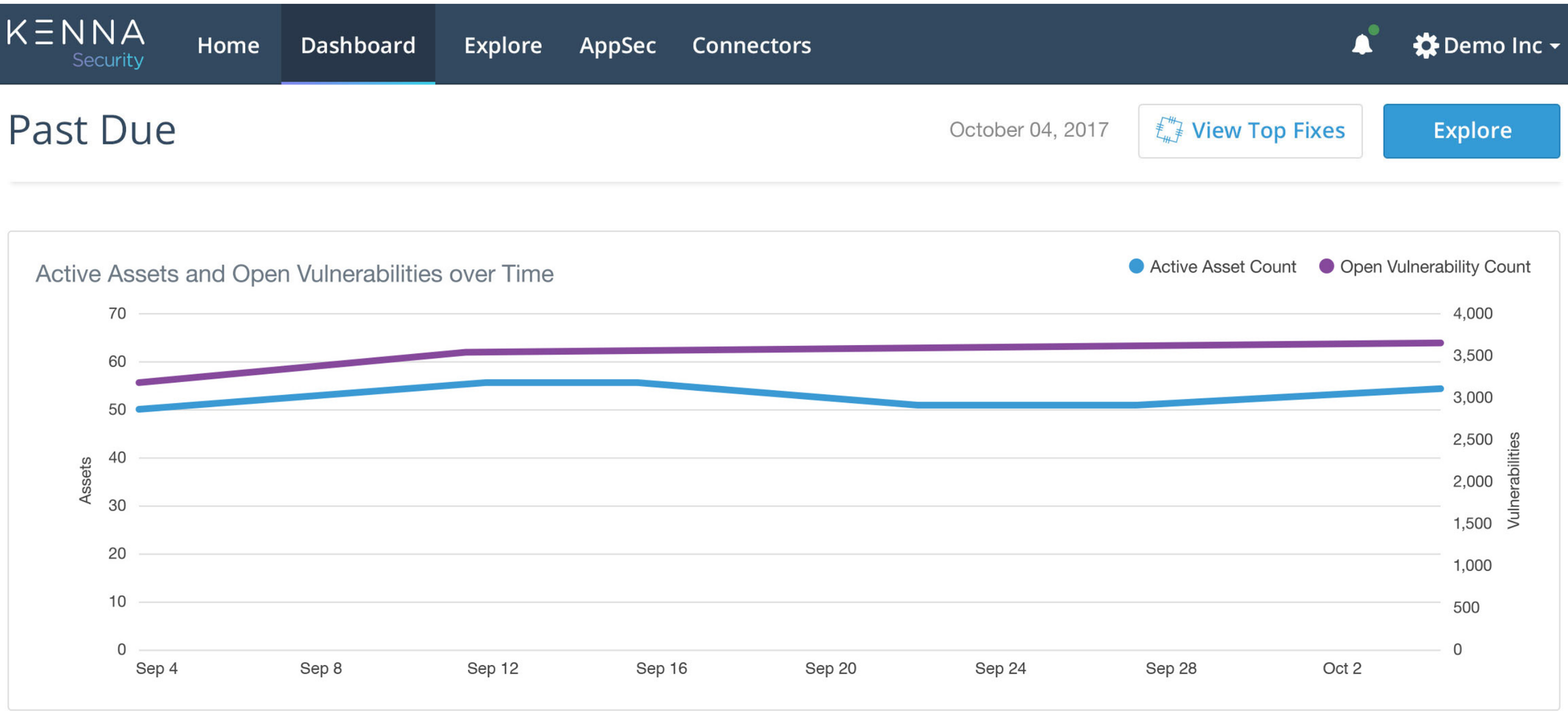
Reporting

Asset and Vulnerability Counts are also tracked over time.



