

CASE STUDY - ADDING CUSTOM ROLES TO THE CARBON BLACK CLOUD

OVERVIEW

I started working at Carbon Black in late Summer of 2018. I was fortunate enough to work with a large UX team there. One bigger than I previously had the pleasure of working with. I was new to security and needed to ramp up very quickly. My teammates helped that process go smoothly

The Carbon Black Cloud product protects endpoints (computers, servers, etc.) from cyber attacks of many types. Malware, Ransomware, Trojans, etc. It does this via a sensor on the endpoint that will alert the CB user of a suspected compromise and allow an Analyst or Threat Hunter to take action

In many cases, the product will block or terminate a suspicious software action in order to protect the user. An analyst is then alerted, and they can investigate further, mark as a false positive, or take other steps within the console to remediate the problem

The issue I was trying to solve with this project was how to facilitate console Admins to create new custom roles and allow them to understand the permissions they would be providing the user when creating and assigning both default and custom roles

THE PROBLEM WITH CARBON BLACK RBAC

- Carbon Black administrative product users were unable to assign users roles with the appropriate level of permissions.
- Current user roles were not granular enough, some users had to be granted roles with more permissions than admins desired, a case of privilege escalation admins could do nothing about.
- With the addition of granular roles being a proposed part of the solution, it became clear that users wanted completely custom tailored roles they could create to assign to new and existing users. The ability to create custom roles would no longer require admins to assign an undesired set of permissions
- It was not clear to Admins which roles contained which permissions. We wanted to expose those permissions to the user. There were so many though. How could we simplify?

GOALS FOR CARBON BLACK RBAC & CUSTOM ROLES

- Prevent users from inadvertently escalating permissions by granting roles greater permissions than needed. Make users safer
- Expose the permissions granted to each role, so that admins can mitigate risk and truly understand what each role can do
- Allow administrators to simply and easily create custom roles to assign to CB users
- Allow users to create custom roles from existing roles
- Cut down on support calls and feature requests regarding what was seen as a deficient RBAC scheme, with too few roles and opaque permissions
- Increase customer satisfaction by alleviating the specific pain point of being forced to use rigidly defined overly coarse roles

THE AUDIENCE

We needed to fulfill the needs of two specific personas* within the Carbon Black Cloud.

- **Anthony** - A user who may very well only use the Carbon Black Cloud product to add users to their proper roles. Never performing the job of analyst or threat hunter
- **Marie** - Who is a frequent user of the software, but is also responsible for addressing gaps in her company's defenses. Things like privilege escalation and insider threats.

* The personas shown here are slightly later versions than the ones used for the RBAC case study. I helped the research team with the design and some development of these CB personas.

ANTHONY

Every ticket is a new opportunity for me to learn.



HELP DESK
medium law firm

AGE 24

LOCATION Newark, NJ

EDUCATION AS in IT

©2019 Carbon Black. All Rights Reserved.

☆ ATTITUDE

- Humble
- Outgoing
- Multitasker
- Eager to learn

📋 TASKS

- Troubleshoot the tickets I can fix:
 - Get the wifi and printers back up
 - Reset your password when you lock yourself out
 - Reinstall software
 - Give clear instructions for issues employee can fix
- Contact employees for more information about their tickets

🎯 GOALS

- Understand enough to know which tickets to escalate and which to take
- Quickly fix and close my tickets
- Keep various employee systems up and running
- Build my technical skills and knowledge

INFOSEC

TECHNICAL

EXPERIENCE

PRODUCT USE

API KNOWLEDGE

IN MY OWN WORDS...

I love software and gadgets, but it's the combination of tech and people that I really like. I'm the front line support. When someone's close to panic about their machine, it feels great to be able to help them out.

MARIE

Come at me -- you really think I won't find you?



THREAT HUNTER
large biotech firm

AGE 35

LOCATION Chicago, IL

EDUCATION BS in CS

©2019 Carbon Black. All Rights Reserved.

☆ ATTITUDE

- Determined
- Insightful
- Level headed
- Strategic
- Competitive — game on!

