

# Product + Design

---

A little about me, my work history,  
and two case studies.

**Justin Barr Young**

November 2019

Website: [jbarr.co](http://jbarr.co)

Email: [justin@jbarr.co](mailto:justin@jbarr.co)

# About me

I'm a design-driven product manager for web and mobile experiences. I specialize in translating complex domains – like cybersecurity and web hosting – into friendly user experiences for startups and enterprise companies alike. I started my career as a **designer** and transitioned into **product management**. For over a decade, I've been working, learning, and mentoring in the sweet spot where design thinking, technology, and business meet.

I've written, talked, and presented on subjects such as product development, Agile design, chatbots, and how to improve UX process in small teams.



**What I like:**

Talking to users

New business domains

Honest prioritization

Complex systems

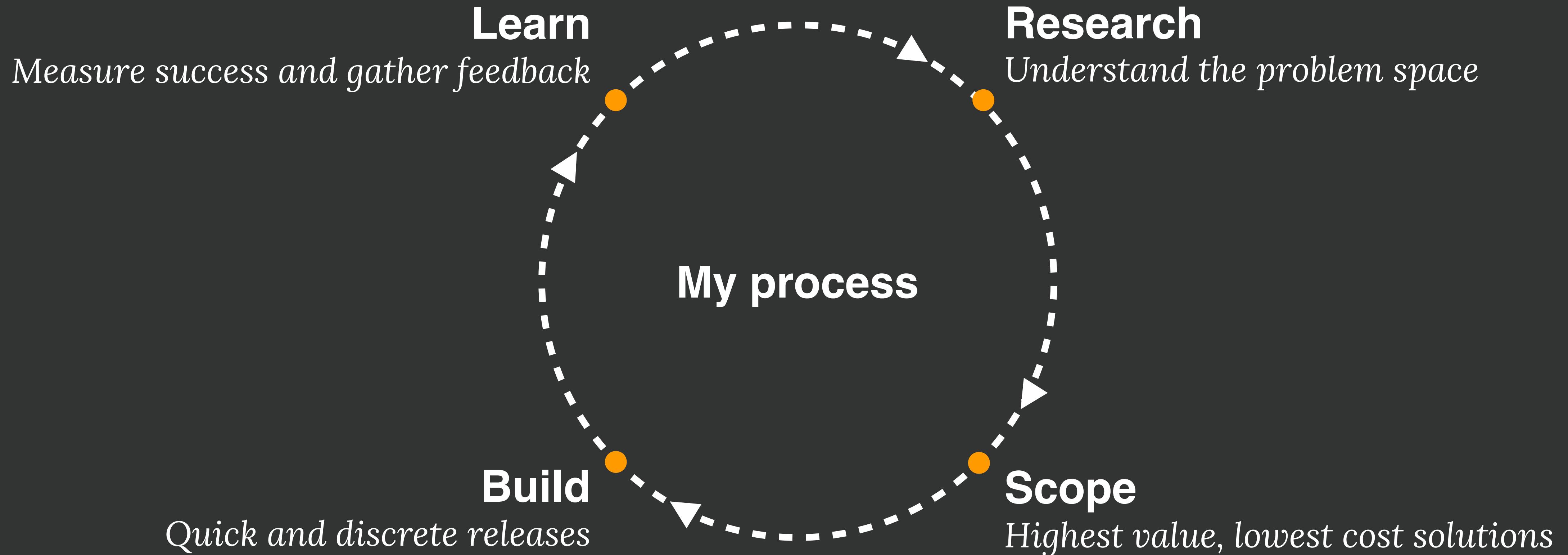
**What I value:**

Cross-functional teamwork

Focusing on business value

Iterative design

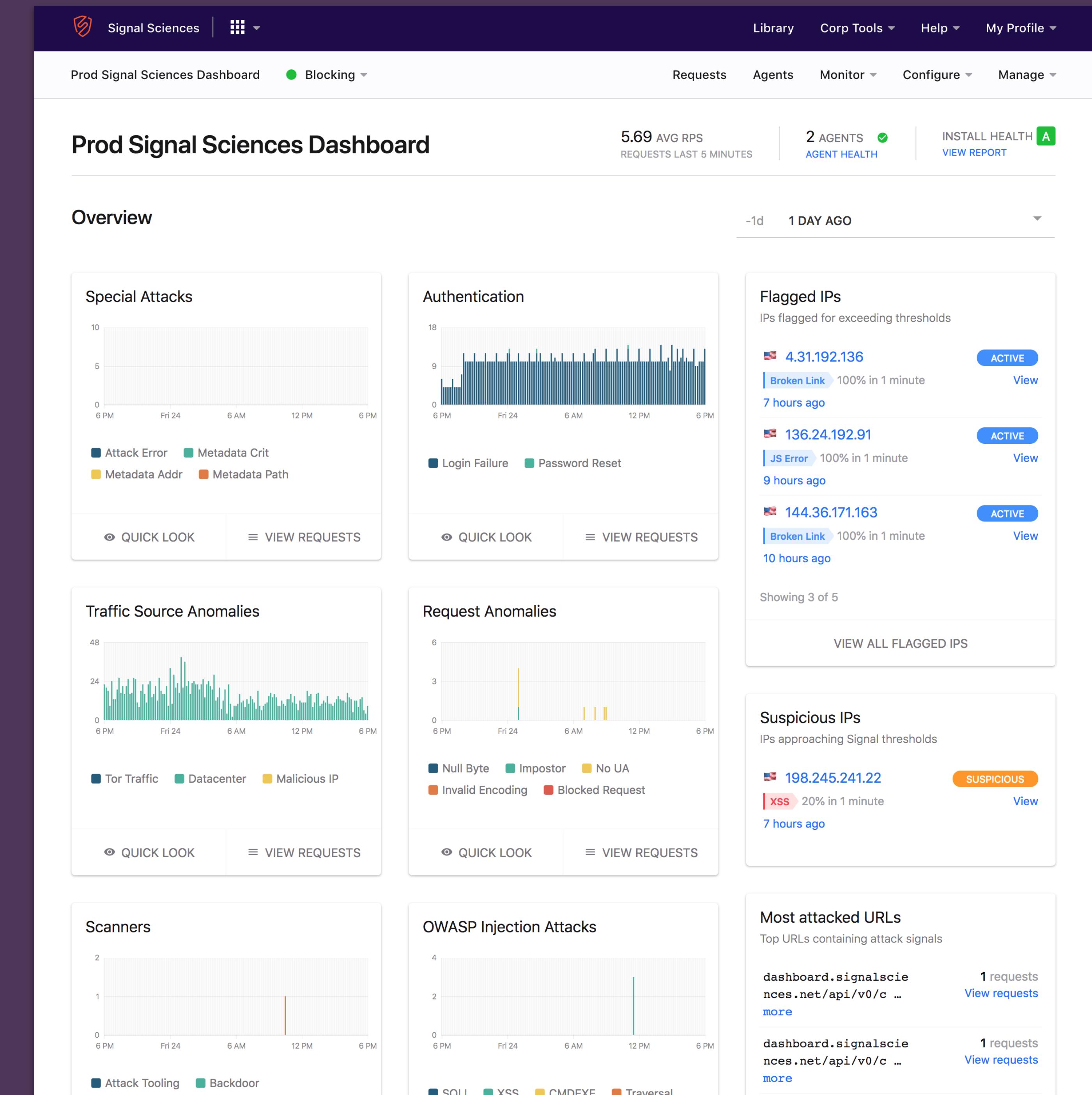
Open and regular feedback



# Signal Sciences

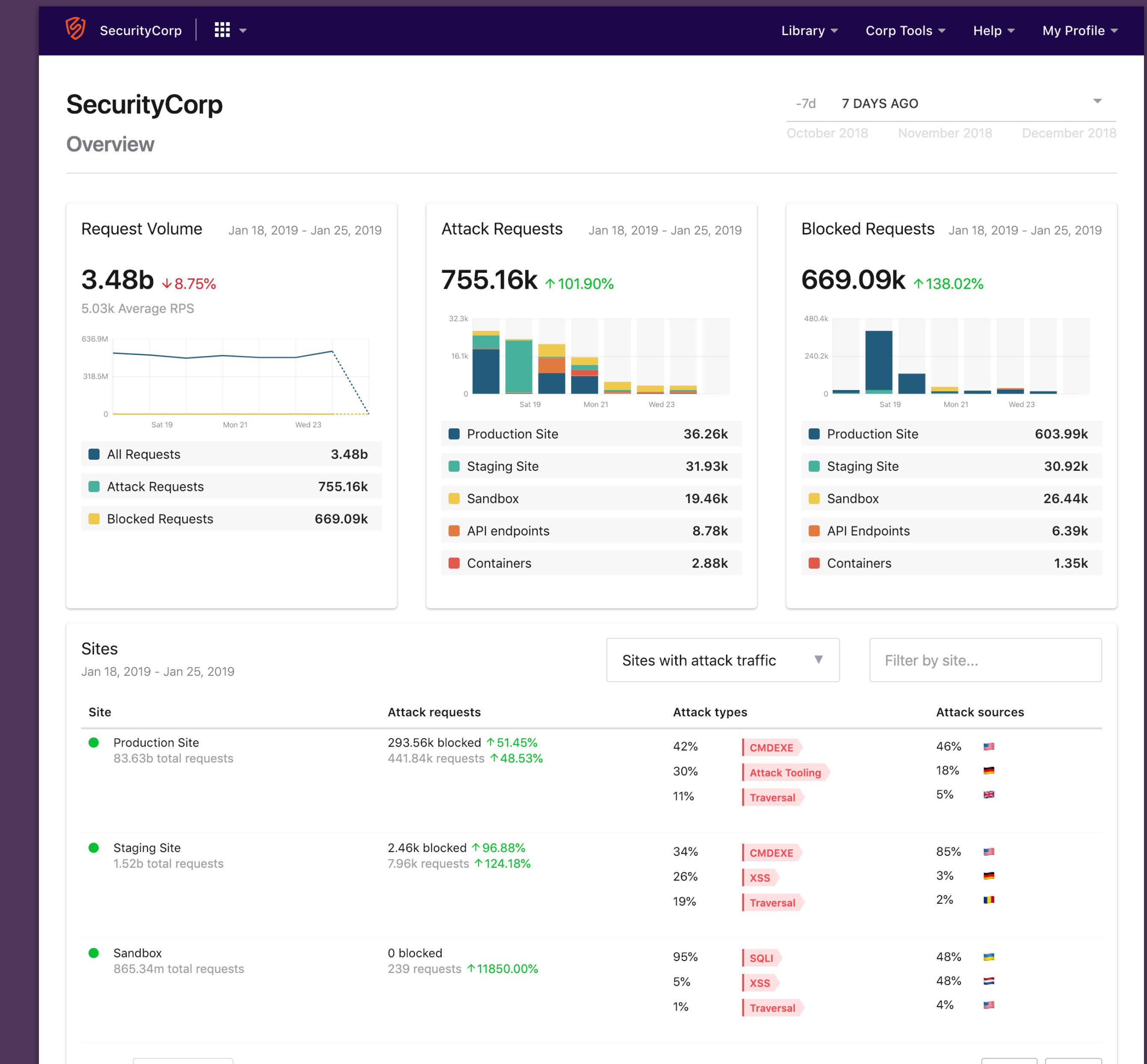
Signal Sciences is a cybersecurity SaaS platform that monitors customers' sites, apps, and online properties for hacking attempts and malicious traffic, and provides actionable data for security teams. The product is recognized by customers and industry experts, including Gartner, for its ease-of-use.