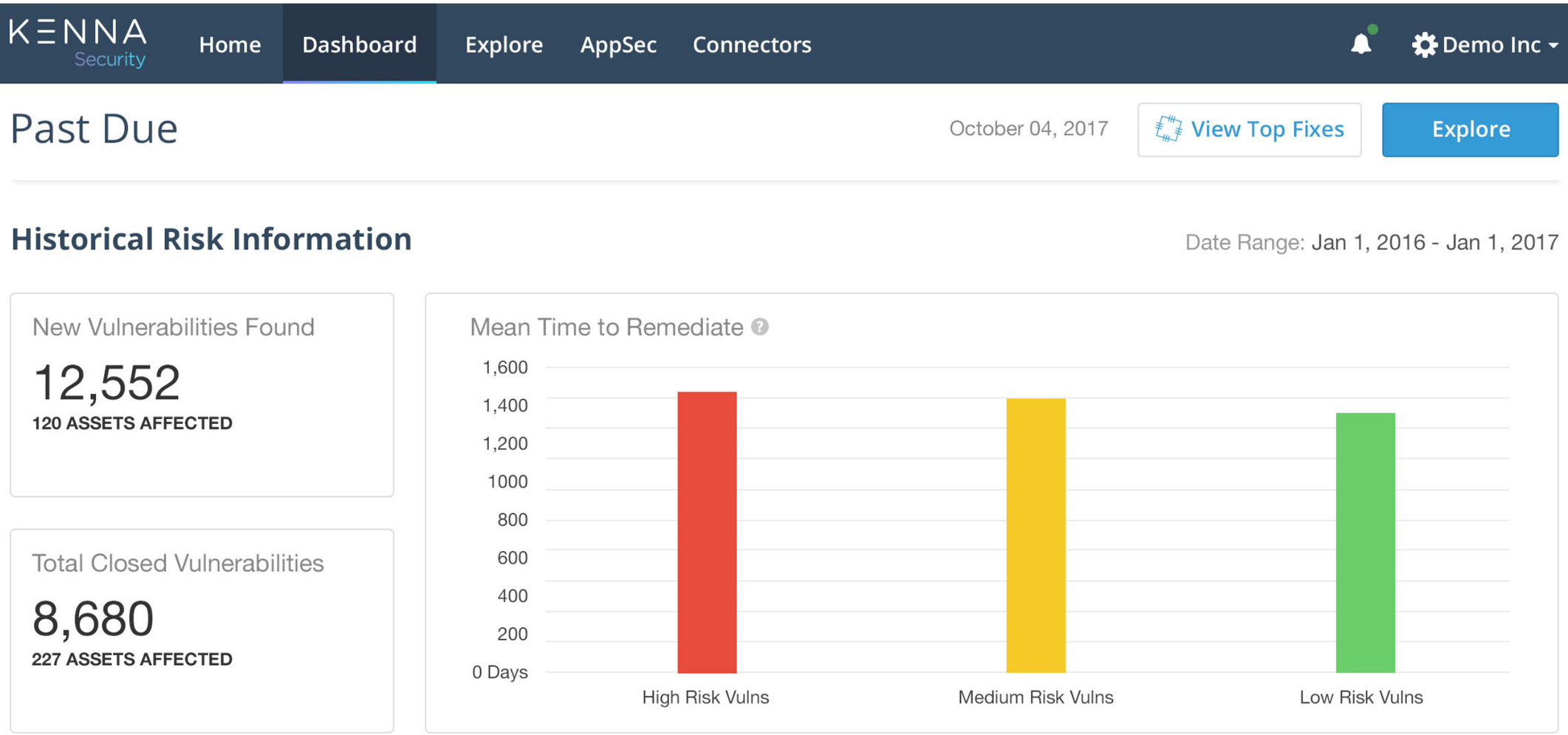
Track / report SLA, vulnerability age, over due

Vulnerability Reports may be based on SLA dates or vulnerability age and tracked over time. The sample report below shows all overdue vulnerabilities based on the following query: **due_date:<now**



Track / report remediation effectiveness: new vulnerabilities detected, closed vulnerabilities, mean time to remediate:

Kenna will track when vulnerabilities are first detected in the environment and when vulnerabilities are closed.
These dates are used to track mean time to remediate.



Export reports to PDF

Group Overview

Export PDF

484	**Assets**
96,325	**Vulnerabilities**
17,870	**Top Priority**
5,170	**Active Internet Breaches**
15,825	**Easily Exploitable**
17,391	**Popular Targets**
100	**Zero Days**

Current Score

700

Highest Score	Lowest Score	Vuln Density
700	320	199
–	5 MONTHS AGO	
Last Week	Last Month	90 Days Ago
700	320	320
–	-380	-380