📋 TASKS

- Look for suspicious behavior -- clues can be subtle, especially when I have to piece together the full picture
- Understand the full extent of a threat
- Address gaps in company defenses
- Monitor security vulnerabilities

🎯 GOALS

- Outsmart the bad guys
- Quickly identify unusual patterns
- Fully understand any threats
- Recognize all security vulnerabilities

INFOSEC

TECHNICAL

EXPERIENCE

PRODUCT USE

API KNOWLEDGE

IN MY OWN WORDS...

Attackers can be very creative — their techniques are constantly changing, and it's my job to thwart them before they can do any damage. I make sure to know this organization like the back of my hand, I monitor the news, and ground myself in fact. I know an attack is coming — it's my job to make sure I recognize it when it does.

THE RBAC & CUSTOM ROLES TEAM

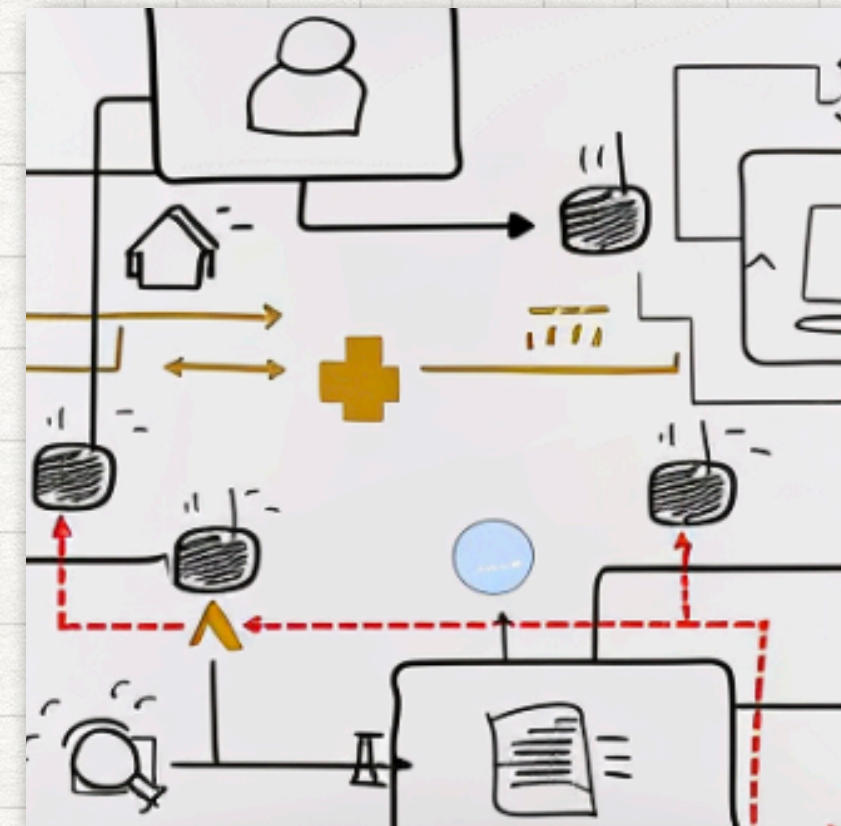
When I started at Carbon Black, I was initially assigned to several small one-off type projects, but soon was assigned to a specific product team. This RBAC project was my first with this team, and I really wanted to make a good impression. The challenges being an extremely truncated timeline, an unclear design vision, and starting with a new team for a high pressure project.. I did not yet know the personalities of my new teammates. The scope was such, that it would affect every customer using the Carbon Black Cloud product. We dove right in on the complex issue together and soon things began to become clearer. For the next couple of years I would work with this team exclusively and I really appreciated and learned from each team member.

- Chris Brewer - Software Architect
- David Getman - Product Manager
- Spencer Nowak - Front End Developer
- Je Suis Encreatia - Front End Developer
- Niccolo Salvatore - Back End Developer
- Julia Slopak - Quality Assurance Engineer
- Mark Madden - Lead UX Designer

FIRST STEPS

- The day I was assigned the project, David, Chris and I began to **whiteboard** the relationship of legacy and new roles and noted how they mapped to specific sets of permissions. In later conversations, being informed with our **personas**, we reached out via **surveys** to get a better baseline idea of what our users truly needed and had experienced previously
- During this time I created the initial **workflows** in Miro for the project. I documented the existing journey and the journey we hoped would allow for greater control of the role based access control feature for our users.