- Currently Product Manager
- Started as Product Designer
- Focused on account and domain management, user customization, and enterprise scalability



# As product lead

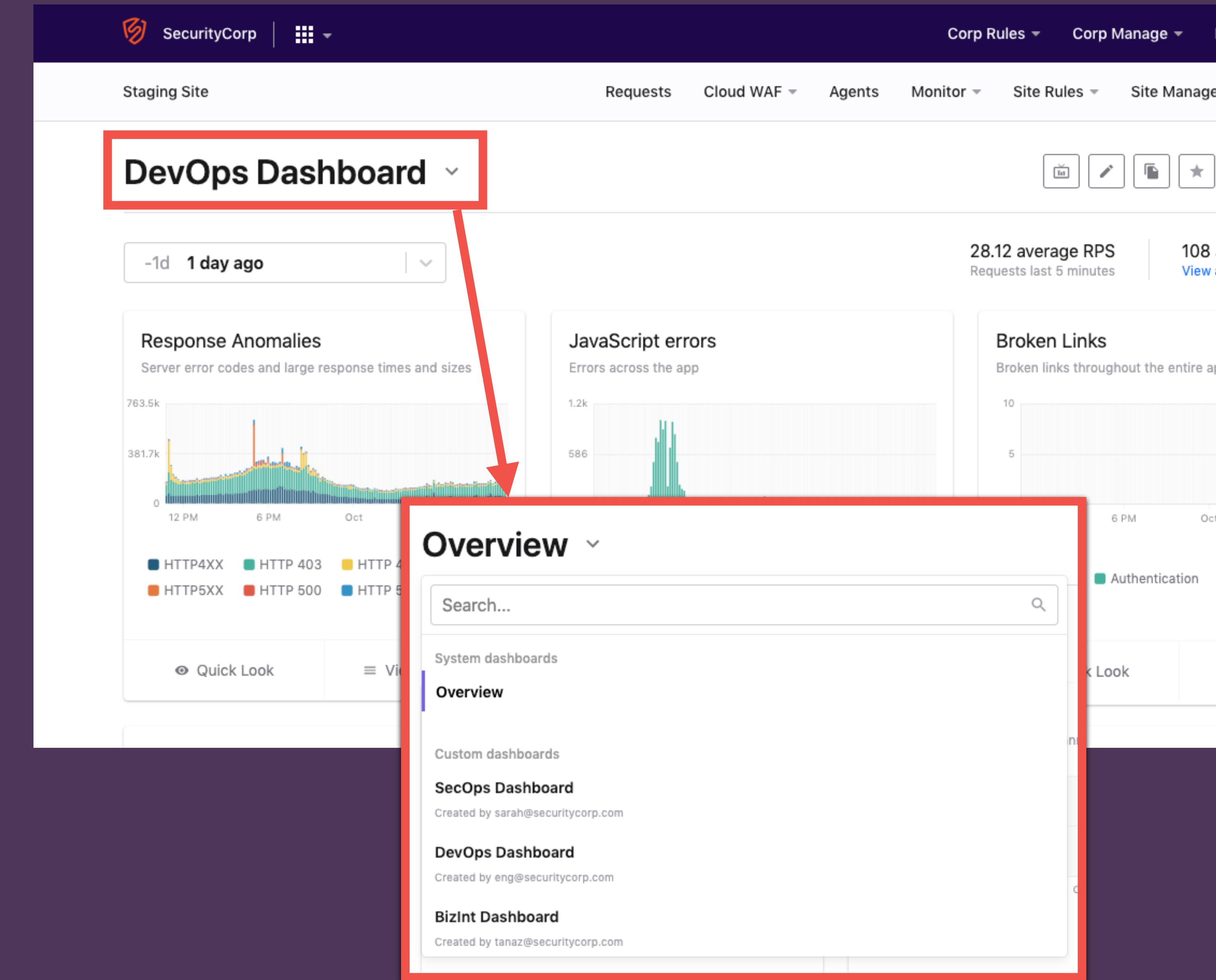
- Manage feature roadmaps for the management console as well as multiple strategic programs, like:
  - International data privacy
  - Managed resellers
  - Third-party integrations
- Product owner for multiple cross-functional development teams
- Redesigned roles and permissions scheme, enabling multi-site features
- Created process training curriculum for teams and employees
- Led Customer Advisory Board feedback sessions



