Interchange 17

Patch Policy/ Security Policy Usability Test

Lucy Dobler,

Ivanti Uno User Research

ivanti

TABLE OF CONTENTS

SUMMARY

The primary purpose of this user test was to validate the User Interface and Interaction designs for security policies for project Ivanti Cloud Uno. The security policies encompass Patch, Device Control and Application Control.

The participants at Interchange 17 were not familiar with Application Control or Device Control, reducing the testing to mainly testing Patch Policy and the Landing Page. Overall we have data from 8 participants summarized in this report, 7 at Interchange 17, and an additional user via a remote session the week after Interchange.

The patch policy design had been tested with users before the Interchange 17 event and had gone through multiple iterations, not just based on user feedback but also on discussions and reviews with various development groups and product managers. Some of the previous findings are included in this report, therefore the data basis for the patch policy encompasses more information than the tests done at Interchange 17.

A secondary goal of this activity was to enrich the Uno user research participant database with more contacts for future user research.

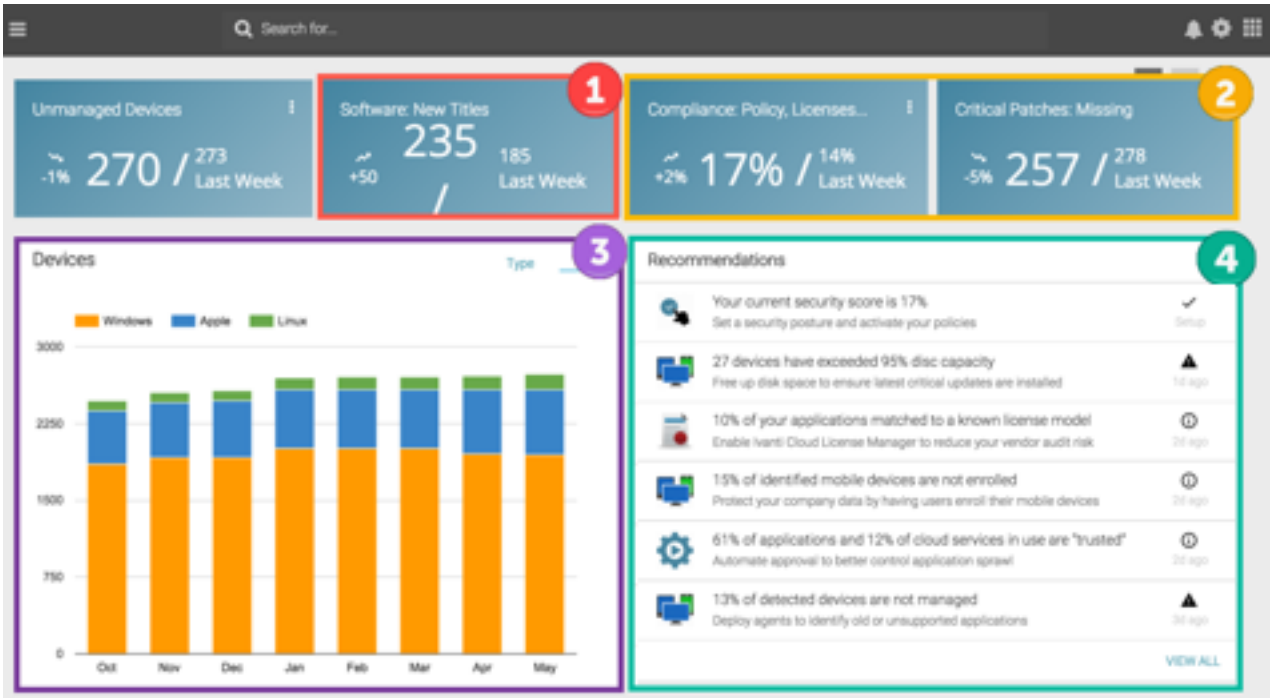
EXECUTIVE SUMMARY OF FINDINGS

- **The instance of a patch policy instance has to allow exceptions at every stage.**
- **End-users blame patches even when they had nothing to do with a problem.**
- **Best Practice/ Recommendation: Shift responsibility for verification of a patch to the business (user)**
- **Server patching and end-user device patching are handled differently and are done by different IT groups**
- **The current Ivanti client management products are not good at notifying the IT Admin about the patching progress and any related errors.**

DESIGN RECOMMENDATIONS

- Make the security posture part of the onboarding / welcome or feature discovery experience.
- Keep the IT Admin informed about the automated processes and errors encountered by implementing Alerts/ Notification or a Watch list.
- Include markers for PCI, HIPAA, SOX etc. compliance in the industry score.
- Consider making the checkmarks on the Security Tiles interactive, so features can be turned on and off.
- Consider making the terms “White list”, “Black list”, “Trusted Vendors” and “Trusted Owners” on the Application control tile shortcuts to the respective lists.

FINDINGS LANDING PAGE



1. This KPI drew the most interest from a Licensing Analyst.
2. Compliance and critical patches drew the most interest from desktop/network engineers.
3. Most prevalent comment: “Nice, but I don’t need to see this all the time.”
4. Most prevalent comment: “Can I customize these and dismiss some? I am only interested in a few of those”.

FINDINGS PATCH POLICY

The instance of a patch policy run has to allow exceptions at every stage.
For example a patch policy might be defined to have 4 stages: Test Group 1 (IT internal), Pilot 1, Pilot 2, Production. In Pilot 1, 95% of devices have been patched successfully. Some users report problems with one application. The IT Admin will want to continue the patch policy instance run as defined, with the exception of either one application, one specific patch from a patch package or a device or user group from the instance when it proceeds to Pilot 2.

At this point it would be useful if Uno creates another one-off instance of the policy that contains the omitted group and is paused. Once the problem is fixed, the IT Admin can go in and simply start the instance to complete the patching process.

End-users blame patches even when they had nothing to do with a problem

A side note to the above paragraph: An end-user is likely to assume any problem that occurs in proximity to a previous upgrade and reboot is caused by the upgrade, even when it isn't. Therefore users will often blame problems on patches, even though the patch had nothing to do with the problem

Shift responsibility for verification of a patch to the business (user)

Every IT Admin we talked to reported some major snafu with patching: 1800 cashier's machines stuck in a reboot loop, a reboot for the whole company at midday at noon are examples. Or a CEO pacing up and down in the IT Admins Cubicle because all Domain Controllers were down and nobody could login within the whole company. The latter incident prompted the IT Admin to decide to shift the responsibility for the verification of patches to the business. A pilot user group is notified per email about new patches and at least 50% of the recipients need to formally approve the patch before the process proceeds to the next stage or the next pilot group.
This seems to be a good practice.

Typical composition of test and pilot groups for patching

The first test group is often the IT subgroup the IT engineer is in or the whole department. If something goes wrong with the patches, IT staff is tech-savvy and know how to help themselves.
The first and second pilot group is often a static group with selected devices / users from all over the organization. They are composed like that to make sure all existing software is covered. A CAD solution might only exist on devices of engineers or in a manufacturing plant - if an OS update is affecting the CAD solution, only this department or these users will be affected.
Production groups are mostly dynamic groups. If the rollout to production is staggered it is mostly by location or by department groups.

Versioning of policy definitions

We asked test participants if they need versioning of the policy definitions or if a rollback to just the latest (working) definition is enough. They answered that one rollback would suffice. One person said "versioning would be nice" but could not elaborate why he would go back more than one version.
Important: This applies to AC and DC policies. For patching policies versioning does not make much sense. If a patch policy instance encounters problems, it will be modified by the IT Admin (e. g. make an exception for one app like taking Lync out). Rolling back to the last state would mean uninstalling patches and that is often not even possible.
MacOS does not support uninstalling patches at all and for Microsoft patches it does not necessarily work because of dependencies.

Industry score

The industry score was not that useful to test participants. They said that the standard within their company is relevant, not what others are doing. One thought it would be nice for his manager, but he doesn't need to see it all the time.
One had a good idea: instead of the industry score the graph could contain marks that indicate compliance standards like HIPAA, PCI, SOX, so they know immediately if they are compliant or not.

Change Management Process

All participants asked, confirmed that their patching process for servers is tied to a change management process. The patching of end-user devices however is not.

Server patching and End-user device patching are done by different groups

When we created the user persona for Tom, the technician, it was built on the premise that he works in a smaller company (around 500 employees, 2000 max.) and is responsible for patching servers as well as end-user devices. Uno is targeting much bigger companies now and it's common to have a desktop engineering and a network engineering group in these organizations. The network engineering group is responsible for patching servers and the desktop engineering group takes care of end-user devices.

Server patching and end-user device patching are handled differently

This is what we heard from the Interchange participants. It shows a trend, though

individually a company can have other settings
e. g. a very small customer we talked to (100 endpoints) has no staging copies for his servers and he "babysits" them during the patching process after hours, to make sure they are working.

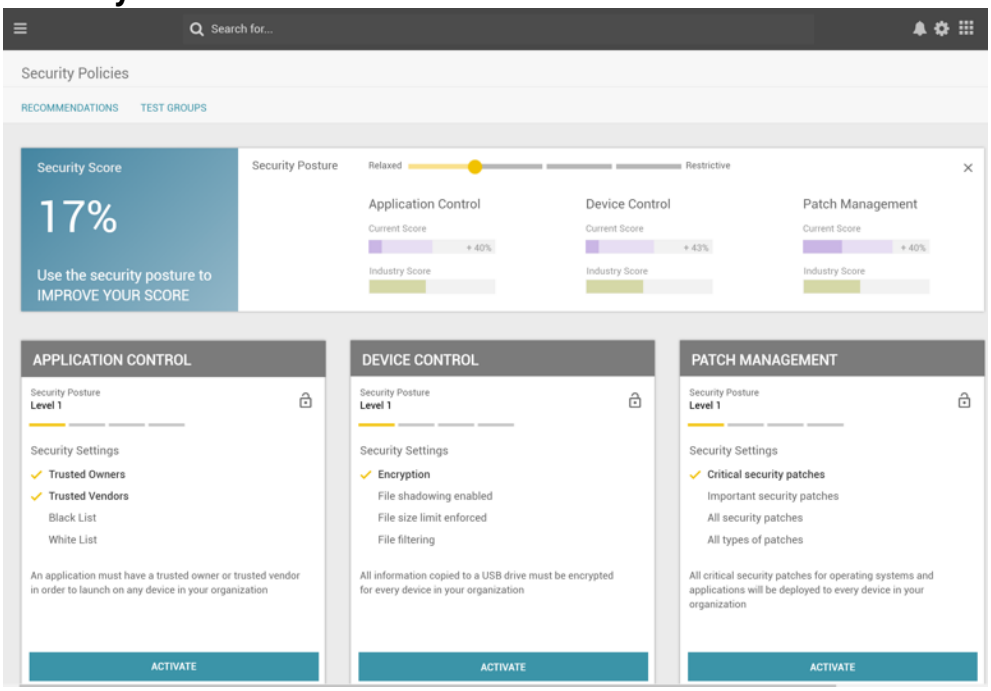
Property	Servers	End-user devices
Maintenance window	very restricted	mostly unrestricted
Change Management Process	yes	no
Deferment by user	not useful, server has no primary user	yes
Test patch on staging copy	yes	no
Pilot group with representative sample of devices	no	yes

Table 1: Server vs End-user Device Patching

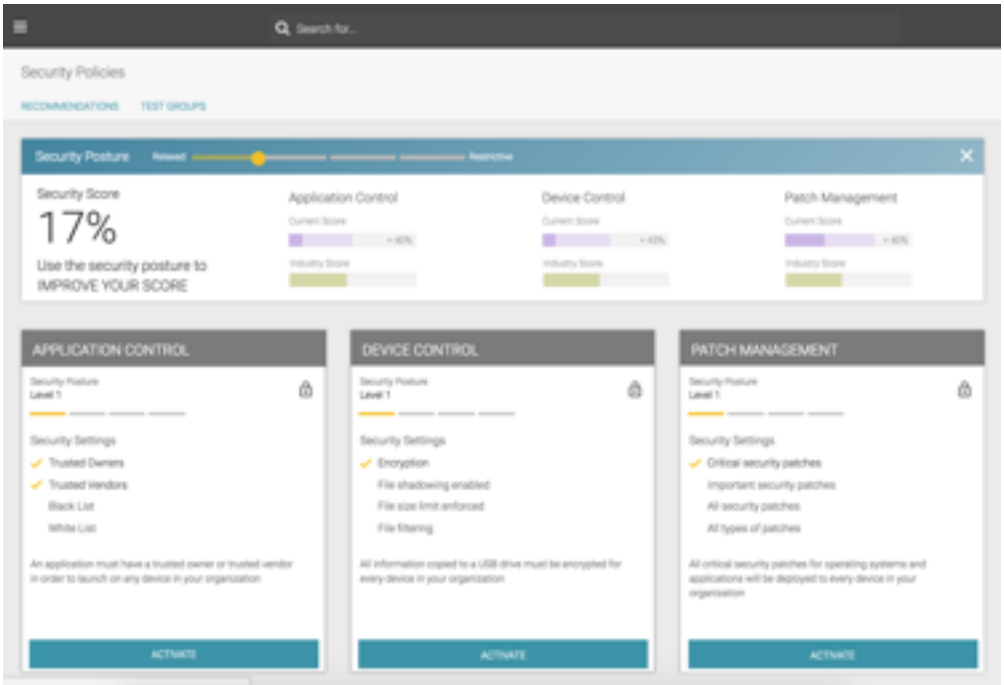
No alerts about the progress of the patching process

Participants complained that it is not easy for them to detect if there is a problem with a patch deployment. They don't get notifications or alerts informing them that there were errors, or if the deployment process stopped altogether. Instead they have to dig around for this information by going through logs. This is something we heard over and over again. It seems to be a problem that is shared by several of our products: LANRev, EMSS, DSM and now Shavlik Protect and LDMs.

Security Posture



In the first version the security posture had more affordance, was more inviting to use.



The security posture in the header was not immediately recognized as an interactive element.

In this iteration the security posture was in the header area for the page. Users overlooked the interactive slider element more easily compared to the previous position.

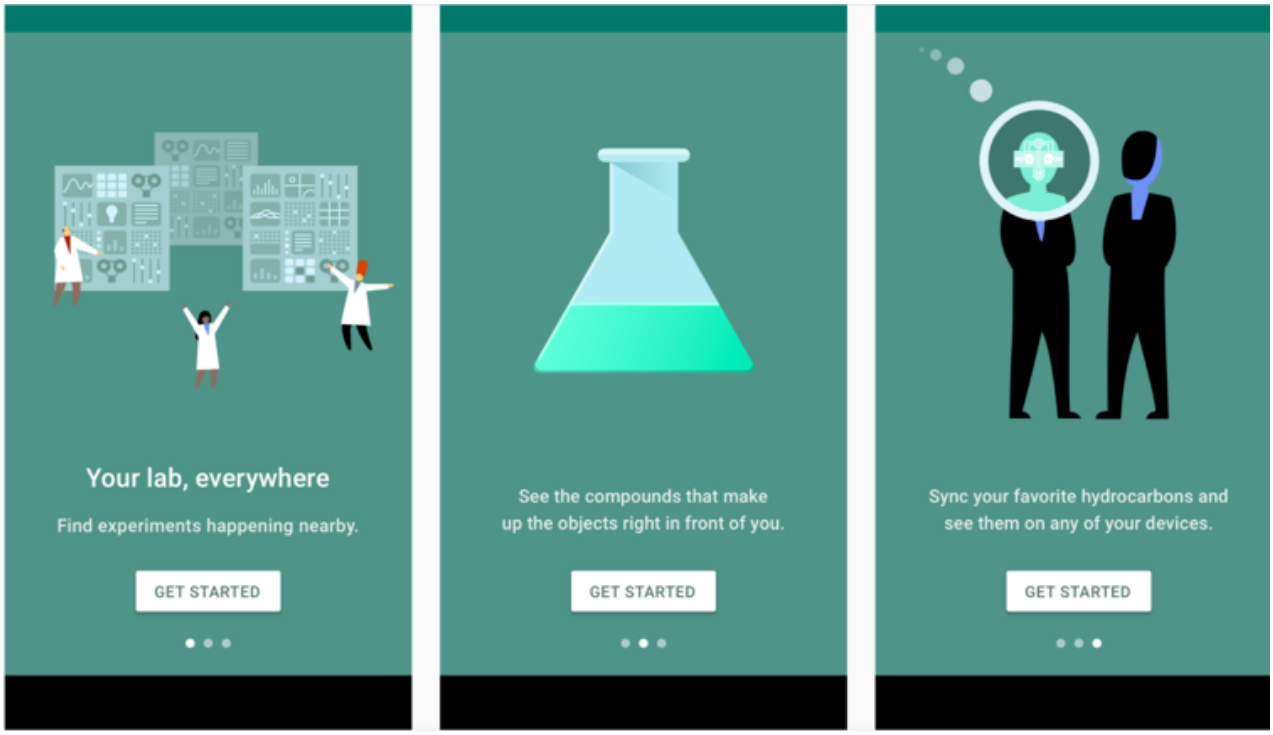
Users did realize that when they changed the slider, the content (checkmarks) in the panels below changed. They believed that the higher you set the security posture, the more checkmarks you get. This is not really true. On the highest level AC would only have a checkmark on whitelist, but not on blacklist, trusted vendor, or trusted owner.

After activating the three policies, the panel with the security posture disappeared. Only one test participant remarked on that and wondered why it was gone.