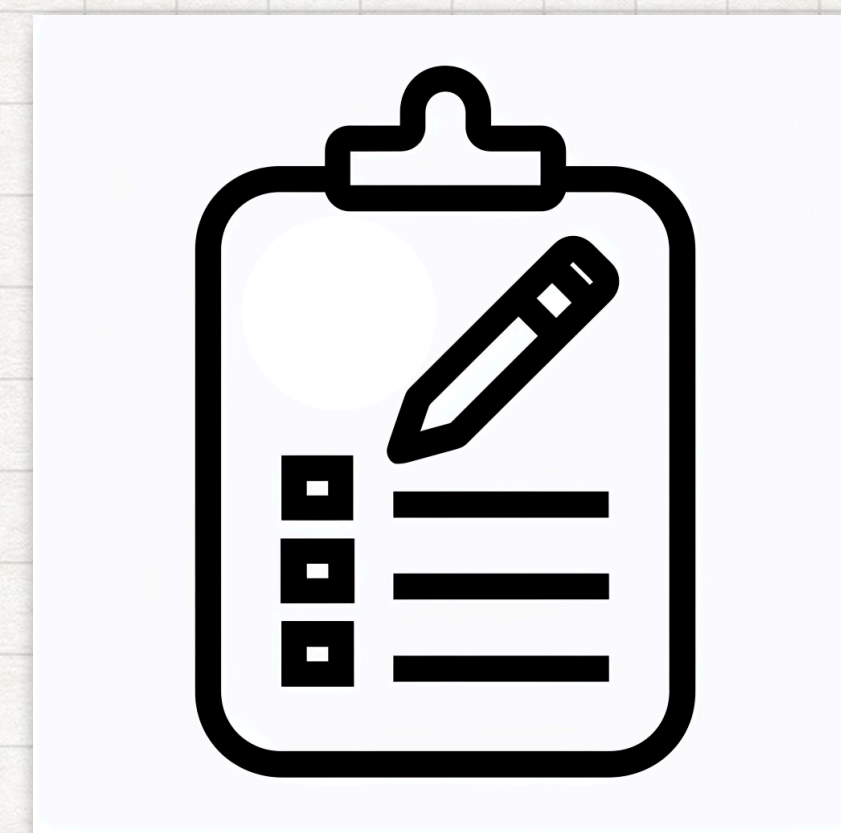
1



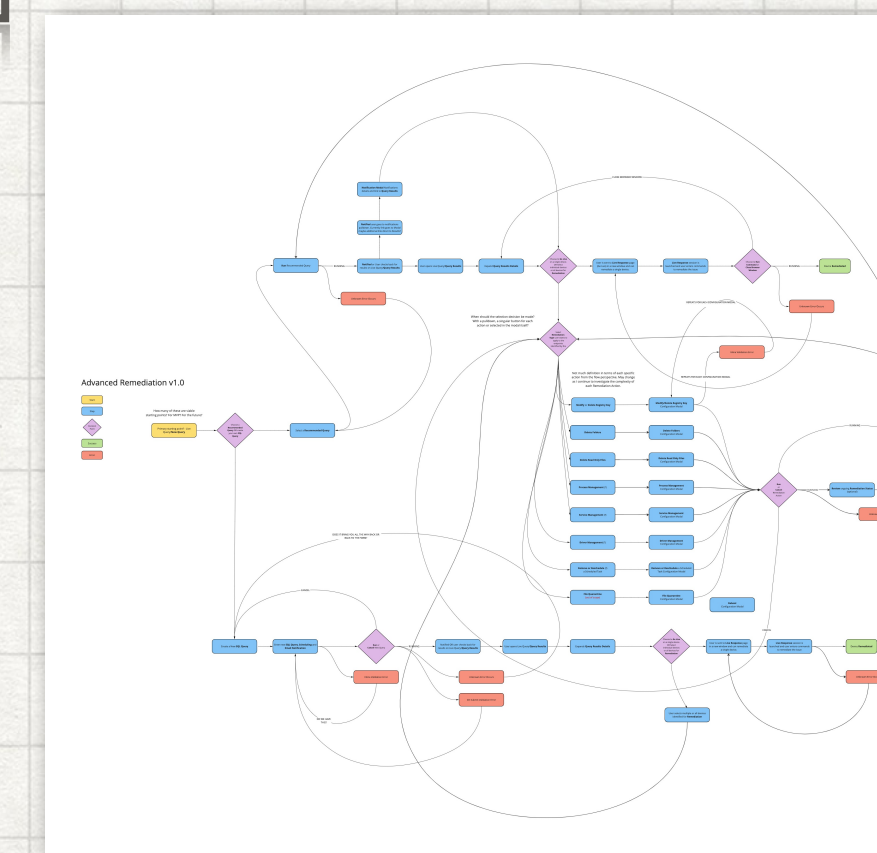
2



3



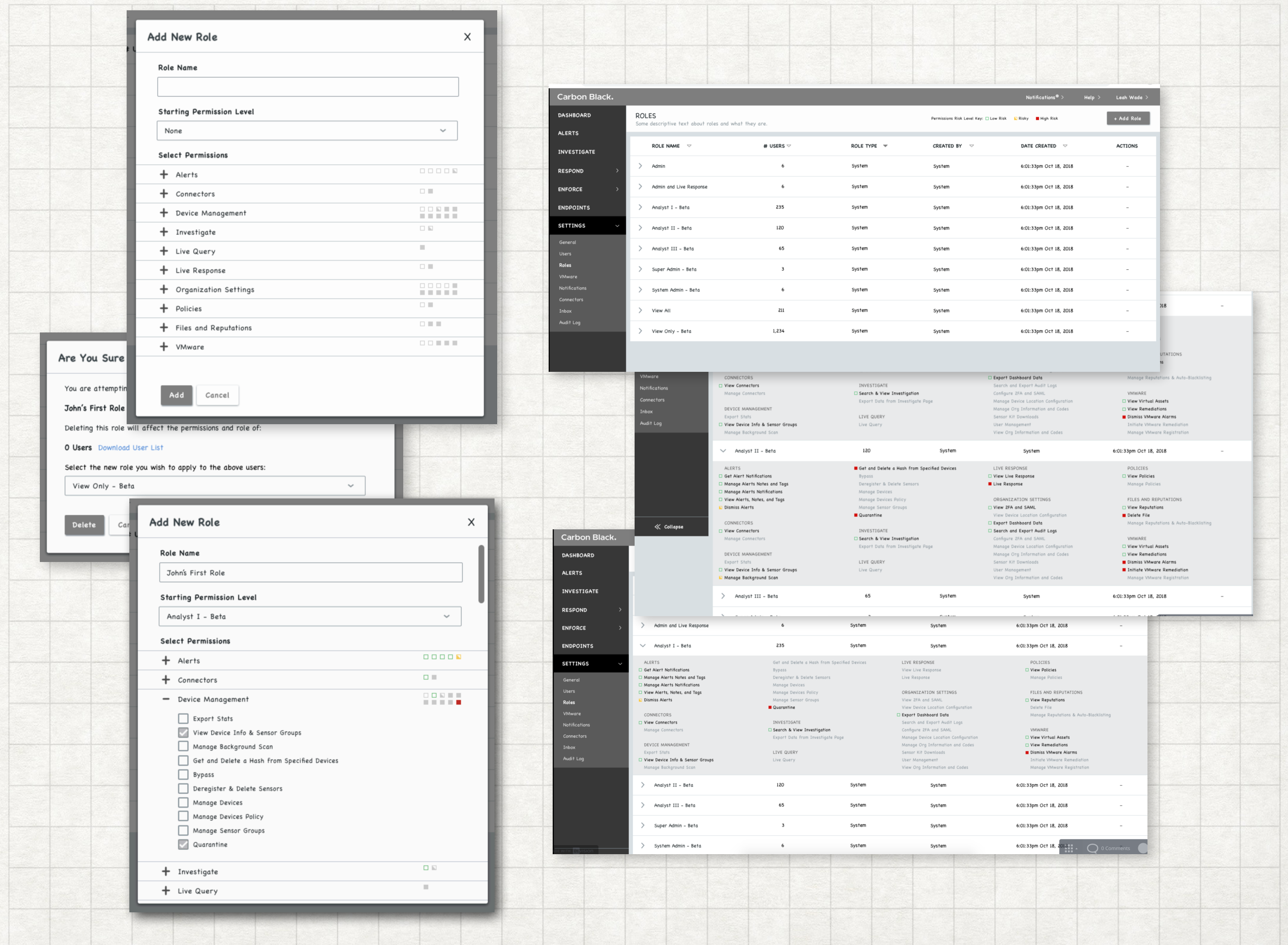
4



NEXT STEPS - WIRE FRAMING

The team identified and discussed the problem together. We examined the current state of the Carbon Black Cloud as it related to RBAC and the support cases it had created. We asked questions through tools like surveys and structured interviews.