Read more about this feature: [corp overview page](#)

# As design lead

- Principal designer for majority of the management console
- Full-stack design: ideation, wireframing, prototyping, testing
- Created industry-first “attack story” feature, increasing sales conversion ([case study #1](#))
- Redesigned console navigation to scale and improve access to high-value features ([case study #2](#))
- Defined user analytics standards across design, product, tech teams
- Reduced customer support tickets 12% through UI improvements



Read more about this feature: [multiple custom dashboards](#)

# Carbon Five

Carbon Five is an Agile design and development consultancy that embeds with startup and enterprise clients to build products and mentor effective teams.

- Design lead for 8 client projects
- Early-stage product validation and prototyping
- Rapid iteration, continuous delivery, and TDD
- Mentored enterprise teams on Agile design transformation
- Managed design backlogs



Carbon Five is a digital product development consultancy. We partner with our clients to create exceptional products and grow effective teams.



Square



Asian  
Art  
Museum



SFMOMA



alt school



charles SCHWAB



Disney



NATIONAL  
GEOGRAPHIC



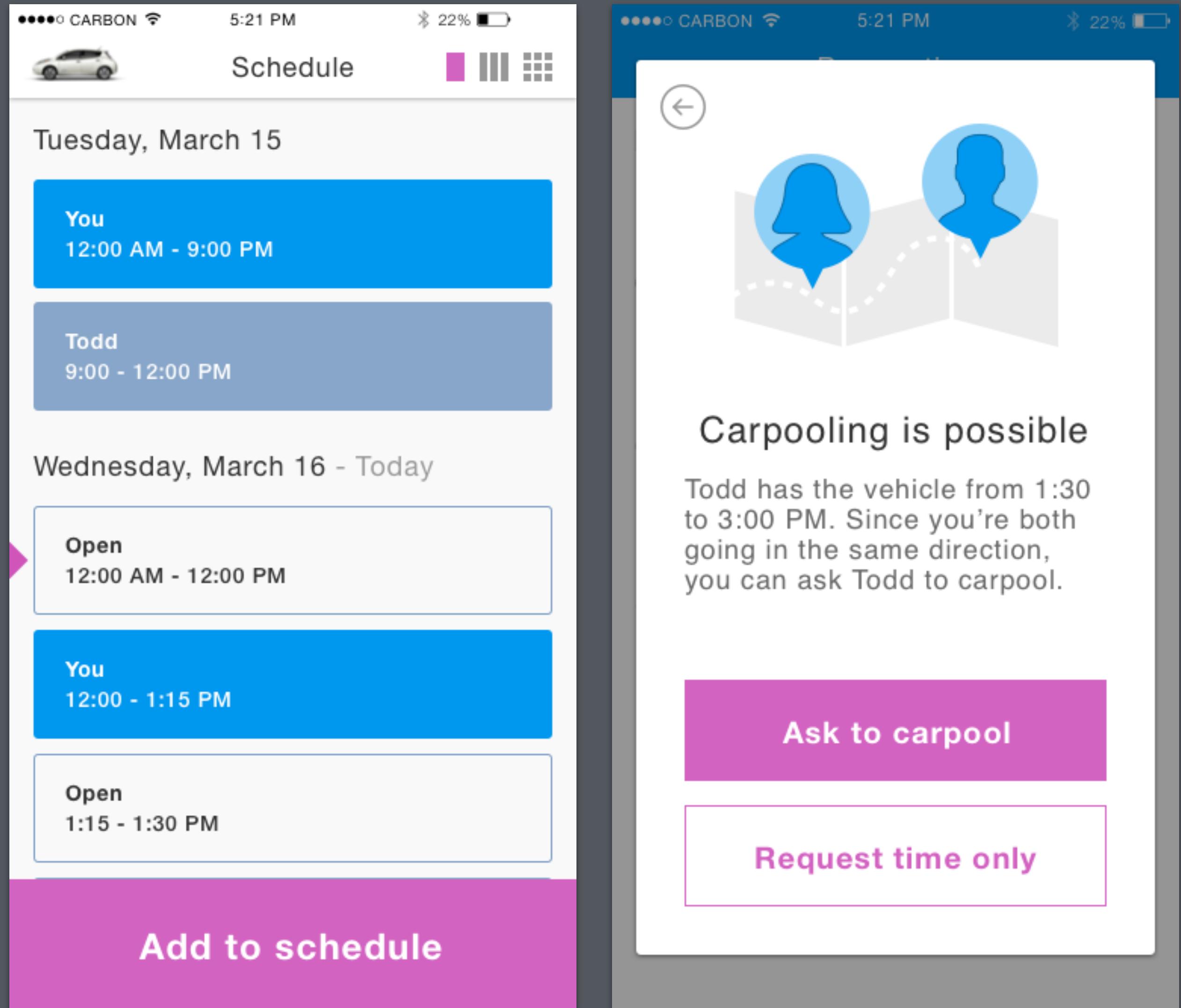
GRAND ROUNDS

[See what we've done](#)

# Nissan

Carbon Five partnered with Nissan to test an early-stage car sharing product concept. The auto manufacturer wanted to learn how two or more parties might co-own a car.

- Designed real-world experiment
- Recruited 50 families to record schedules and driving habits
- Gave families vehicles and tracked driving behavior for a month
- Built dashboard to analyze data
- Conducted customer interviews
- Prototyped car-sharing app



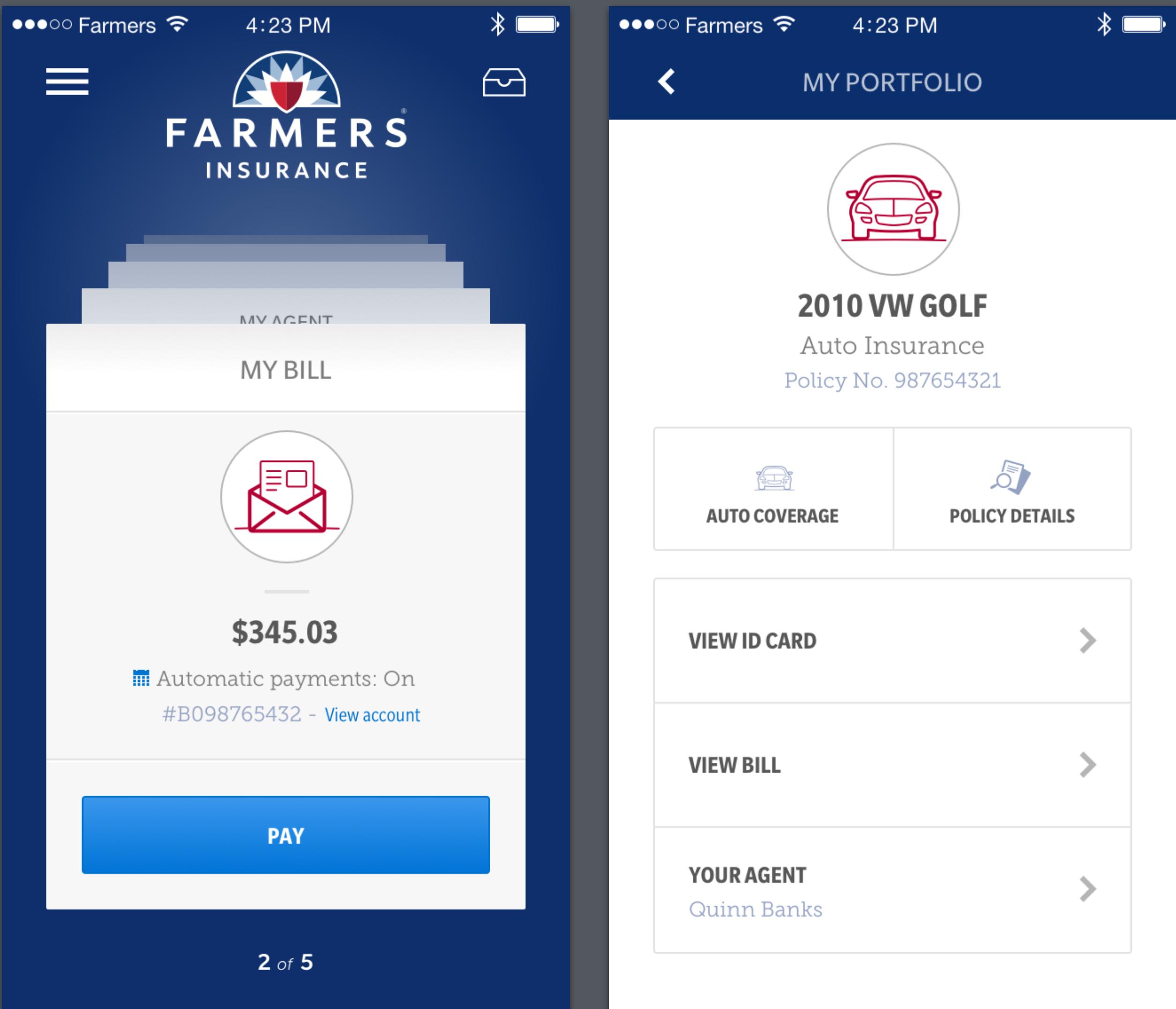
Read the [full case study](#)