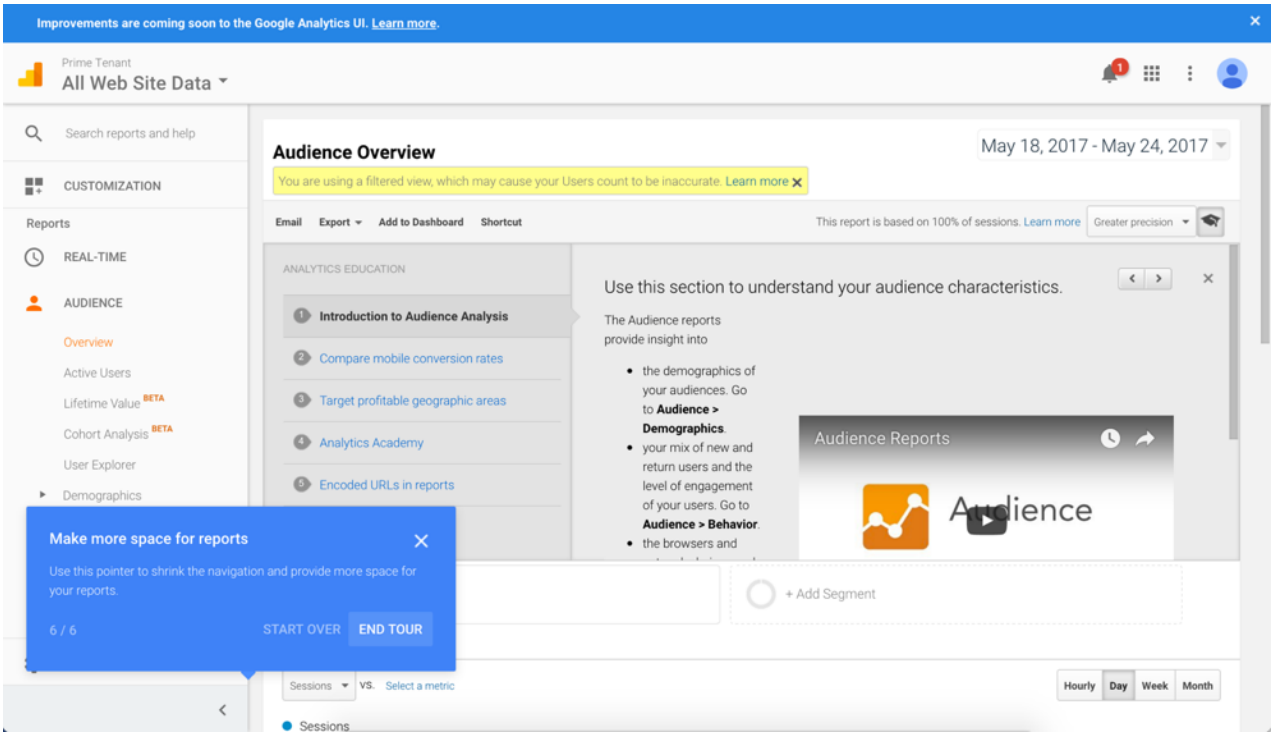
In this design the security posture functions like a help mechanism to set the first default for the novice user. After setting it to the desired level and activating the corresponding policies it fulfilled its purpose. It should therefore not be a permanent element of the page but rather be part of the Onboarding/ Feature Discovery Experience. This hasn't been fully designed and specified yet, but whenever new functionality or data becomes available to the user, a panel or another UI element shows up to introduce the user to the new feature. The panel often consists of multiple pages that the user can walk-through to learn about the product, or dismiss it.

Recommendation: Make the security posture part of the onboarding / continuous feature discovery experience.

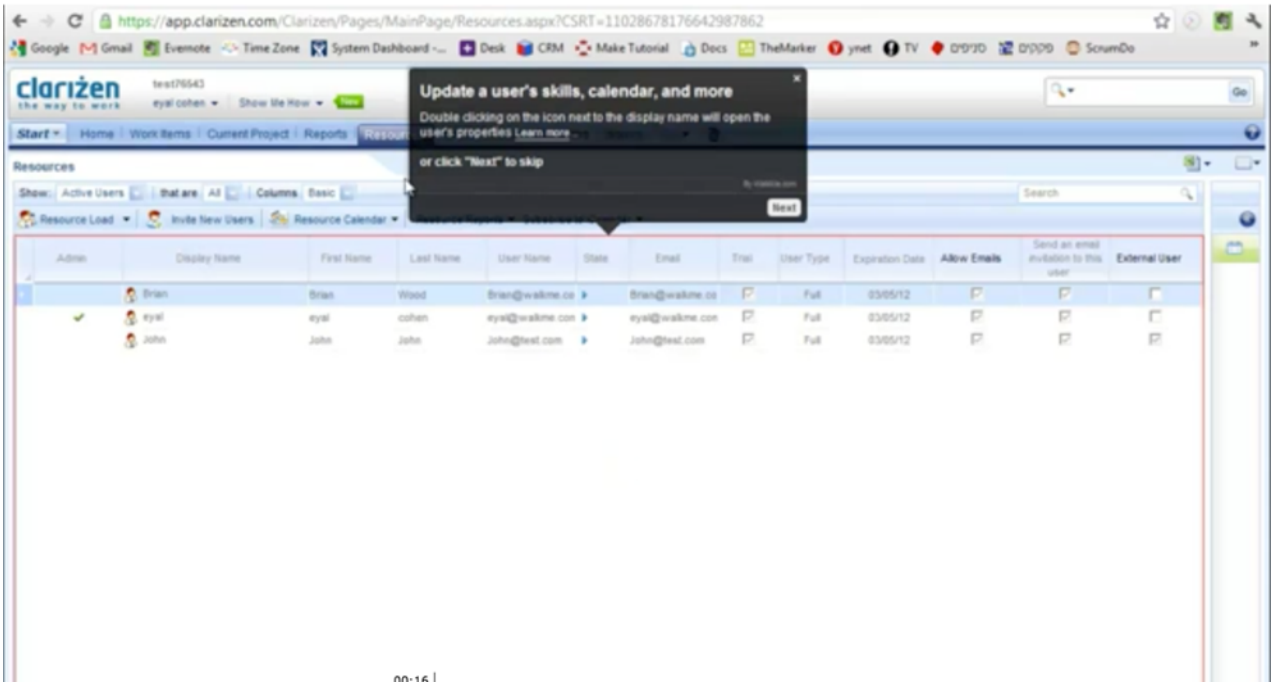
In our test the participants were only interested in patching. Putting the security posture in the onboarding experience would solve the problem that the security posture would permanently remain on the page if the user only selects patching, but leaves AC and DC inactive.



Example for an onboarding experience with a rotating carousel as described in the Material Design Guidelines.



Example for onboarding / feature discovery experience with Callouts from Google Analytics.



Example for onboarding experience with callouts from Walkme.

Personas need to be revised

The user persona "Tom, Technician" was built on the assumption of a small company size of around 500 endpoints as mentioned earlier. Uno is now targeting bigger companies and they have more specialized IT roles. From the user test and interviews done over the past months the new suggested user personas are: Desktop Engineer, Network (or Infrastructure Engineer) and Security Engineer. With the service management module Uno will also be relevant for Service Desk Analysts, Service Desk Managers and IT Managers, CIOs, and CSOs.

PARTICIPANTS

The participants were current LanDesk and Shavlik users. Though the conference was attended by customers of the former HEAT products, they didn't participate in any test sessions for patch policy. For more details on the participants and their respective companies see the next paragraph.

The test subjects self-selected to participate in the usability study.

COMPANY SIZES AND NUMBER OF ENDPOINTS

User	Title	Company	No. of Employees	No. of Endpoints
Oscar	IT Engineer	Pinnacle Foods	2,000	3,600
Kumar	Technical Supervisor	Geico	36,000	16,000 servers, desktops unknown
Kirch	Senior Systems Engineer	Geico	36,000	16,000 servers, desktops unknown
Todd	IT Infrastructure Manager	Hillsborough County Sheriffs Office	3,400	4,500
Betty	LANDesk Administrator (Software Compliance)	State of South Dakota	8,000	9,800
Matt	IT Support Manager	Fairfax Media	6,400	6,500
Stefan and Richard	Chief Software Engineer, CEO	Five 9s	15 - Five9s is a Partner	Customers range from 200 to 10, 000 endpoints
Simon	Chief Technologist	Ivanti	Na	na
Jens*	Administrator	Entwaesserungs-werke Koeln	600	700

* Note: Jens, the last participant was not a test participant at Interchange. A remote testing session was conducted with him in the week after Interchange 17.

Table 2: Participants and Company Information

PROCEDURE

UX testing took place on three days, starting Tuesday May 9th to Thursday May 11th at the Interchange 17 event at the Mirage Resort in Las Vegas.

A room (Key Largo) with a check-in desk was reserved for UX activities. It accommodated 6 testing stations. Testing started at 10:30am, after the Keynote presentations in the morning had finished. It continued throughout until around 5pm daily, except for Thursday when testing ended at 1pm.

The testing station was equipped with a laptop, an external monitor, external keyboard and a mouse.

The laptop was used to access the prototype. The session was recorded at the same time using Camtasia. The prototype was created with Axure by the Lead Designer Robert Fuller.

The average testing session lasted one hour. Some users had more time and additional topics could be explored. Others had to leave early, so the duration had to adapted and not all tasks could be completed.

PROTOTYPE

The policy prototype can be accessed here: http://u3h2nf.axshare.com/#g=1&p=ivanticloud&c=1

As it will be changed continuously, the state of the designs at the time of testing is documented in the screenshots in the last section of this report.

PROFILE INTERVIEW QUESTIONS

This first part established the participants and the companies background and IT landscape. It is useful to have this context since vastly different answers and reactions can sometimes be explained by this background information.

The information was mainly collected to build out the user research contact database, so the information is not covered in its entirety in this report for patch policy.

The company and role information are referenced in Table 2.

Organisation / Company

- Name
- Industry
- Location
- Global distribution of sites and branches

Basic Profile

- Role
- Experience in Role
- No of Employees in company
- No of IT employees in company
- IT Subgroup the participant is in
- Short description of his most frequent tasks

Device Landscape

- No of Endpoints
- How many of these are Win/ Mac/ Linux?
- Any Mobile Device Management? Percentage of IOS vs Android (or Blackberry)
- Are they using any endpoint management solutions right now? Which ones? Are they using it for desktops and servers?

Explore Automation needs

- What are the most frequent tasks for them? What do they spend the most time on?

Explore how they are automating routine, recurring tasks with the following questions:

- What do they automate? What would they want to automate? What are the tools they currently use to do this?

ANSWER TO AUTOMATION NEEDS QUESTION

- Employee Onboarding and Offboarding: HR should trigger the process and everything after it should be completely automated.
- Patching Process: There is still a lot of manual work required, it should be automated more.

USABILITY TEST SCRIPT AND QUESTIONS FOR APPLICATION CONTROL DESIGN

The security policies combine policies for Application Control, Device Control, and Patching. One major focus was to get more feedback on Application Control, but none of our test participants were uvery familiar with it. Some reported that they utilize Application Control in their company, but it's not within their team and they couldn't identify which tool was used for it.

The section about Application Control was therefore skipped but we still asked what the terms Whitelist, Blacklist, Trusted Owner and Trusted Vendor meant to them.

General Questions around Policies

- ➔ When the customer does a rollout of any change, software, security policy, patches; how many stages do they do that in? Just one? Test + Production? Or multi-phase rollout?
- ➔ Do they use the same rollout process for ALL types of change?
- ➔ How long does a typical change take to rollout: a day, a week, a month? (does this vary with size of the environment??)
- ➔ Should the policies be VERSIONED, or do they just want to UNIQUELY NAME each policy?

General Questions around Application Control (before starting the prototype)

- ➔ Are they using Application Control (AC) right now or have they done so in the past?
- ➔ If not, did they ever consider implementing it, maybe only for specific user groups?
- ➔ If yes, how do they organize it? Which groups have special restrictions or exceptions to the rules? Any test groups for AC?
- ➔ If they are using a product for AC right now - can they show us how they have set it up?

Policies and Change Management

Are they using a Change Management Process at their company? Are policy changes (AC, DC, Patch) tied to the Change Management Process?

Landing Page

- Explore the Screen.

➔ Record what they say about the data, what is meaningful to them and which data they are confused by.
➔ Record the reaction when they read through the recommendations.

- Encourage them to act on the recommendations

➔ Leads to the policy page.

Policy Page

-> Policy page repeats the recommendation for improving the score on the left.

Security Posture

- Explore the policy screen.

➔ Do they understand the relationship between the security posture level and what each level contains, as seen in the table below?
➔ If they are wondering about the security posture: do they understand it as a score? Would a score be helpful to them?
➔ What is the security posture they would select for their company?

Application Control Terminology

- When they read through the table- do they know what all the terms mean? Whitelist / Blacklist, trusted Vendor, trusted Owner?

Device Control Terminology

- When they read through the table- do they know what all the terms mean? File Shadowing?

ANSWERS TO THE TEST SCRIPT QUESTIONS

General Questions around Policies

- ➔ When the customer does a rollout of any change, software, security policy, patches; how many stages do they do that in? Just one? Test + Production? Or multi-phase rollout?
  - **Multi-phase rollout is the most common.**

- ➔ Do they use the same rollout process for ALL types of change?
  - **Server patching and end-user device patching is done differently.**

- ➔ How long does a typical change take to rollout, a day, a week, a month? (does this vary with size of the environment??)
  - **One test participant had a (strict) SLA that all patches had to be rolled out within 2 weeks.**
  - **Others reported that it might take them up to 4 weeks to rollout patches to end-user devices.**
  - **Servers are patched earlier, many reserve the days after patch Tuesday to complete server patching as fast as possible (e. g. by working late).**

- ➔ Should the policies be VERSIONED, or do they just want to UNIQUELY NAME each policy?
  - **For Policies in general one rollback is probably enough.**
  - **This does not apply to patch policies. Patches often can't be uninstalled. MacOs does not even offer this functionality and with Microsoft inter-dependencies might prevent an uninstall.**

General Questions around Application Control (before starting the prototype)

- ➔ Are they using Application Control right now or did they in the past?
  - **Participants were not familiar with AC. Some reported they have it in their company but it's managed by another group.**

- ➔ What do you do about ransomware?
  - **We added this question to find out if ransomware attacks ever triggered the**

idea of implementing Application Control.

- **About half of the participants said they had ransomware attacks. They remediated by restoring backups and reported this as being sufficient.**
- **The other half reported they haven't had any problems with ransomware so far.**

➔ If not, did they ever consider implementing it, maybe only for specific user groups?

- **This question was skipped. Participants were not familiar with AC**.

➔ If yes, how do they organize it? Which groups have special restrictions or exceptions to the rules? Any test groups for AC?

- **This question was skipped. Participants were not familiar** with AC.

➔ If they are using a product for AC right now - can they show us how they have set it up?

- **This question was skipped. Participants were not familiar with AC. This was also more intended for the remote user testing sessions that allowed screen sharing with the participant.**

Policies and Change Management

➔ Are they using a Change Management Process at their company? Are policy changes (AC, DC, Patch) tied to the Change Management Process?

- **They all had Change Management Processes implemented at their company. Server Patching is tied to the Change Management Process, but not end-user device patching. They didn't know about AC or DC.**

Landing Page

- Explore the Screen.

➔ Record what they say about the data, what is meaningful to them and which data they are confused by.

- **See Findings Landing Page**.Findings Landing Page

➔ Record the reaction when they read through the recommendations.

- **See Findings Landing Page.**

Security Posture

➔ Do they understand the relationship between the security posture level and what each level contains, as seen in the table below?

- **The participants understood that changing the posture slider position changed the content in the tiles below.**

➔ If they are wondering about the security posture: do they understand it as a score? Would a score be helpful to them?

- **The most prevalent reaction to the posture was to wonder what setting each level would contain.**

➔ What is the security posture they would select for their company?

- **Participants felt they needed to know more about what each level means and which settings are contained to make a decision over what they would set the posture to for their company.**

Application Control Terminology

➔ When they read through the table- do they know what all the terms mean? Whitelist / Blacklist, trusted Vendor, trusted Owner?

- **Participants understood Whitelist, Blacklist and trusted Vendor. Trusted Owner was explained as being a trusted End-user by one participant. After he clicked and explored the details of the Application Control Policy he corrected himself and realized the Trusted Owner is the user account that installs an application.**

Device Control Terminology

➔ When they read through the table- do they know what all the terms mean? File Shadowing?