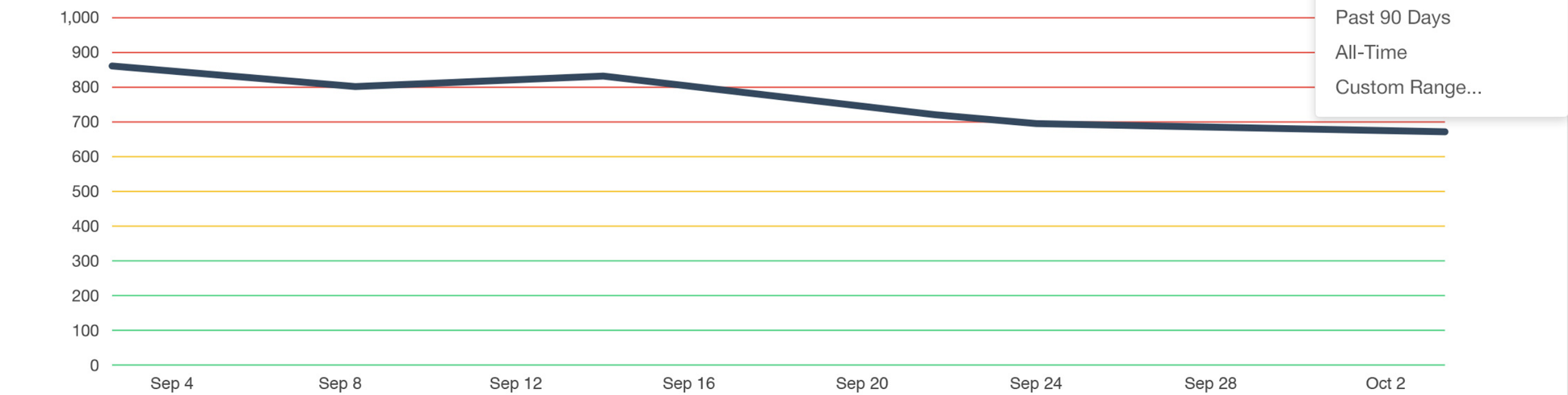
Group Created: November 23, 2015

Risk Timelines

Date Range: Past 30 Days

- Past 30 Days ✔
- Past 60 Days
- Past 90 Days
- All-Time
- Custom Range...