# Farmers

---

Carbon Five partnered with Farmers to rebuild both its Android and iOS apps and train its brand new mobile development team in Agile process.

- Created style guide that was compatible across both operating systems and every design size
- Established Design Ops practices
- Knowledge transfer to developers
- Mentored junior designers
- *Did not visually design the app*



Read the [full case study](#)

# Media Temple

Media Temple is a web hosting and cloud solutions provider.

- Principal UX Designer
- Started as a UX Engineer
- 5 products launched and improved UX across 8 others
- Redesigned and rebuilt award-winning website and account dashboard with over 1 million combined monthly users
- Contributed to responsive framework and component library

Hello, Justin.

Account Number: 228719

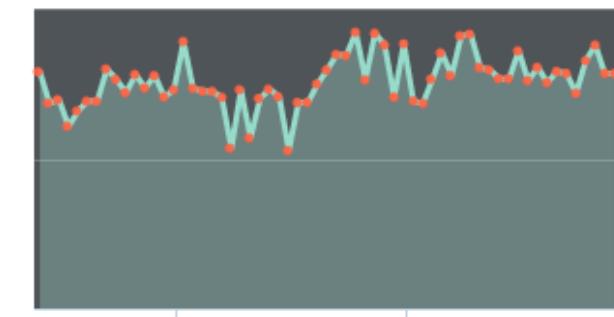
**BILLING**

**MONITORING**

Monitor up to 5 domains

jay-bee-why.com

Response Time over last hour (GMT):



See all monitoring reports »

**Security**

jay-bee-why.com

Malware scan, Site vulnerability scan, Spam scan

Last scan: Jul 20

Manage Security »

**ADD A DOMAIN**

**LIST ALL DOMAINS**

**ADD-ON SERVICES**

Service Name	Service Type	Plan	Renewal Date	ADMIN
CloudFlare	All	Free	N/A	ADMIN

**CLOUDTECH SERVICES**

Hosting Service	Parent Service	Plan	Renewal Date
Security Pack for Always-On	fully-managed-ux.com	\$0	Aug 4, 2015
CloudTech Always-On Essential	fully-managed-ux.com	\$199	Aug 4, 2015

**WANT FREE HOSTING?**

Looking for free hosting? You get one more month's free hosting for every person you refer. [Learn more.](#)

# Case study #1

## Events feature

I redesigned Signal Sciences' Events feature, which lists and describes hacking attempts against a customer's service.

- Introduced usability and navigation improvements
- Focused on event narrative and providing context
- Created industry-first “attack timeline” feature
- Aligned business logic, UI, and data model
- Highlighted customer value

The screenshot shows the 'Events' section of the Signal Sciences platform. At the top, there is a navigation bar with links for Overview, Requests, Agents, Monitor, Configure, Site Settings, and Blocking. A green dot icon next to 'Blocking' indicates it is the active tab. Below the navigation is a breadcrumb trail: Sites > MySite > Monitor > Events. The main area is titled 'Events' and features a map of Eastern Europe and Russia. Two specific IP addresses are flagged: '80.11.22.33' (marked with a red flag) and '111.111.11.11' (marked with a blue flag). To the left of the map is a list of recent events:

IP Address	Signal	Status
80.11.22.33	xss	ACTIVE
80.11.22.33	Traversal	ACTIVE
80.11.22.33	Attack tooling	ACTIVE
80.11.22.33	xss	EXPIRED
80.11.22.33	Attack tooling	EXPIRED
80.11.22.33	xss	EXPIRED
80.11.22.33	xss	EXPIRED

A modal window for the flagged IP '111.111.11.11' is open, showing details like Status: ACTIVE, IP: 111.111.11.11, Signal: XSS, and Action taken: Blocking all requests from this IP. It also notes that requests will be monitored for 24 hours until January 15, 2017, at 04:59pm. Buttons for Remove flag now, Whitelist IP, and Blacklist IP are available. Below the modal is a 'Timeline' section with a series of icons and corresponding event details:

- IP was flagged with XSS and Traversal on the Network. Within the last 24 hours.
- IP marked Suspicious on this site with XSS. January 15, 2017, 4:52 PM GMT.
- 10 requests tagged XSS from this IP within 10 minutes. 100% of site threshold (View Rule).
- Flag applied to IP. January 15, 2017, 4:48 PM GMT.