- **Participants said they know the terms on the DC policy tile. They did however explain that the term devices refers to all devices like laptops and PCs and not just removable storage devices.**

TASK PRINTOUT GIVEN TO THE PARTICIPANT AS A PRINT OUT

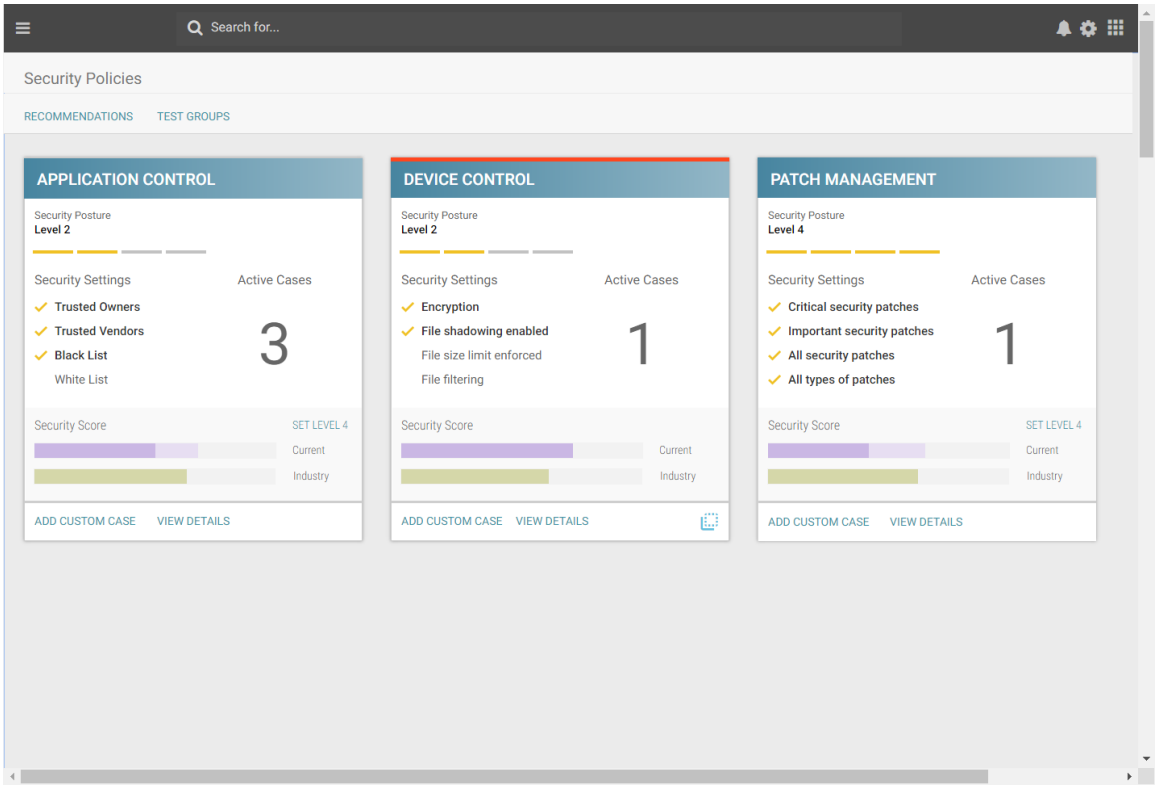
1. Explore the landing screen and tell us what you make of the numbers.
2. Follow the first recommendation on the landing page.
3. Set the security posture to 2.
4. Activate all Policies.
5. Your default patch policy is set to roll out 1 hour after hours of operation (HOP). You want the financial staff to get patches 4 hours after HOP. How would you do that?
6. One of your end points was infected with VeryBadRansomWare.exe and you want to add it to the blacklist. How would you do that?

USABILITY ISSUES WITH TASKS

Task number one was for exploration of the landing page. For tasks 2 throughout 5 no particular usability issues were observed. Participants were able to complete the tasks quickly.

Any special observations are noted below the screenshots in the next section of the report.

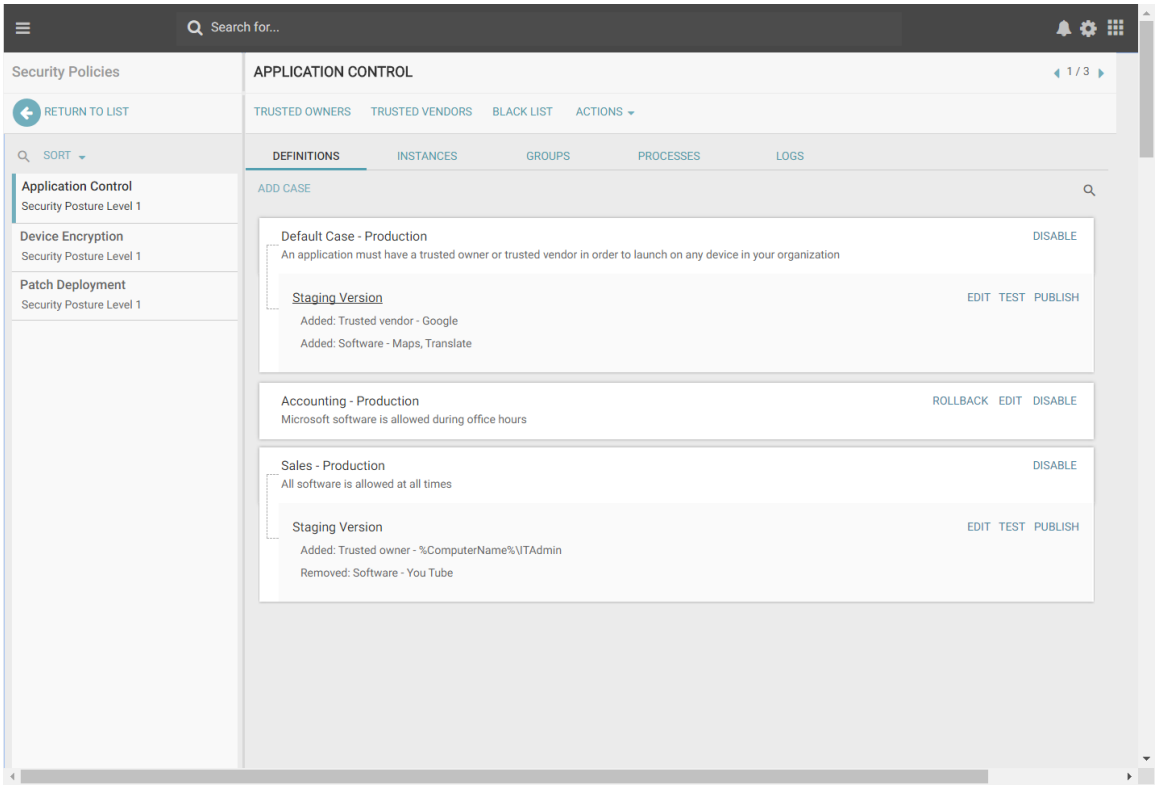
Task 6 turned out to be problematic. Due to time constraints on the participants side task 6 was only tested with one participant. He had difficulty completing the task.



The test participant expected to be able to click on the term “Black List” and tried it repeatedly.

He then tried “Add custom case” within the Application Control tile repeatedly. This leads to the Create AC policy wizard (see **Create AC policy wizard** in the screenshot section). The black list is not contained in the wizard.

To add an application to the black list the user has to click on “View Details”. The participant was only able to complete the task after being asked: “Is there anything else you could click on?”



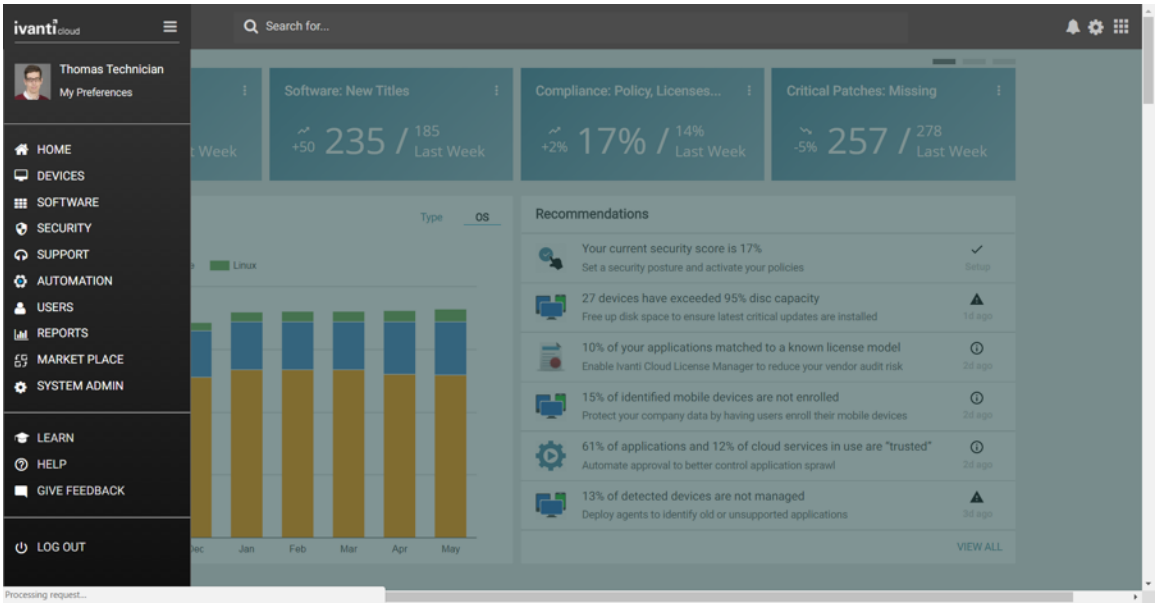
After arriving on this page the participant spotted the tab “Black List” and was able to complete the task.

SCREENSHOTS OF PROTOTYPE

LANDING PAGE

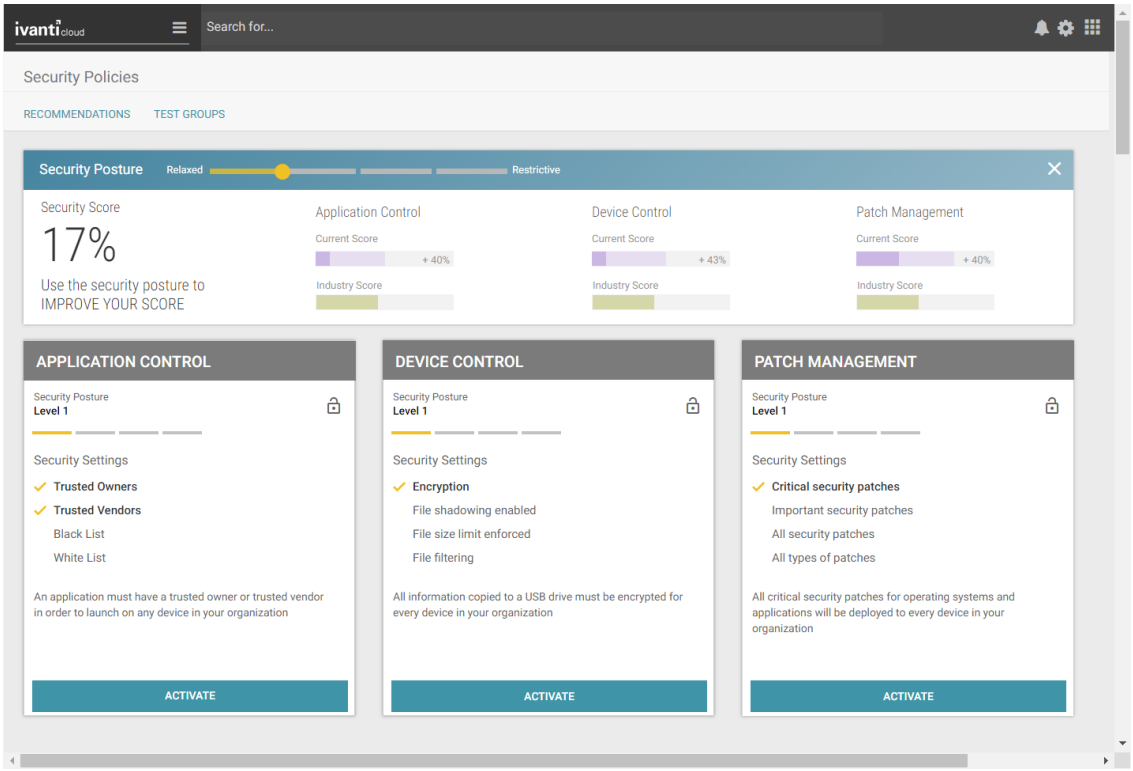
Landing Page

Landing Page with Menu



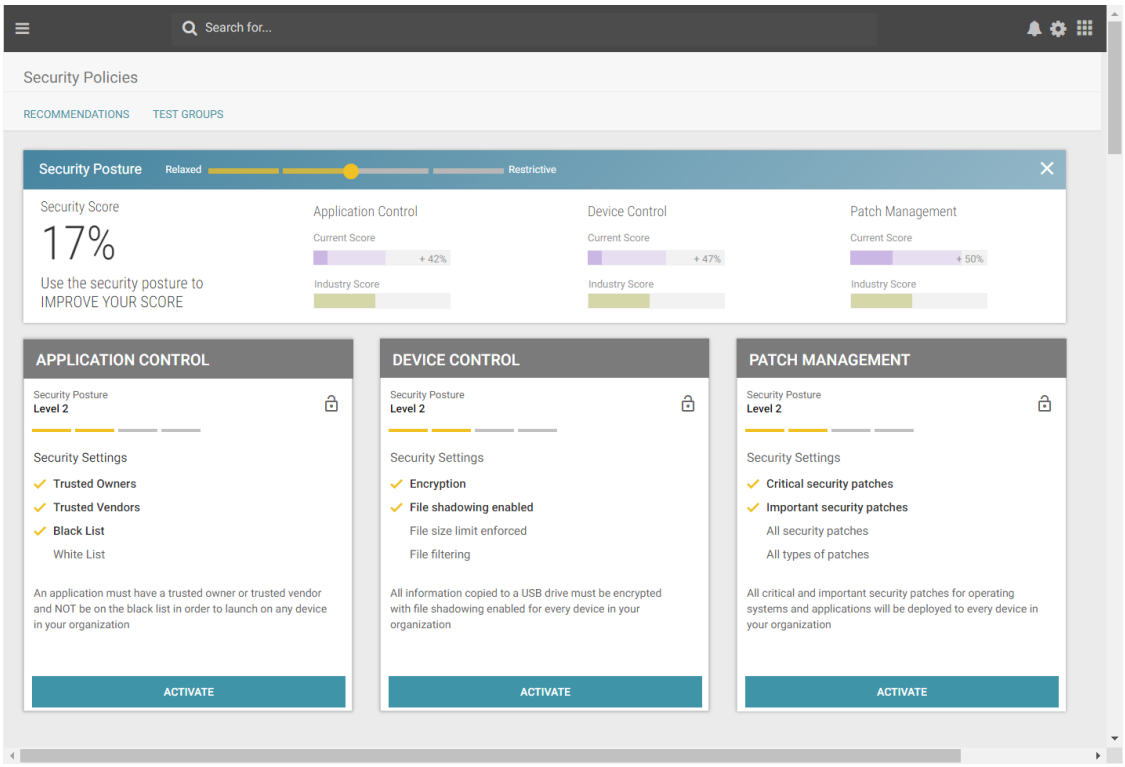
SECURITY POLICY PAGE

Security Policy Overview Page with Security Posture set to 1

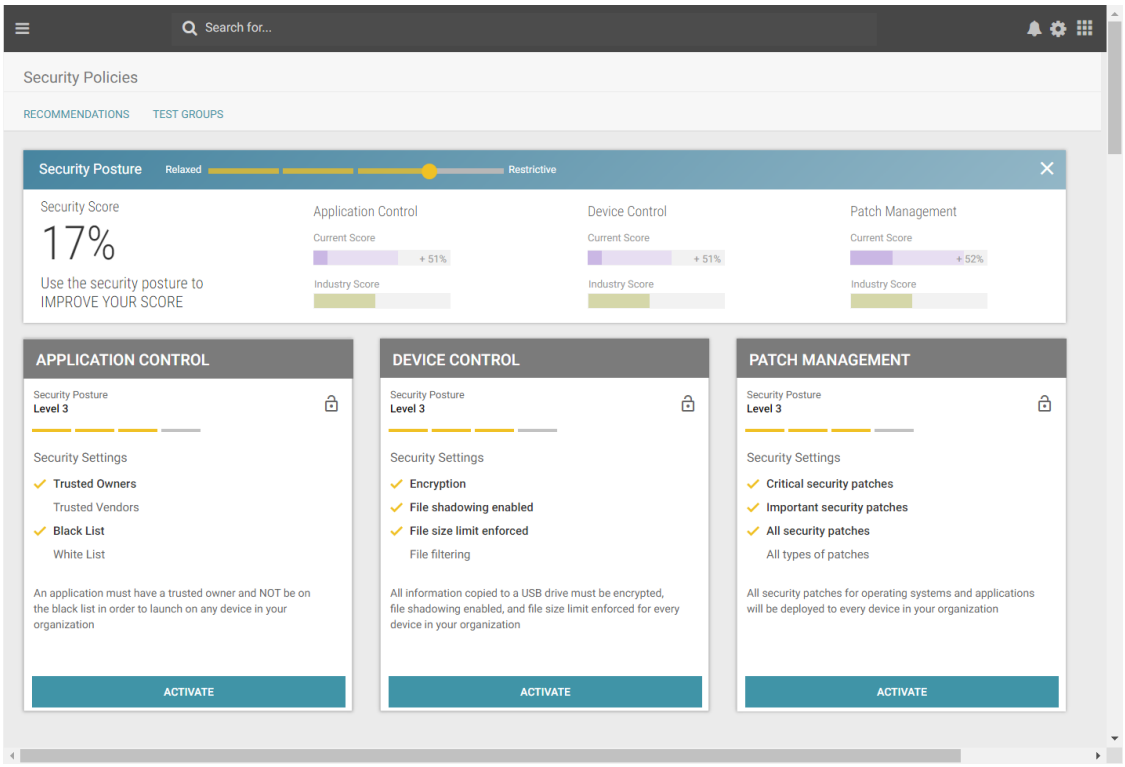


Three participants assumed they could click on the entries on the bottom tiles (e.g. White list) to enable additional functionality.