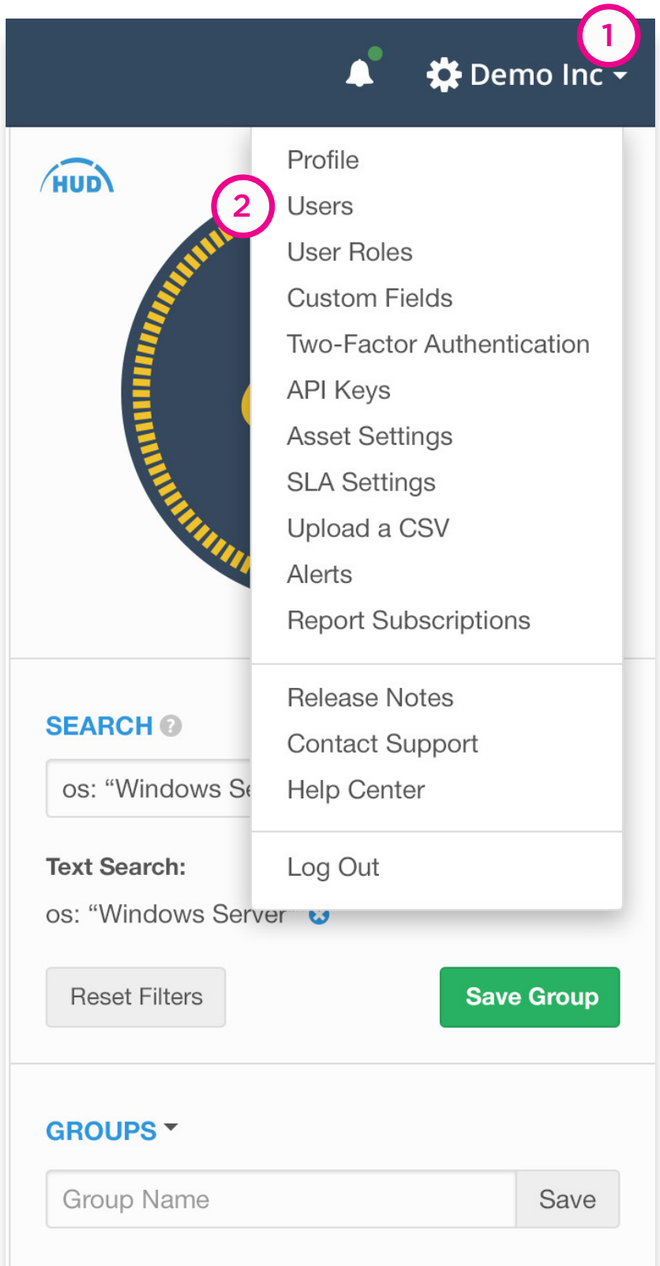
Risk Meter Score over Time

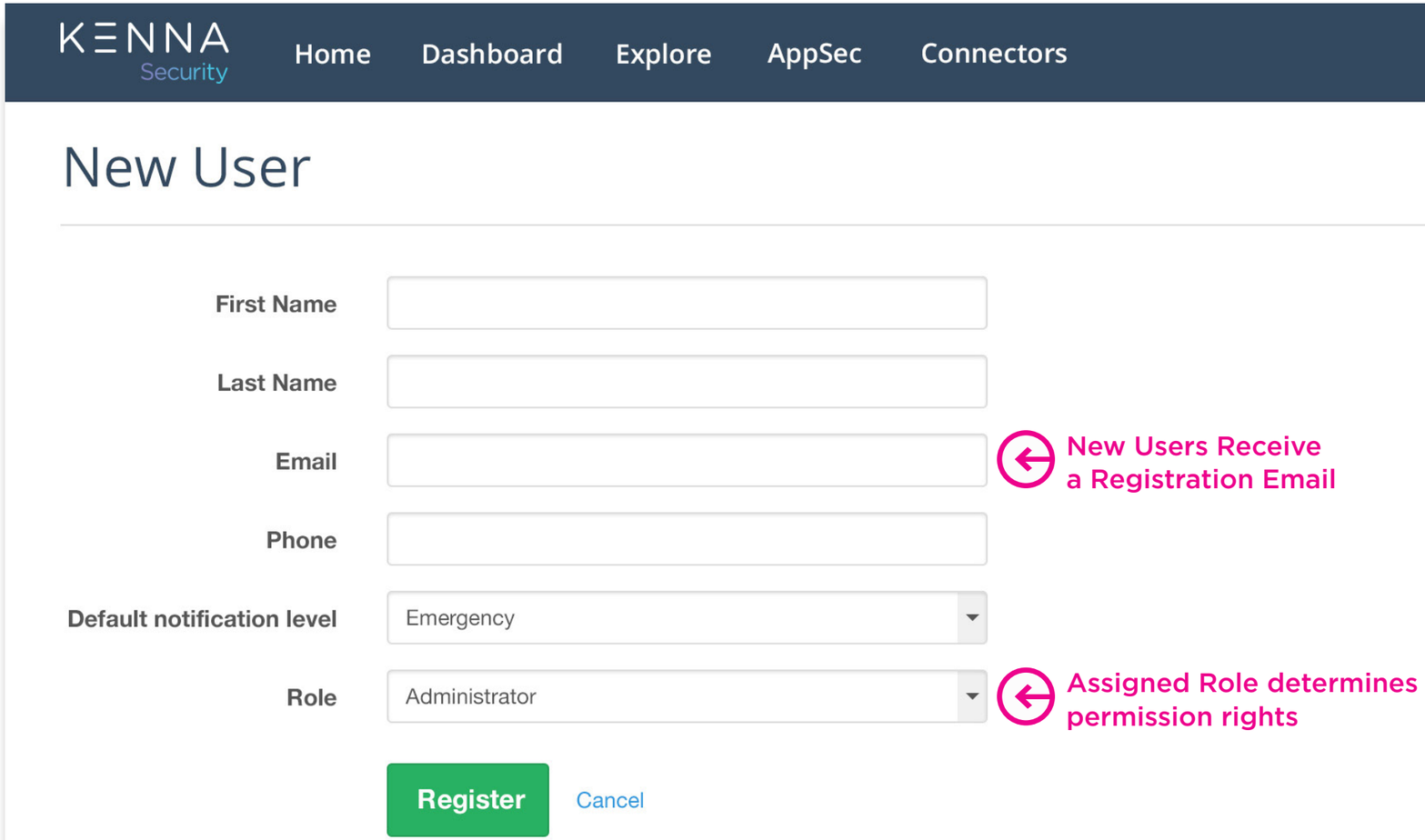


Access Control

Create / manage user access to Kenna platform:

Additional users may be added to the platform using the settings console.