Once we had interpreted the data and results we had gathered, I was able to begin wire framing solutions. Ideas flowed freely as we iterated to come to the best solutions to solve the issues our users had experienced.



NEXT STEPS - USABILITY TESTING

Once I had created a few rounds of initial wireframes, we needed to test our assumptions. We achieved this via online, researcher guided, usability tests. Subjects were asked to complete tasks like adding roles, deleting roles, identifying risks by permission and role, creating custom roles from an existing template and from scratch. As users worked their way through the Figma prototypes I created, we saw some notions confirmed and some ideas discarded as a result of these tests.

“I WOULD REALLY LIKE A DESCRIPTION RATHER THAN JUST THE ROLE NAME, TO ALLOW SOMEONE TO ALLOW ADDITIONAL CLARITY ON WHAT THE CUSTOM ROLE IS AND HOW IT DIFFERS. IF THERE’S A LOT OF TURNOVER IT WILL ALLOW PEOPLE TO CATCH UP QUICKLY”

— Participant 1

“I DEFINITELY LIKE THAT THERE WAS A STARTING PERMISSION LEVEL FIELD. I WAS KIND OF NERVOUS THAT I WASN’T GOING TO HAVE THAT CAPABILITY AND I’D HAVE TO PICK ALL THE PERMISSIONS. WAY EASIER THAN RECREATING A ROLE EACH TIME”

— Participant 2

“THE ONES WE CARE MOST ABOUT ONES THAT GRANT THE TYPES OF PERMISSIONS THAT COULD CHANGE SYSTEM LEVEL SETTINGS. WE DEFINITELY WOULDN’T WANT ANYONE TO JUST DO THAT AND ACCIDENTALLY CHANGE SOMETHING THAT SHOULDN’T BE CHANGED AND CHANGE THE WHOLE SYSTEM”