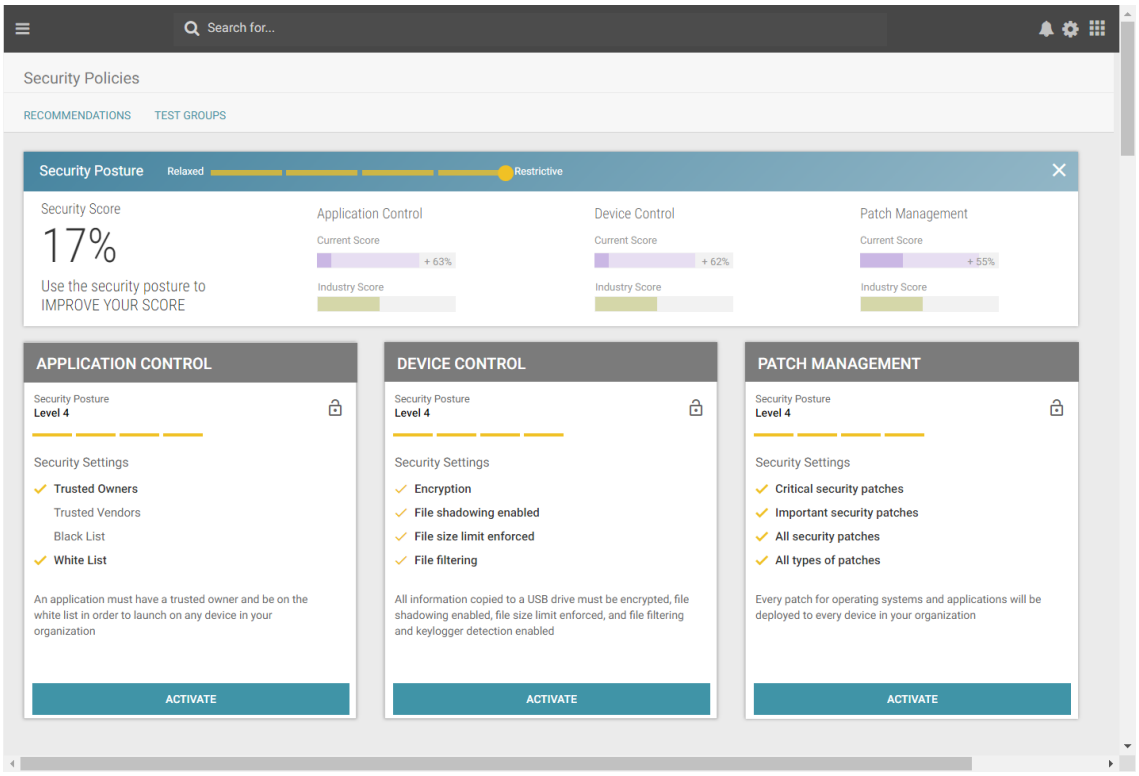
Security Policy Overview Page with Security Posture set to 2



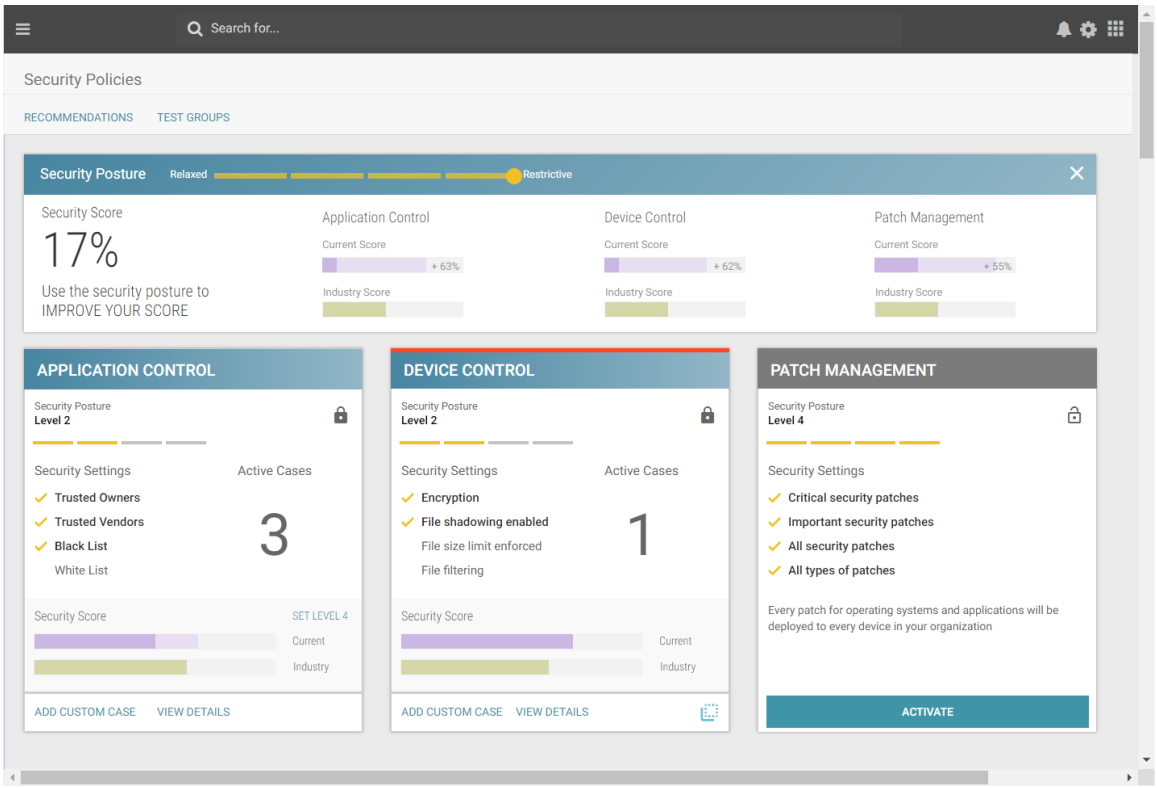
Security Policy Overview Page with Security Posture set to 3



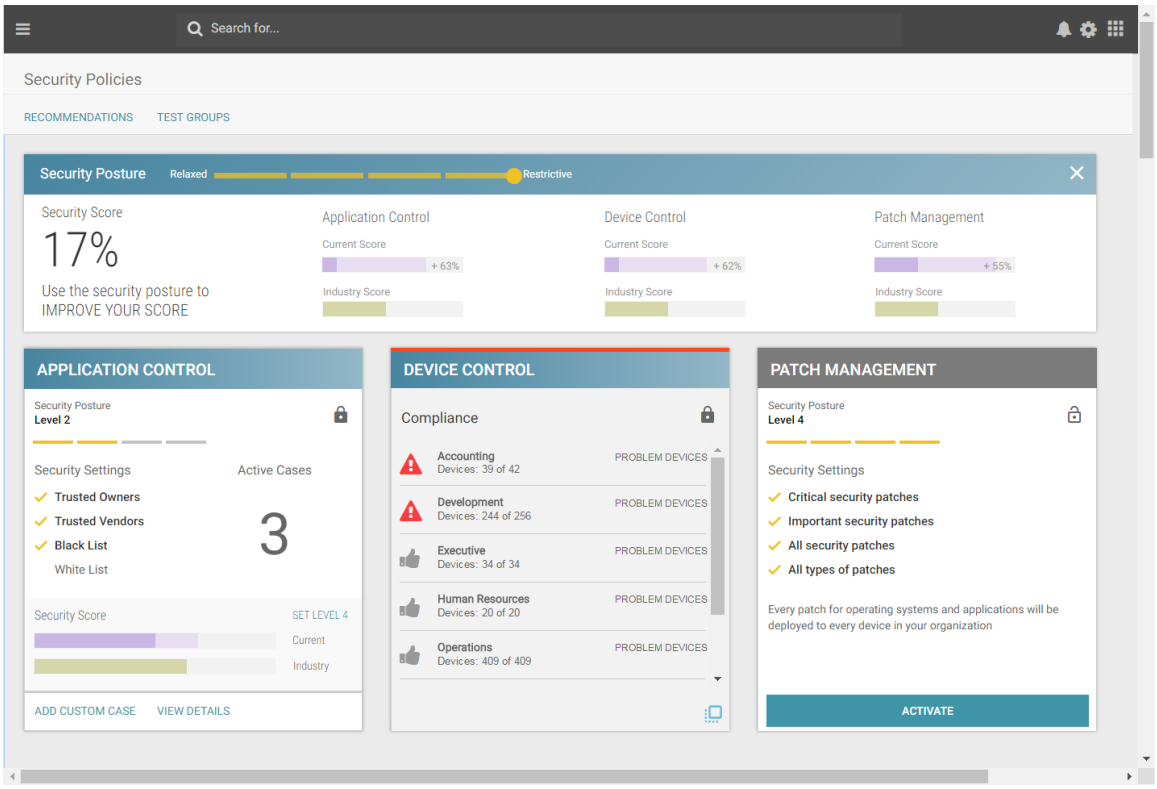
Security Policy Overview Page with Security Posture set to 4



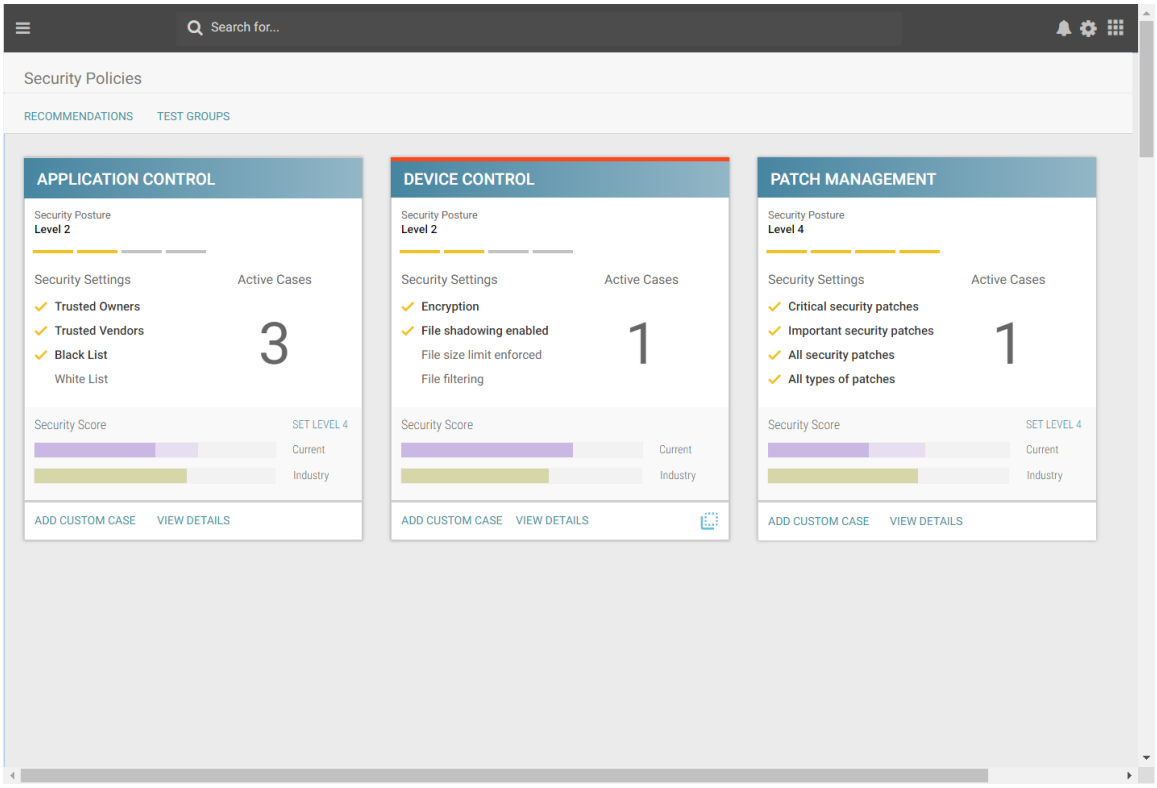
Security Policies Overview with AC and DC policy activated



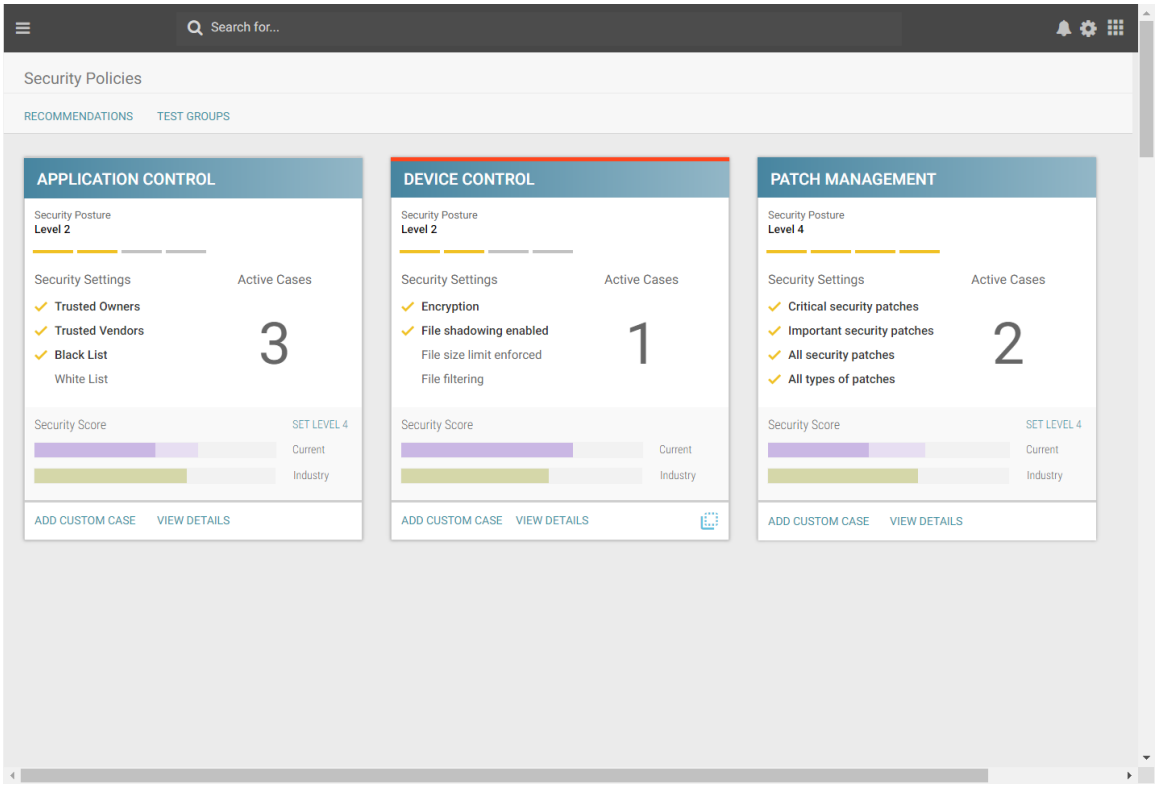
Security Policies Overview with Device Control Card flipped, showing Alerts



Security Policy Overview with all Policies activated

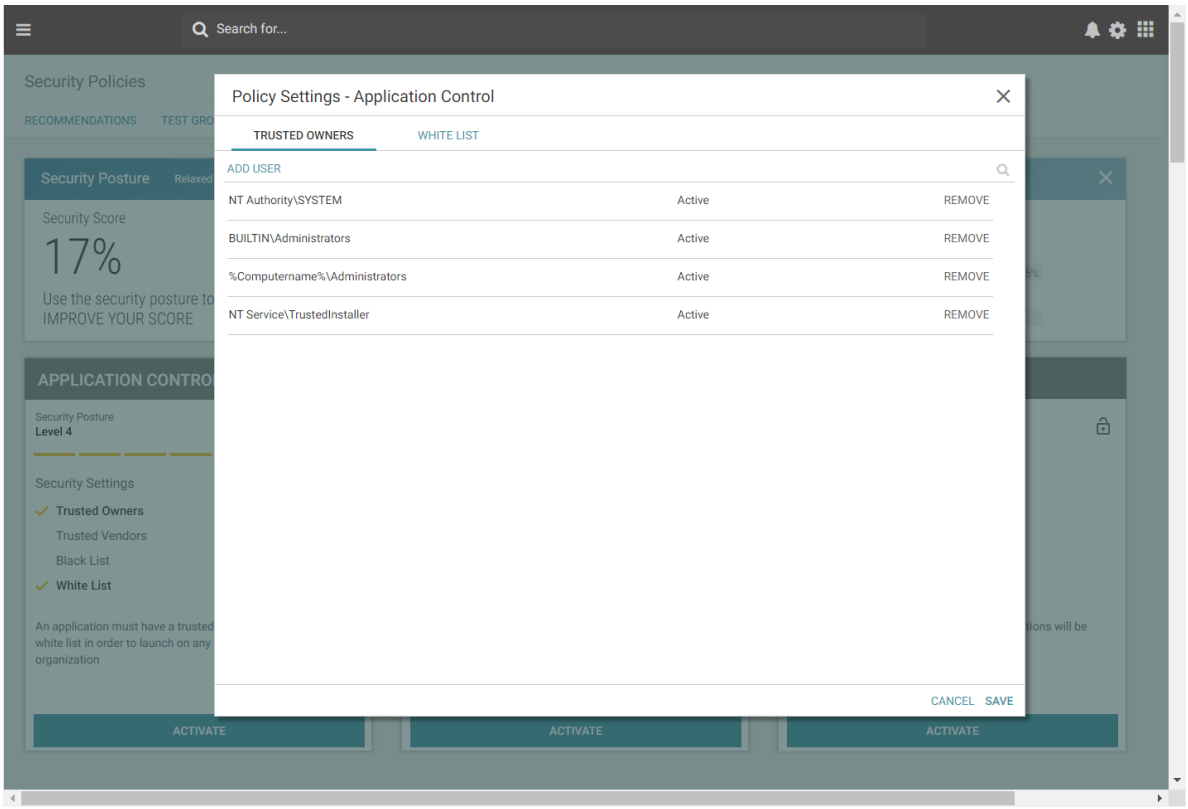


Security Policy Overview after an additional custom case for Patch Management was added. The count of custom cases for Patch Management increased from 1 to 2.