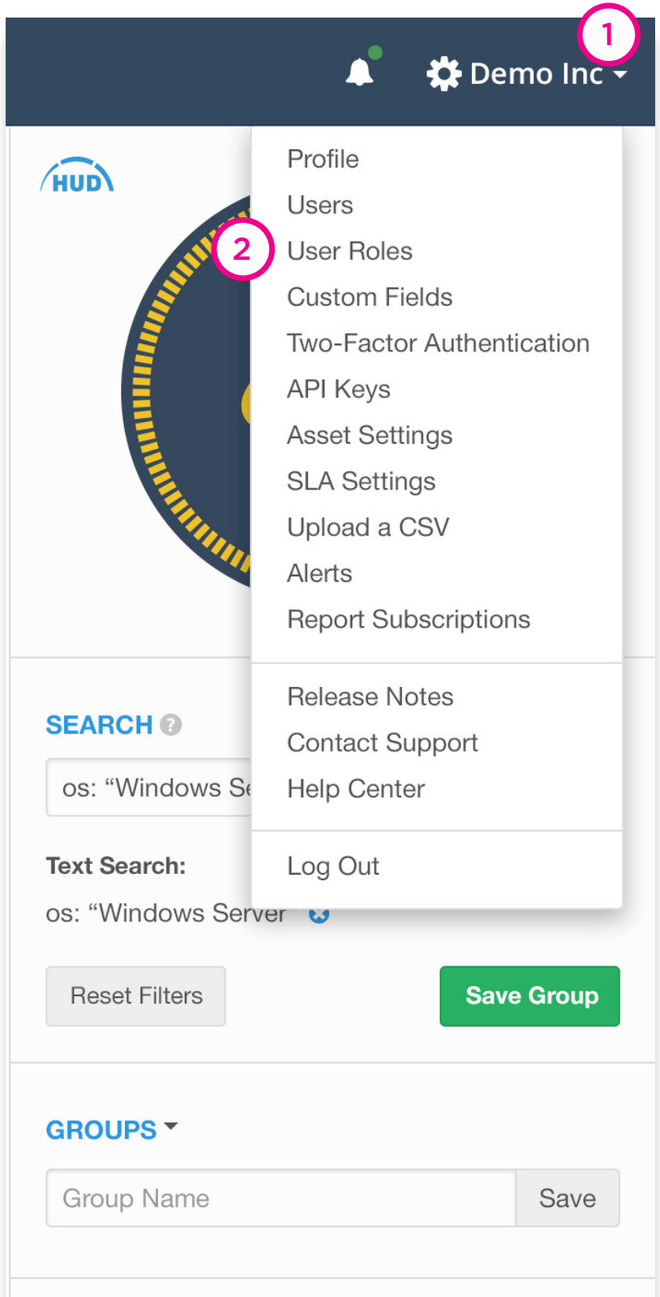


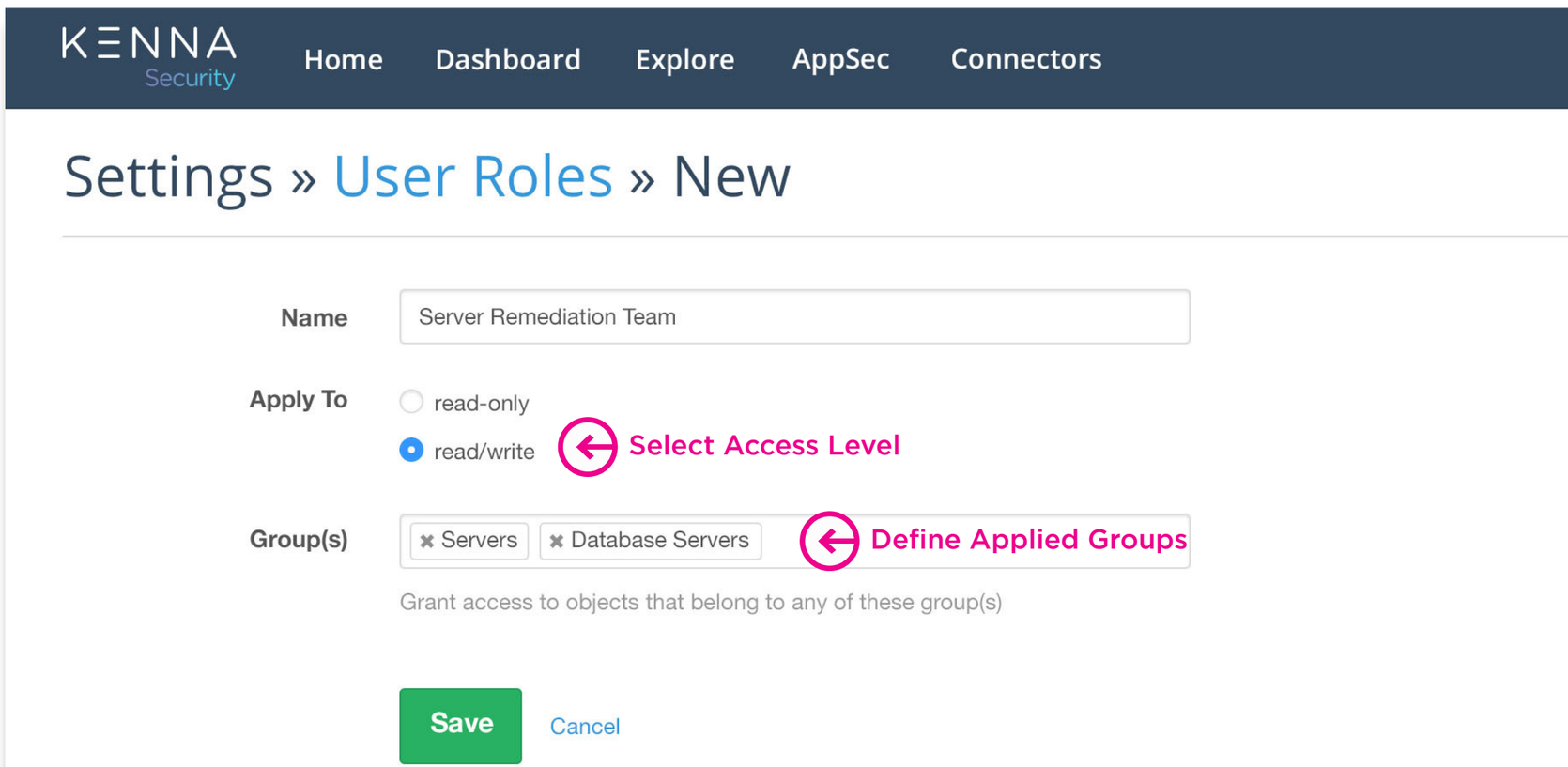


Role Based Access Control

Access to Risk Meter groups, assets, and vulnerability data may be granted / restricted based on user role:

TEST: Create a new user role





Success Checklist

Category	Implementation Functional Requirements	Description
Integration	Ingest vulnerability data from third party scanning vendors	Qualys, Tenable, Nexpose, other
Integration	Ingest 3rd party threat intelligence feeds	Correlate external active threats, exploit and zero day intelligence against assets and vulnerabilities
Integration	Platform scalability	Ingest vulnerability data for x assets with no measurable impact to platform performance
Integration	Integrate with workflow / ticketing tools	ServiceNow, Jira
Integration	API	Ability to ingest asset information from various sources (pen test, CMDB)
Reporting	Vulnerability Risk Reporting	Report asset and vulnerabilities and relative risk based on threat, exploit and local environmental context
Reporting	Generate reports based on logical groups, associated data, dates/times	Asset and vulnerability risk reports based on business context (unit), region, IT support org, asset owner, platform technology, date
Reporting	Generate reports to track exceptions and SLA	Asset vulnerability exception reports on a per host, per vulnerability, or per business basis: set exception expiration dates and SLA