— Participant 5

CONCLUDING STEPS - REVISION, IMPLEMENTATION, QA, BETA, GENERAL AVAILABILITY

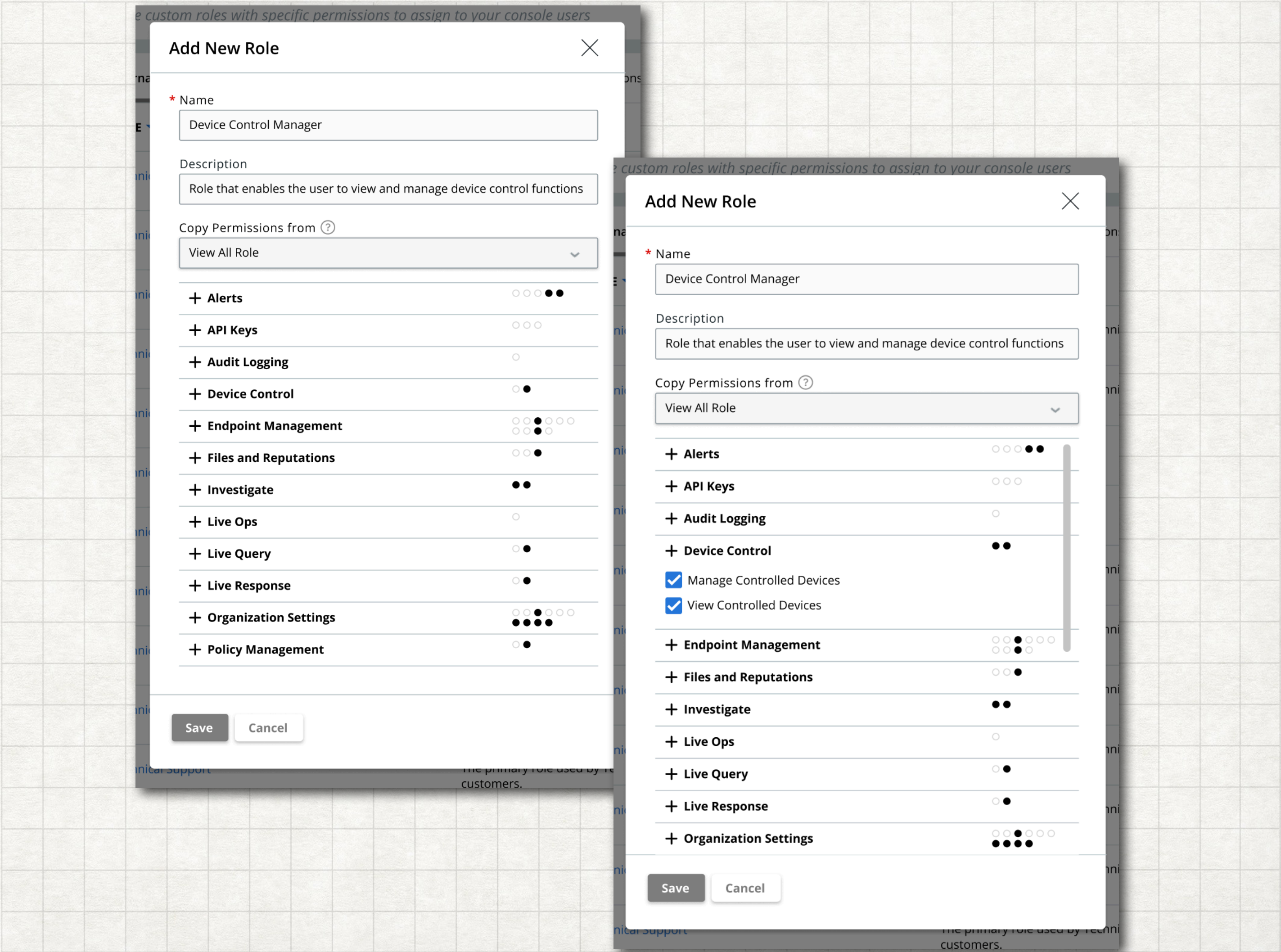
We translated user test results into actionable tasks, then I set to work on the final look and feel. Operating within the design style and component system constraints and armed with the tangible results from user testing, the final pieces began to fall into place.

I worked directly with Je Suis and Spencer on the front end development and implementation of the feature. We collaborated on the final state and disposition of the RBAC components with an eye toward accessibility.

During QA, I worked with Julia to make sure we had considered all the ways the user might escalate privilege and find any bugs or regressions before the release.

We performed both Closed and Open Beta releases and made final adjustments based on user feedback at each step.

GA!



OUTCOMES

- We learned our users did not want us assigning risk levels to permissions. They wanted to determine the level of risk regarding a particular permission themselves
- We increased the number of default roles from 3 to 7. Allowing for much finer grained role assignment choices. This met most of our customer's needs for everyday product use
- We were able to obfuscate the number of individual permissions so users could have control over their permission choices without navigating an unreasonable amount of permissions and noise. We tied related sets of permissions to a single product visible permission. Simplifying the number of permissions users were confronted with from ~160 down to 43
- We presented each role with its related permissions in a way admins could compare and contrast them easily and allowed those roles to serve as templates for new custom roles
- Customers liked and could easily understand the new custom roles feature. However, we learned that our customers were likely only to adjust these settings a few times a year and only for about 10% of their workforce
- Support calls regarding Carbon Black Cloud RBAC dropped to almost zero, freeing up support personal, and reducing COGs
- A highly requested upgrade was successfully shipped!

THANK YOU!

**"THIS IS WHAT I WAS LOOKING FOR...CREATE A NEW ROLE USING A
DEFAULT ROLE** AS A TEMPLATE SO I DON'T NEED TO CREATE ONE FROM
SCRATCH, AND THEN JUST REMOVE/ADD."

— *Participant 1*

Mark P. Madden

talorien@yahoo.com

508.277.8561

Portfolio - www.markpmadden.com

LinkedIn - www.linkedin.com/in/mark-madden-287108

More about CarbonBlack - www.carbonblack.com