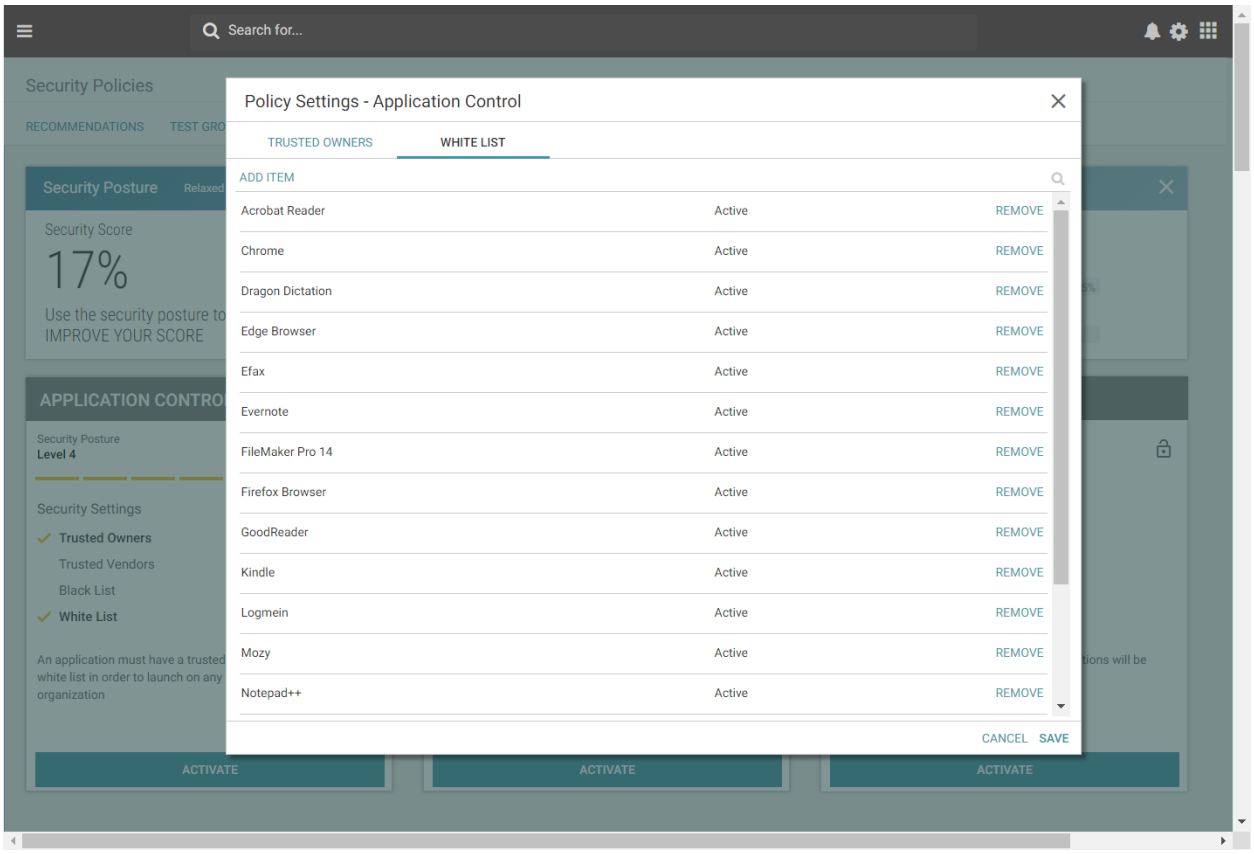


APPLICATION CONTROL

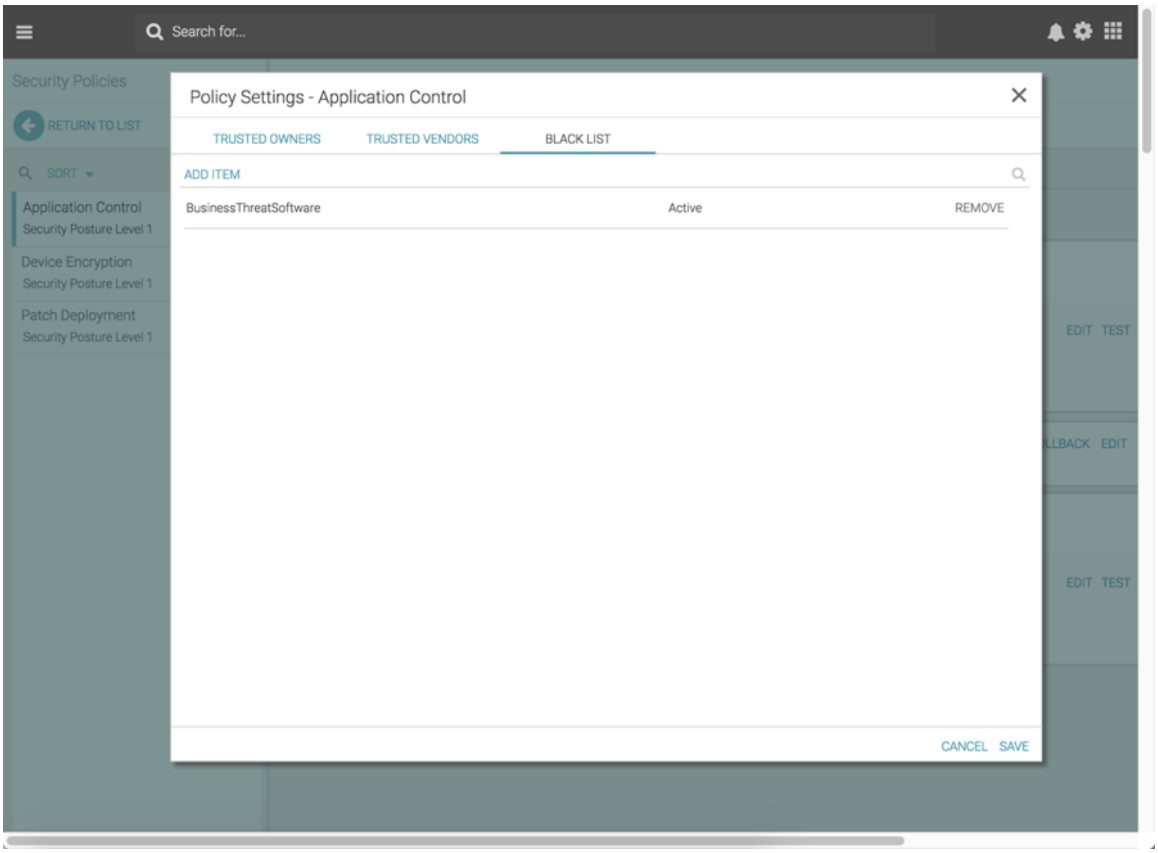
Application Control Mandatory Settings for Activation – Trusted Owner



Application Control Mandatory Settings for Activation - Whitelist

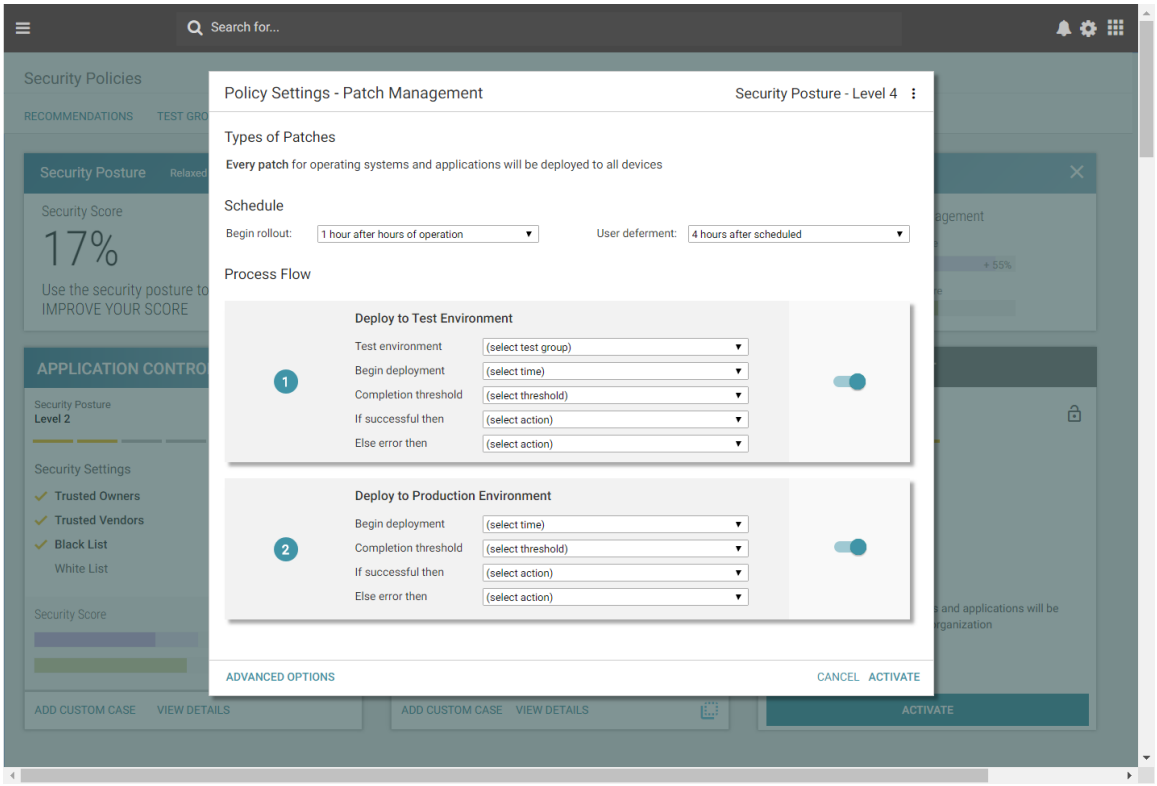


Application Control – Mandatory Settings for Activation – Blacklist



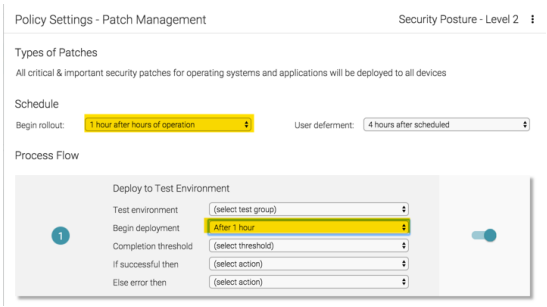
PATCH DEPLOYMENT DETAILS

Patch Policy: Mandatory settings to activate Patch Policy

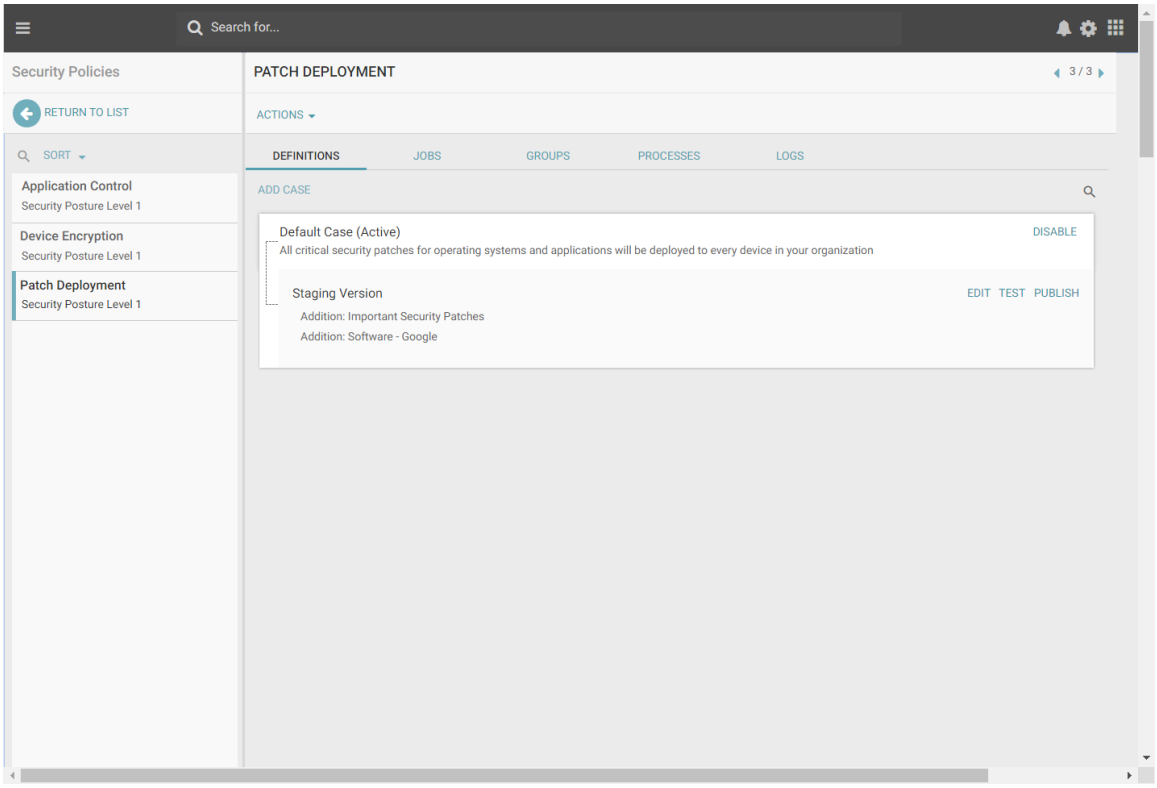


There is “Begin Deployment” and “Begin Rollout”. That was confusing to one user.

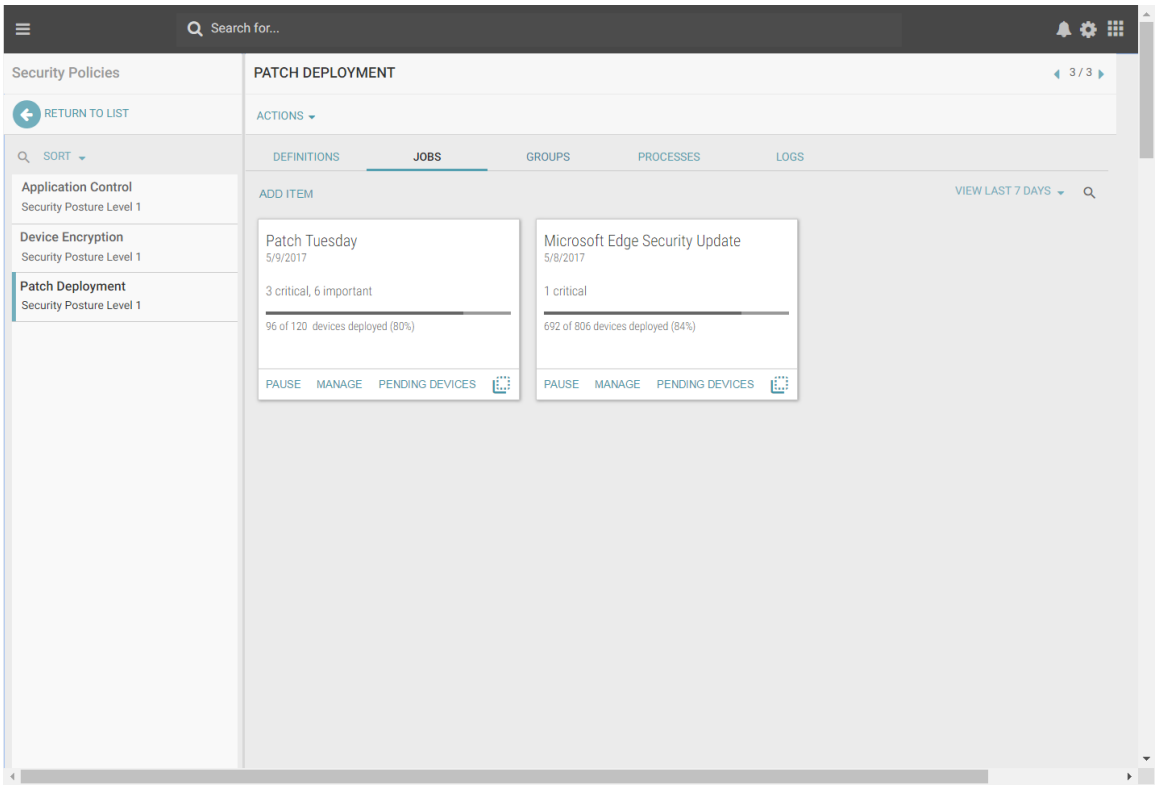
Recommendation: Remove the upper value. The begin of a phase should be handled in the phase information block.