# Problems:

- Navigation didn't provide enough contextual information to be useful
- Details of event were out of order and hard to parse
- Business logic relationships were not clear: *what's the relationship between an "event," a "flag," and an "attack"?*
- Valuable and proprietary insights into an attack were a competitive advantage but poorly articulated

The screenshot shows a web-based security monitoring tool. At the top, there are navigation links: Dashboards, Configurations, Blocking, Help Center, and Luxury Retreats. The main title is "Luxury Retreats / Events". Below this, a section titled "Events Last 30 days" displays a list of 27 events, each showing an IP address, the action taken ("was flagged"), and the time it was lifted. To the right of this list, specific details for the first event (IP 149.210.238.145) are expanded:

- 149.210.238.145 was flagged**  
Flag lifted 20 hours ago.
- Who we flagged**  
149.210.238.145  
149-210-238-145.colo.transip.net
  - Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map\_codes)
  - Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:Port Check)
  - Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:getinfo)
- Why we flagged it**  
We saw 105 relevant tags across 105 requests from this IP in 60 sec.
- Attack Tooling** 100%
- When we flagged it**  
We flagged this IP on Jun 13, 2017 at 20:22 UTC.  
The flag was lifted 24 hours later on Jun 14, 2017 at 20:22 UTC.
- What actions did we take**  
While this IP was flagged, we blocked 2420 requests.

Red annotations with arrows point to specific sections:

- An arrow points to the "Flag lifted 20 hours ago" text with the question "Am I still under attack?"
- An arrow points to the "Attack Tooling" progress bar with the question "What does this mean?"
- An arrow points to the "When we flagged it" section with the question "What are my next steps?"
- An arrow points to the bottom of the event list with the question "Which events are still in progress?"

## New summary component

**Status:** ACTIVE

**IP:** — 192.168.0.100

**Signal:** | Attack Tooling

**Action taken:** 51 requests blocked from this IP while flagged

Requests will be monitored for 23 hours until the flag is lifted on June 2, 2018, 4:10 PM PDT