Reporting	Generate historical trending / progress reports	Report asset, vulnerability metrics over time: risk score, active assets, open vulnerabilities, avg time to remediate
Workflow	Track and group assets / vulnerabilities by functional IT group	Create risk meter groups for the following teams: Windows Server, Unix / Linux, Desktop
Workflow	Prioritize vulnerabilities / patches	Prioritize based on vulnerability risk and likelihood of exploit and recommend most effective (risk reduction) patch
Workflow	Track / manage vulnerability exceptions and false positives	Custom fields to capture exception / FP context: business justification, exception expiration, status
Workflow	Track / manage vulnerability SLAs	Automatically set SLA dates based on vulnerability severity / environmental context. Manually set SLA dates
Workflow	Create tickets with grouped vulnerability / patching actions	Create ServiceNow / Jira ticket with remediation actions (group by asset, business context, functional group, platform technology)
Security	Role Based Access Control	Grant / restrict access to asset / vulnerability data based on user role)
Alerting	Automatic Email Notification	Option to generate email notification for risk and vulnerability state changes: risk score change, vulnerability exploit change

Kenna Security
350 Sansome Street Suite 500
San Francisco, CA 94104

Phone: **(855) 474-7546**
Email: **hello@kennasecurity.com**
Web: **www.kennasecurity.com**

Team Up On Risk

© COPYRIGHT 2019 KENNA SECURITY, INC. ALL RIGHTS RESERVED.