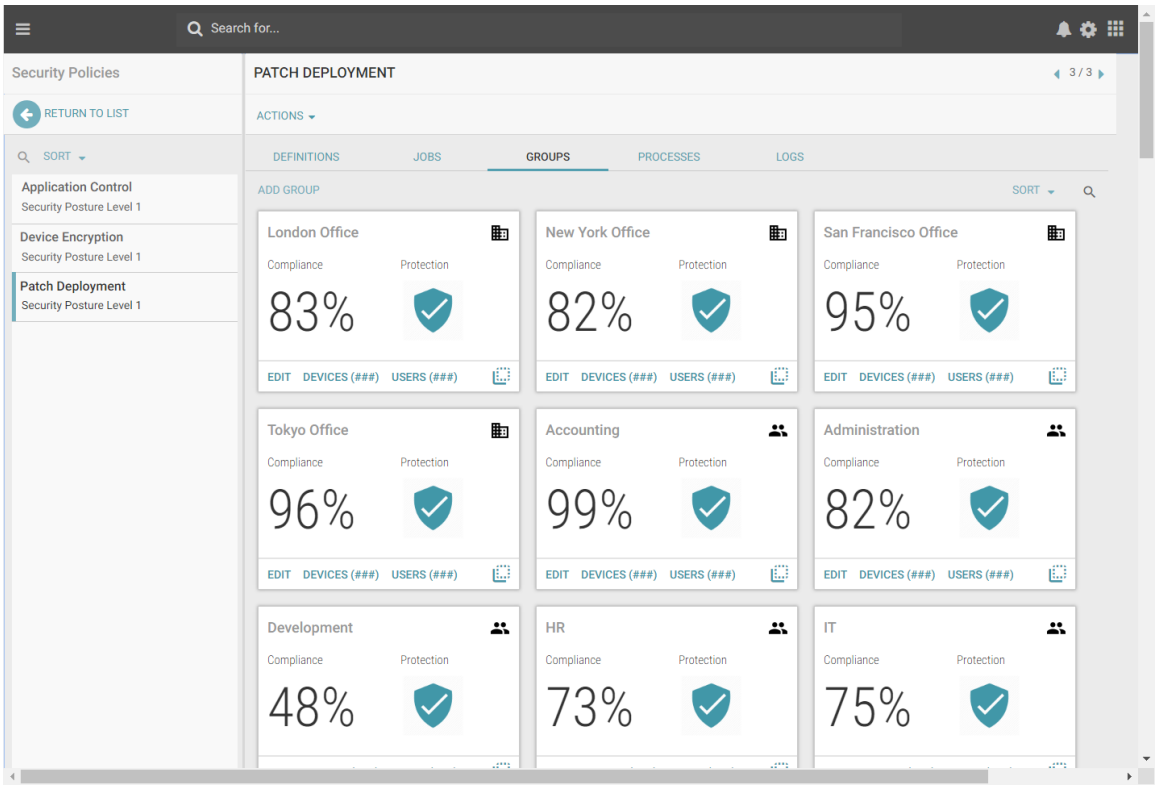
Patch Deployment Detail View – Definition



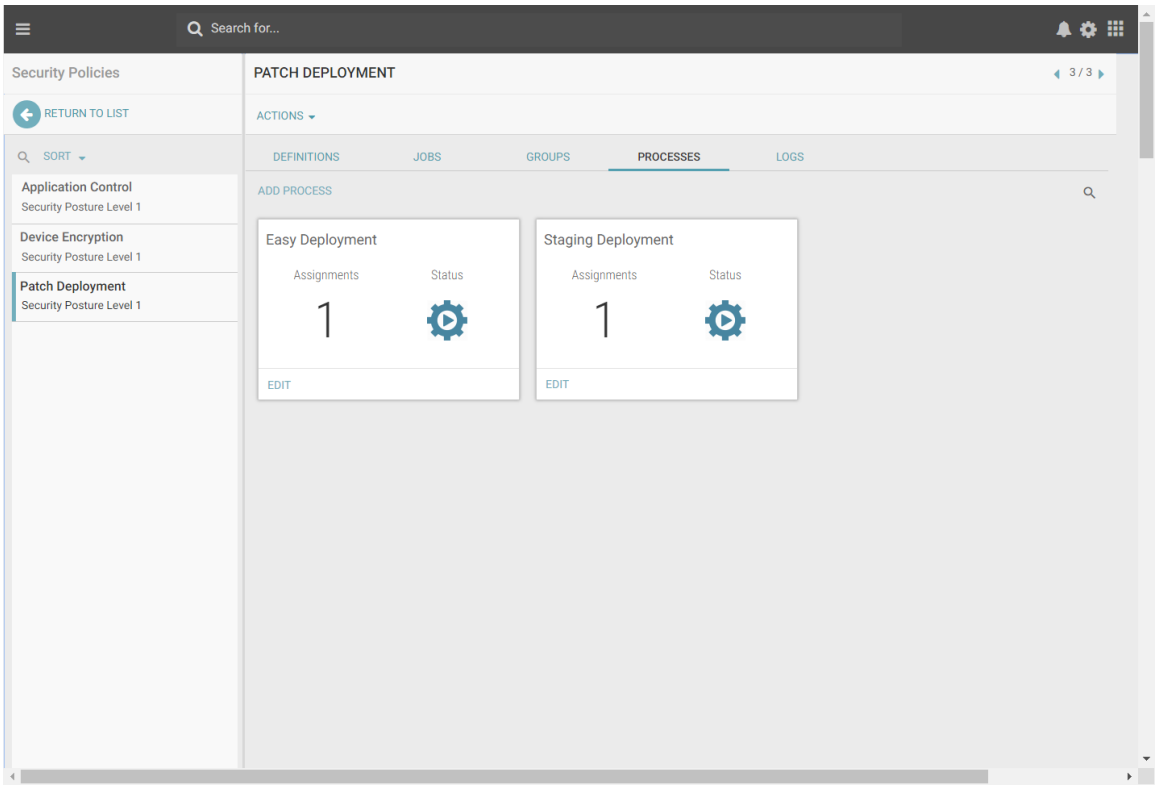
Patch Deployment Detail View - Jobs



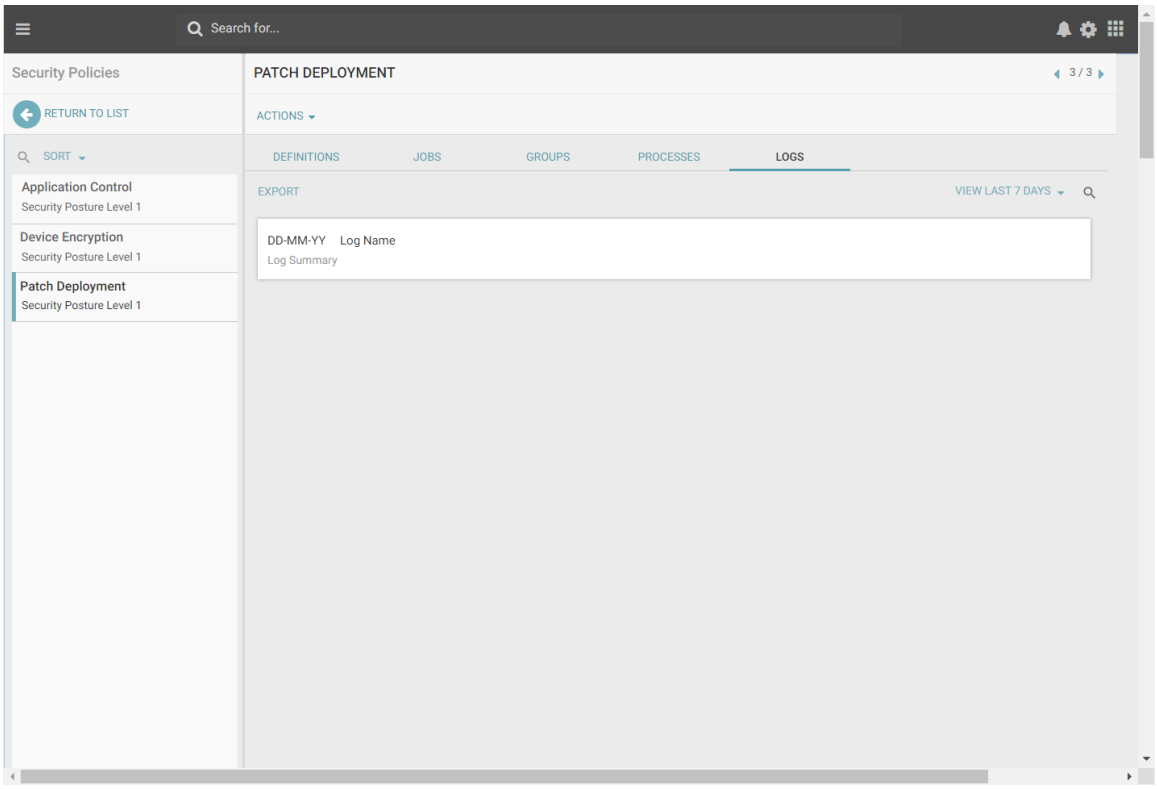
Patch Deployment Detail View – Groups



Patch Deployment Detail View - Processes

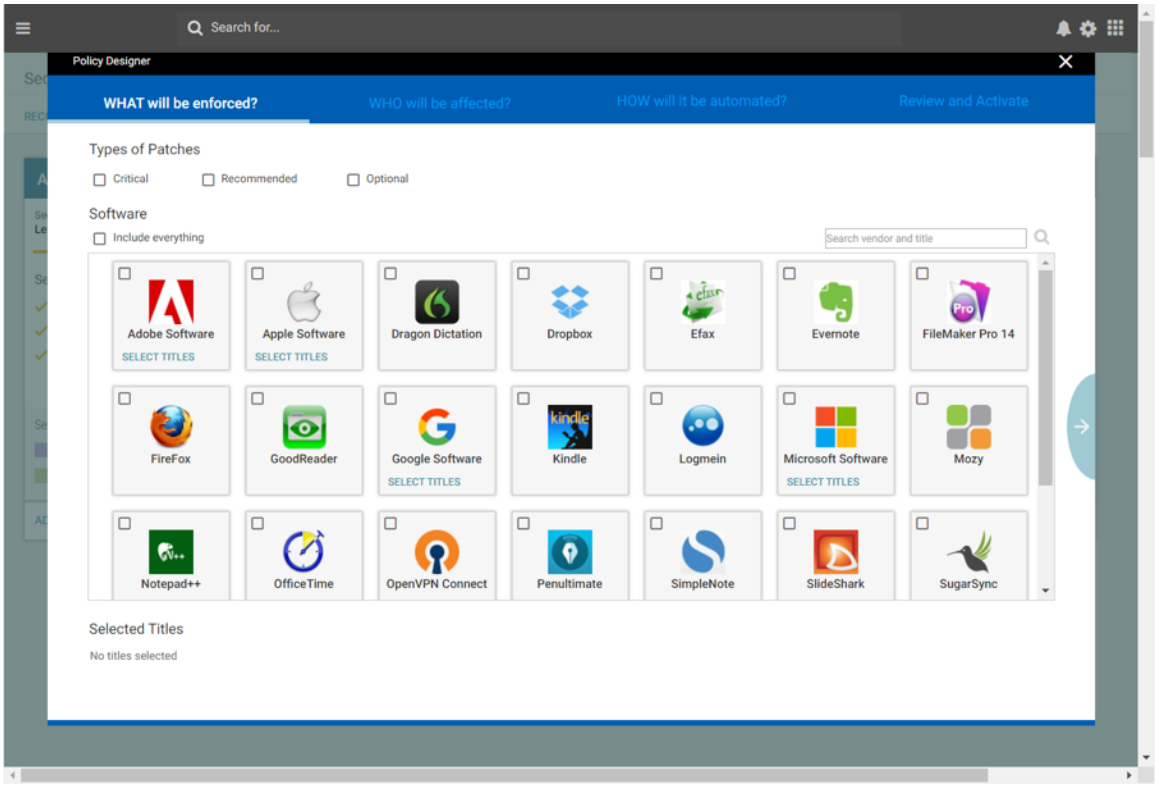


Patch Deployment Detail View - Logs

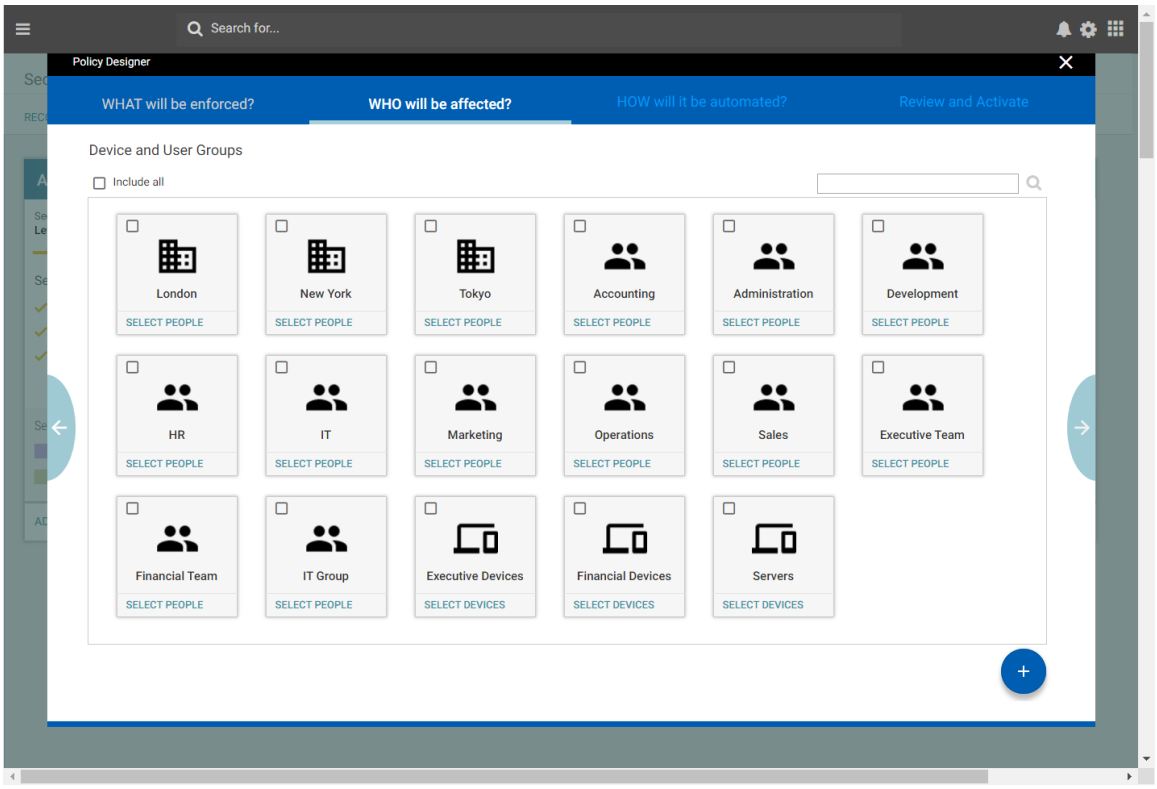


CREATE CUSTOM PATCH POLICY CASE

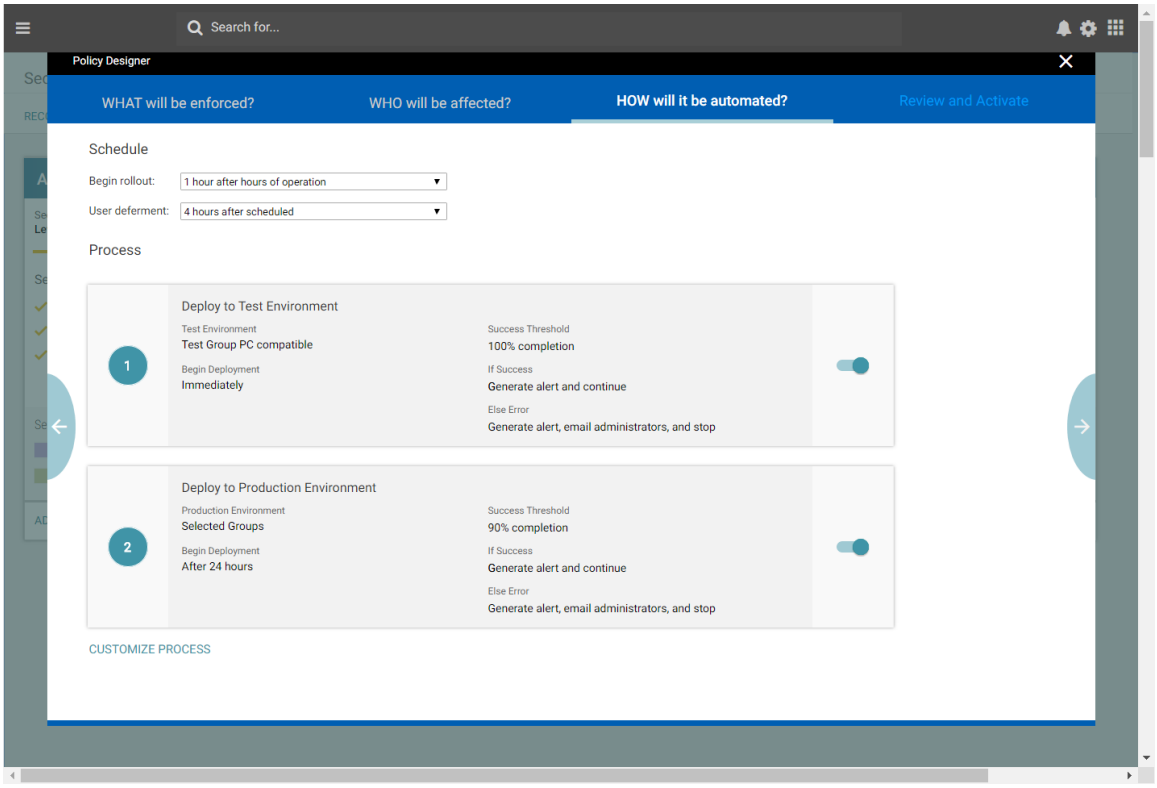
Create custom case for patch policy: WHAT



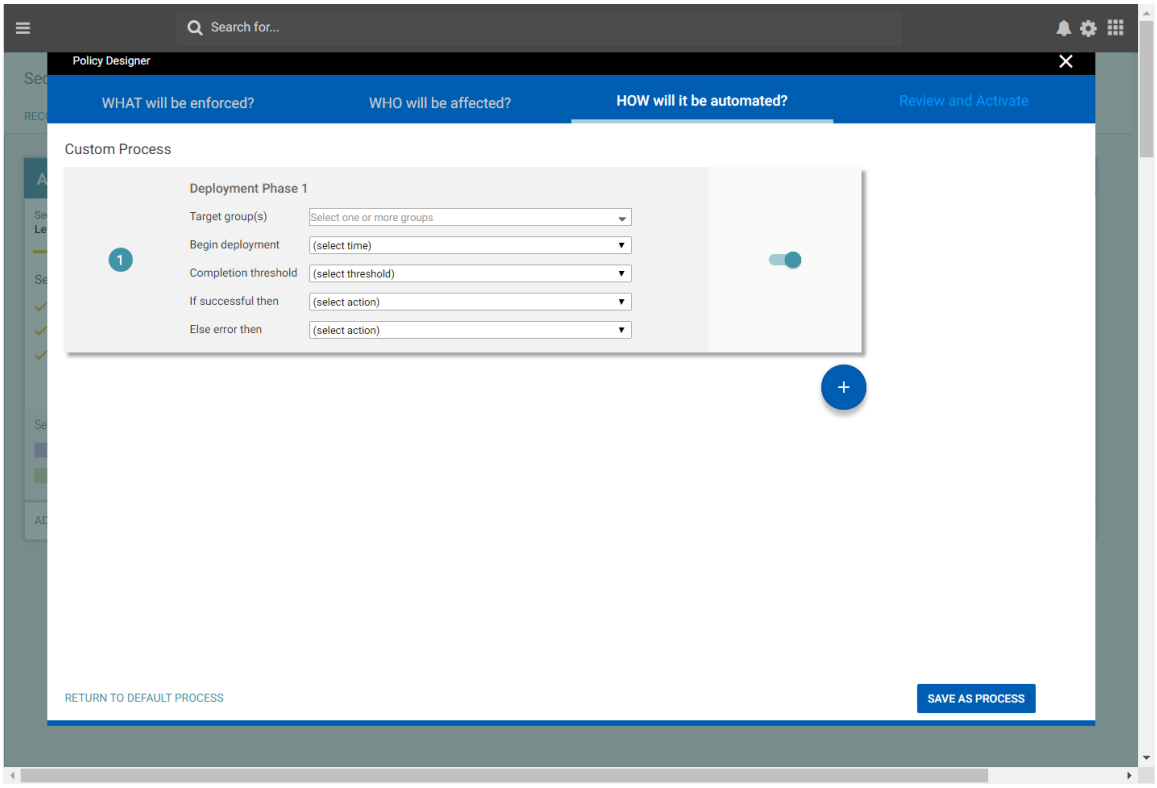
Create custom Case for Patch Policy: WHO



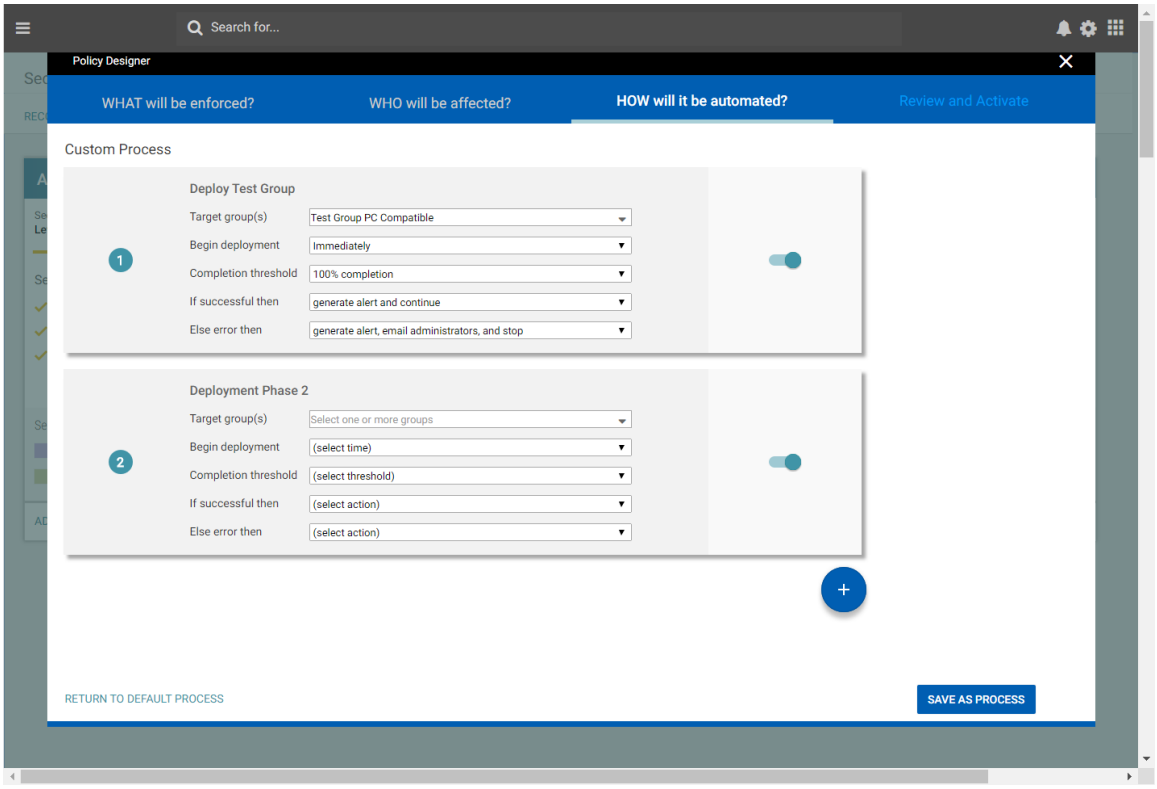
Create custom case for Patch Policy: HOW



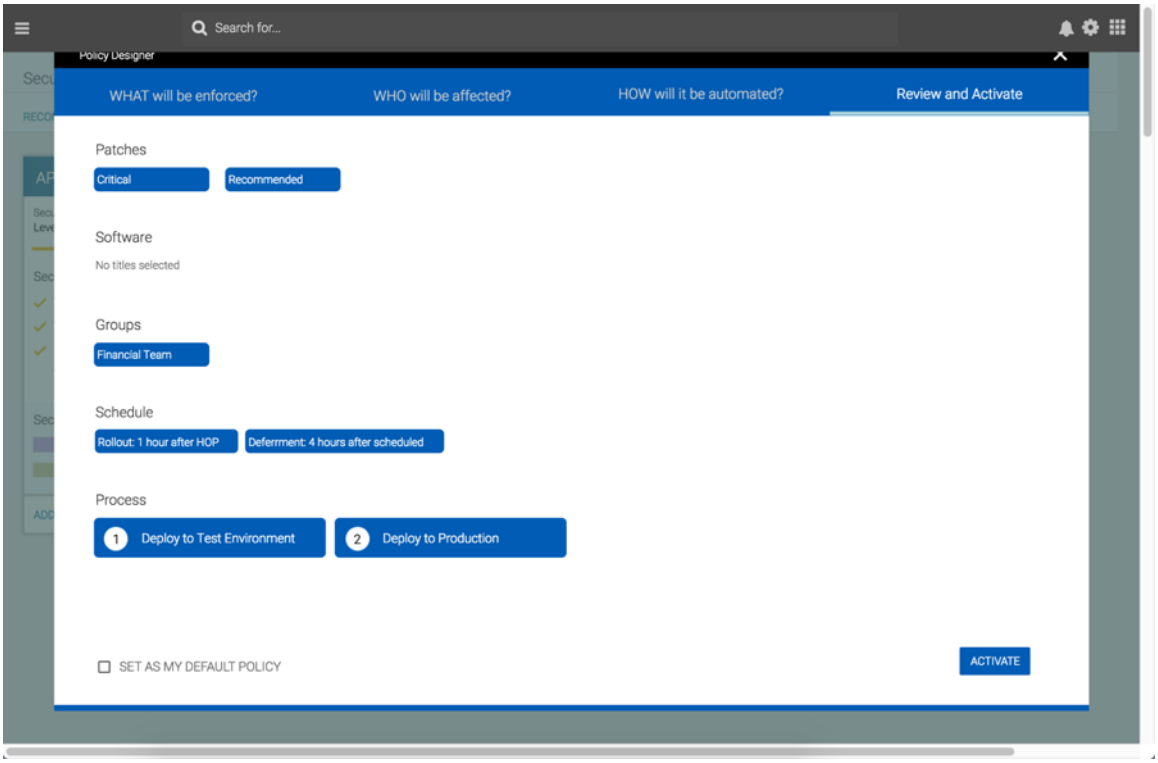
Create custom case for Patch Policy: HOW – custom process



Create custom case for Patch Policy: HOW – custom process with second deployment phase



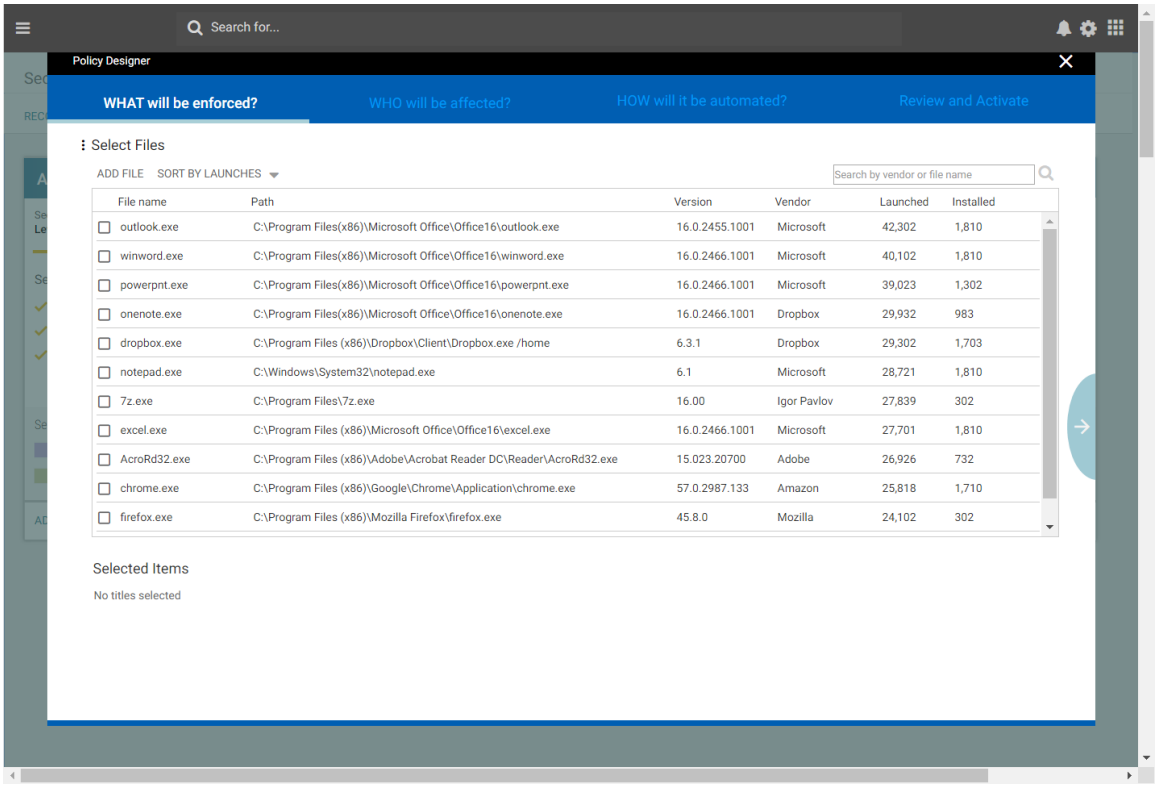
Create custom case for patch policy: Review



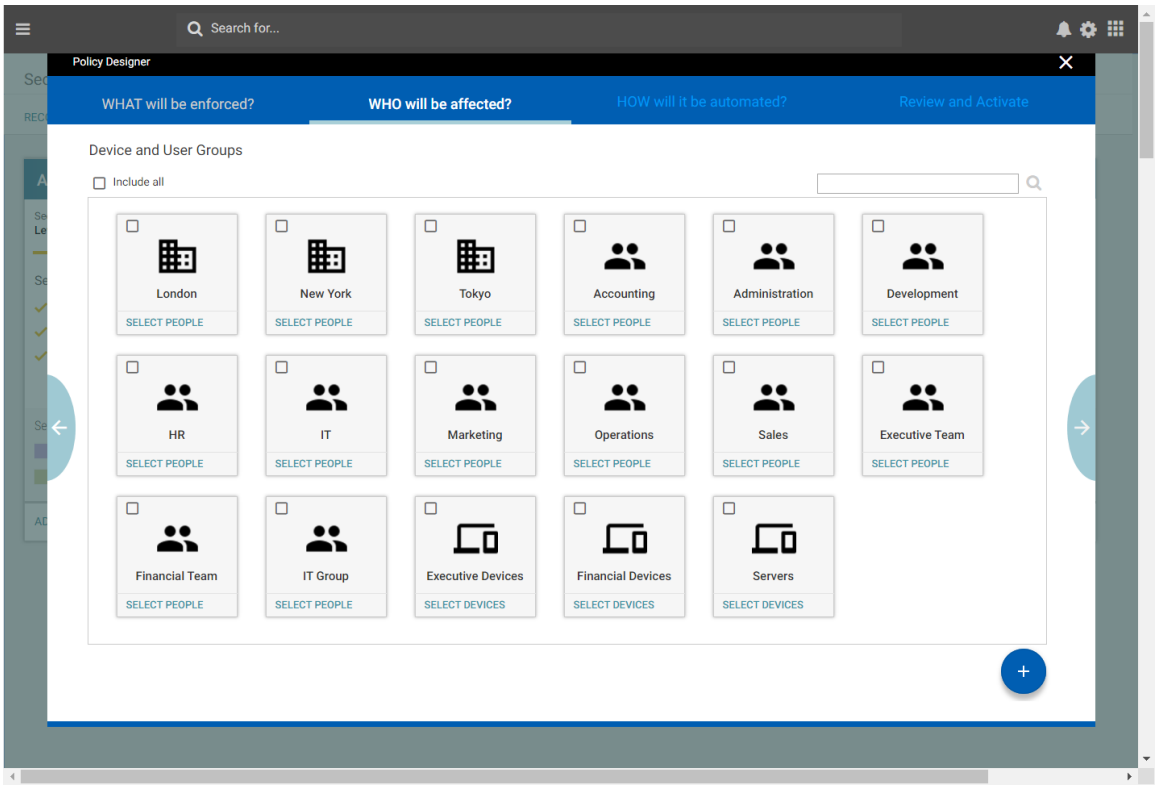
One participant remarked he would like to have this as the primary view for the custom case, so he can see everything on one page.

CREATE AC POLICY WIZARD

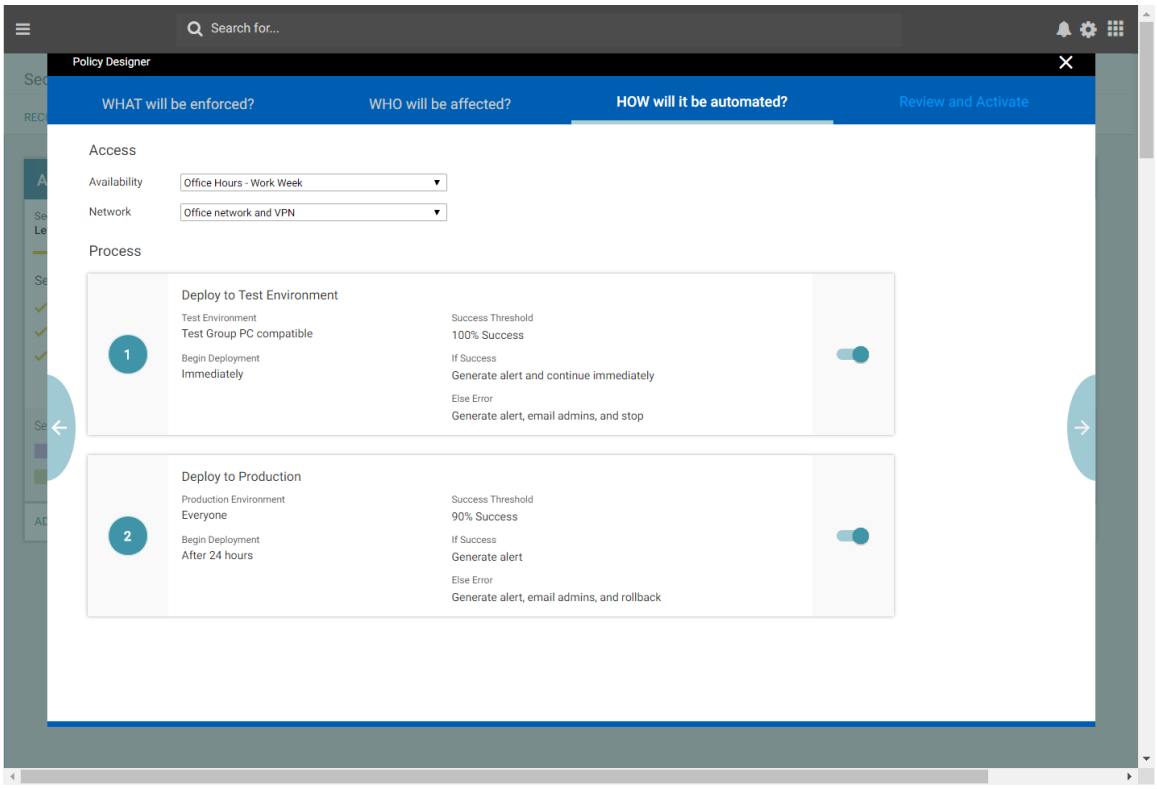
Create AC policy WHAT



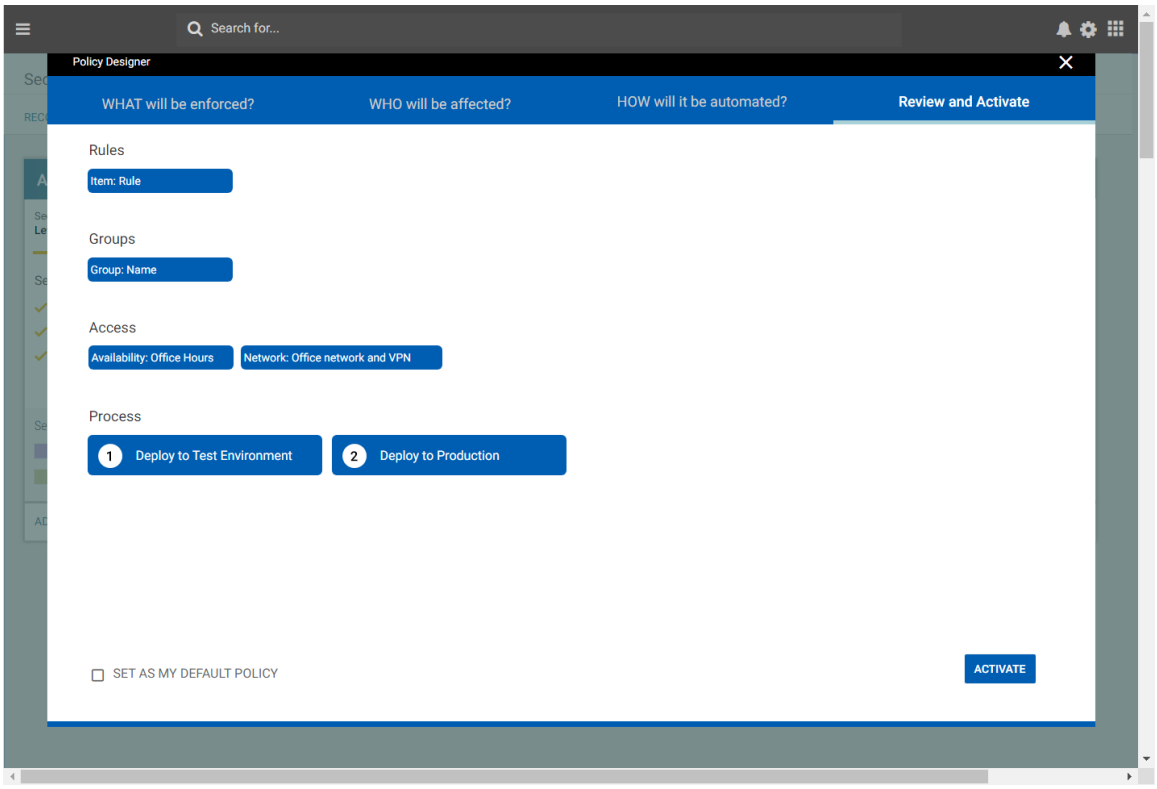
Create AC policy WHO



Create AC policy: HOW

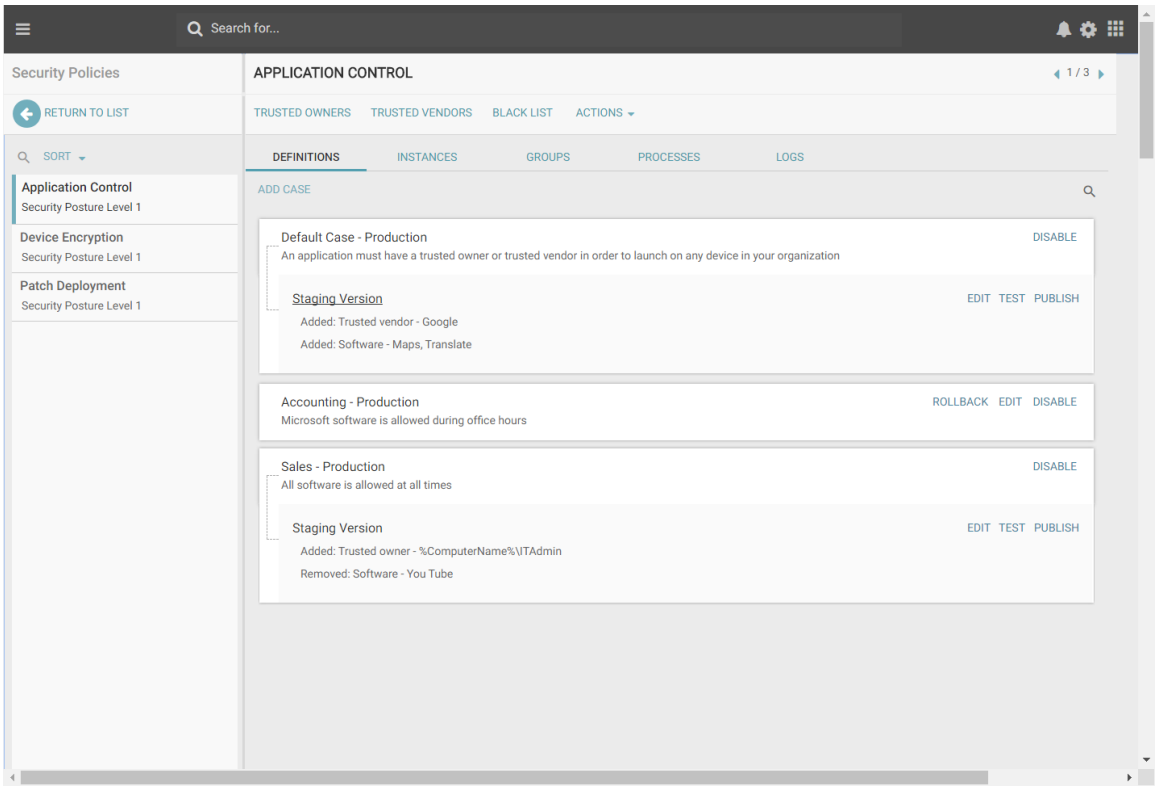


Create AC policy: Review

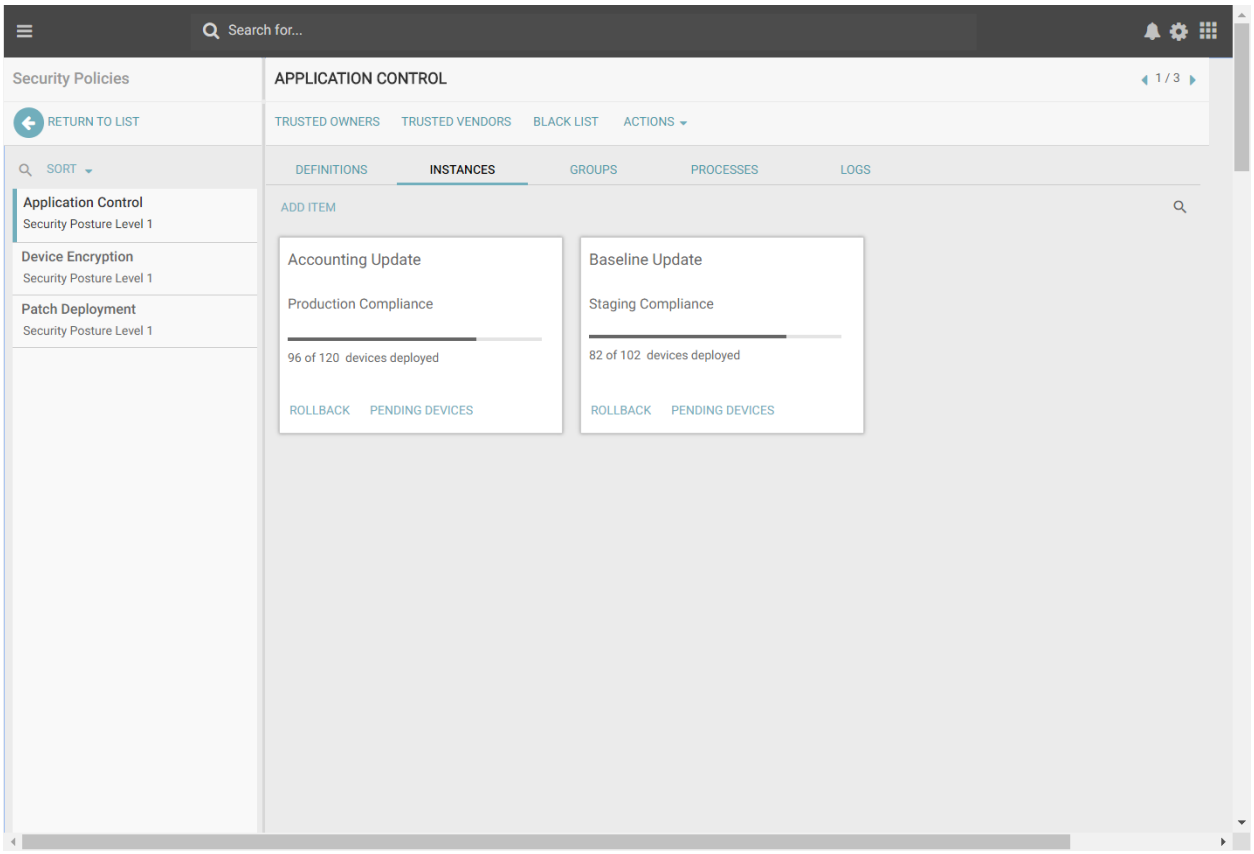


APPLICATION CONTROL POLICY DETAIL

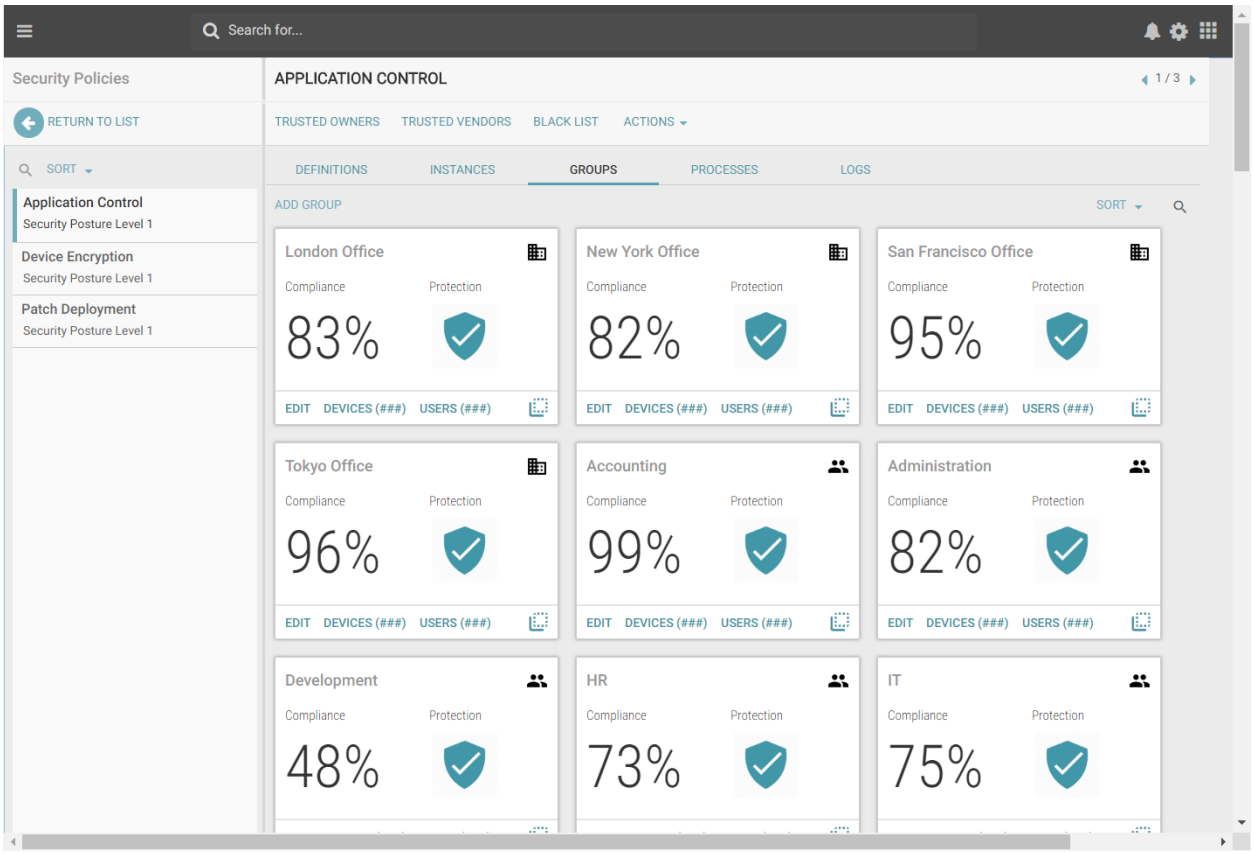
Application Control: Definition



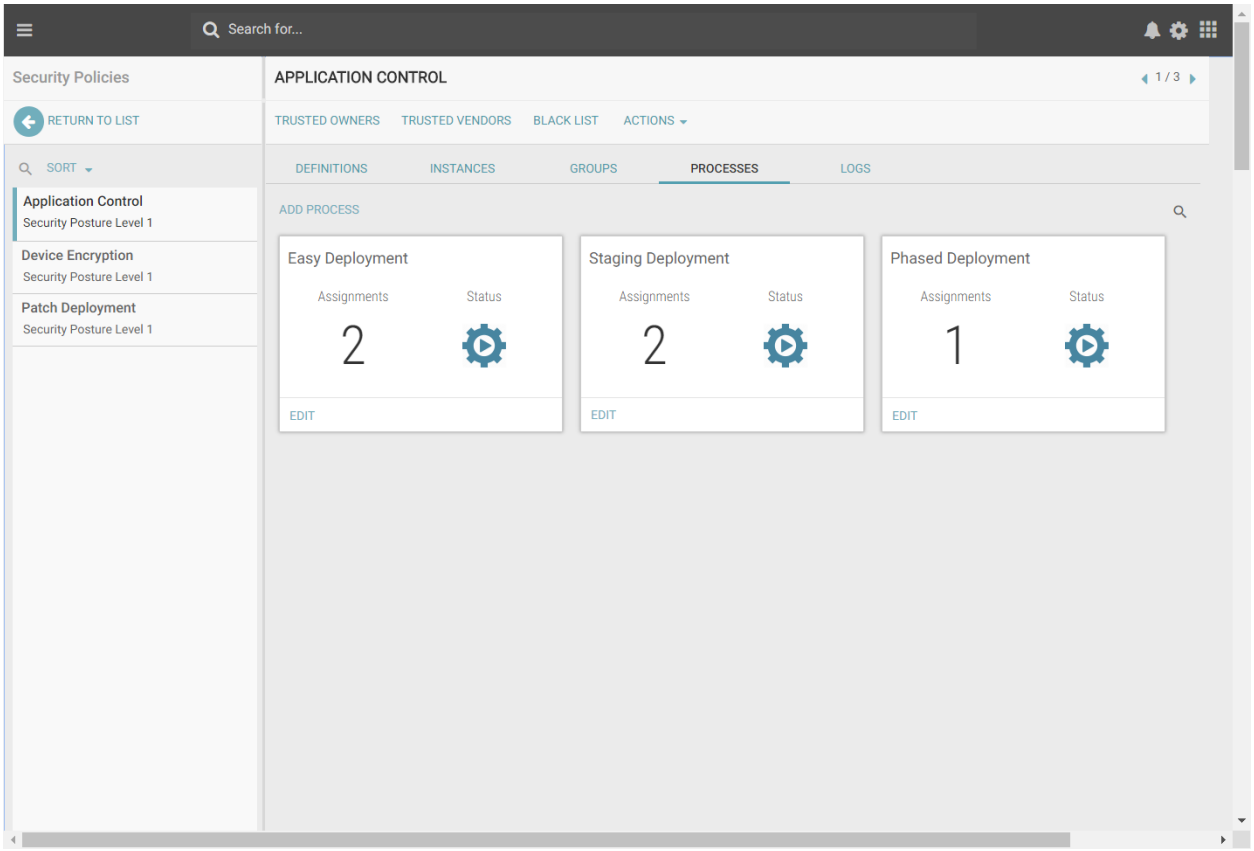
Application Control Details: Instances



Application Control Details: Groups



Application Control Details Processes



Application Control Details: Logs