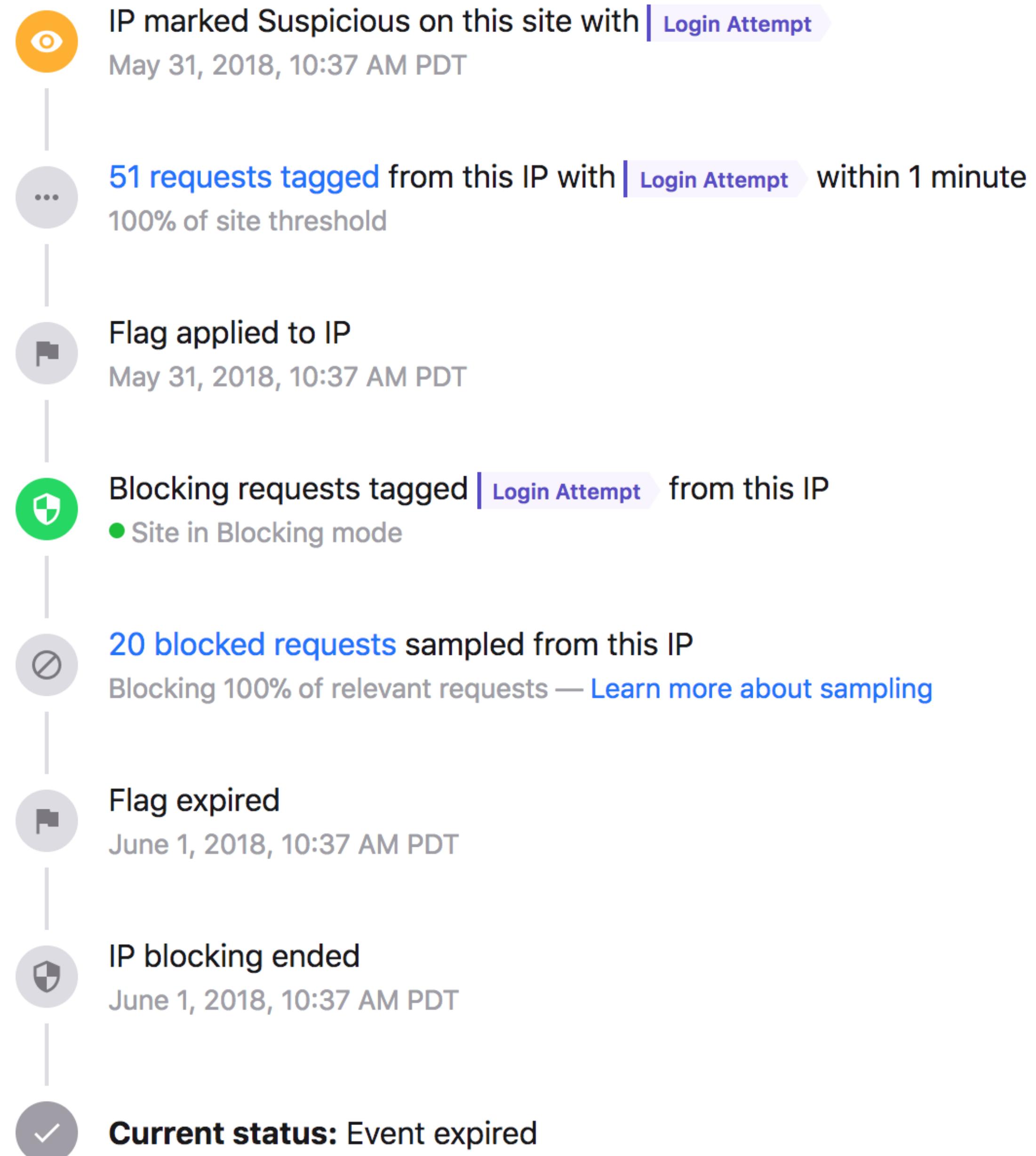
## Updated navigation and status model

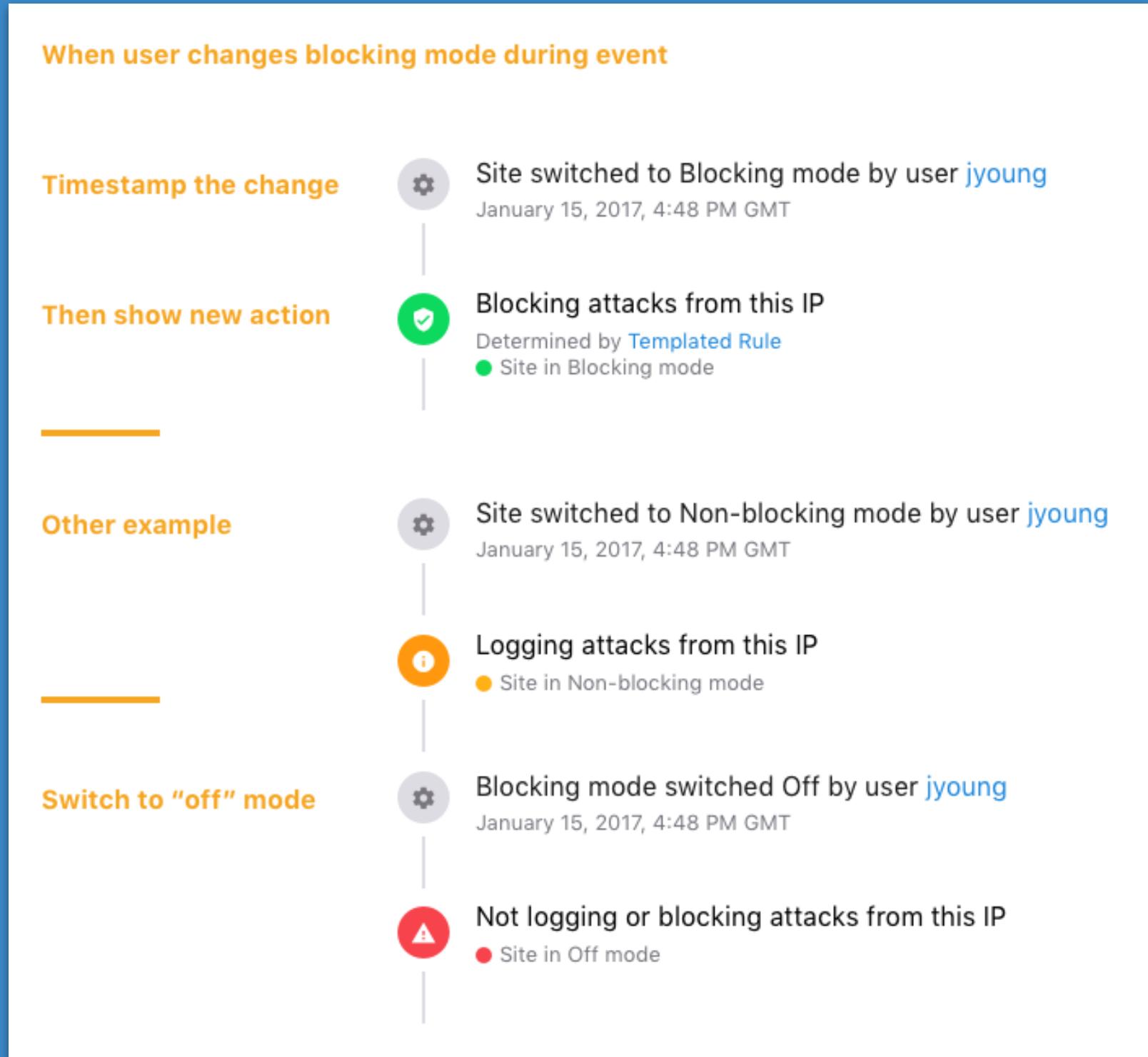
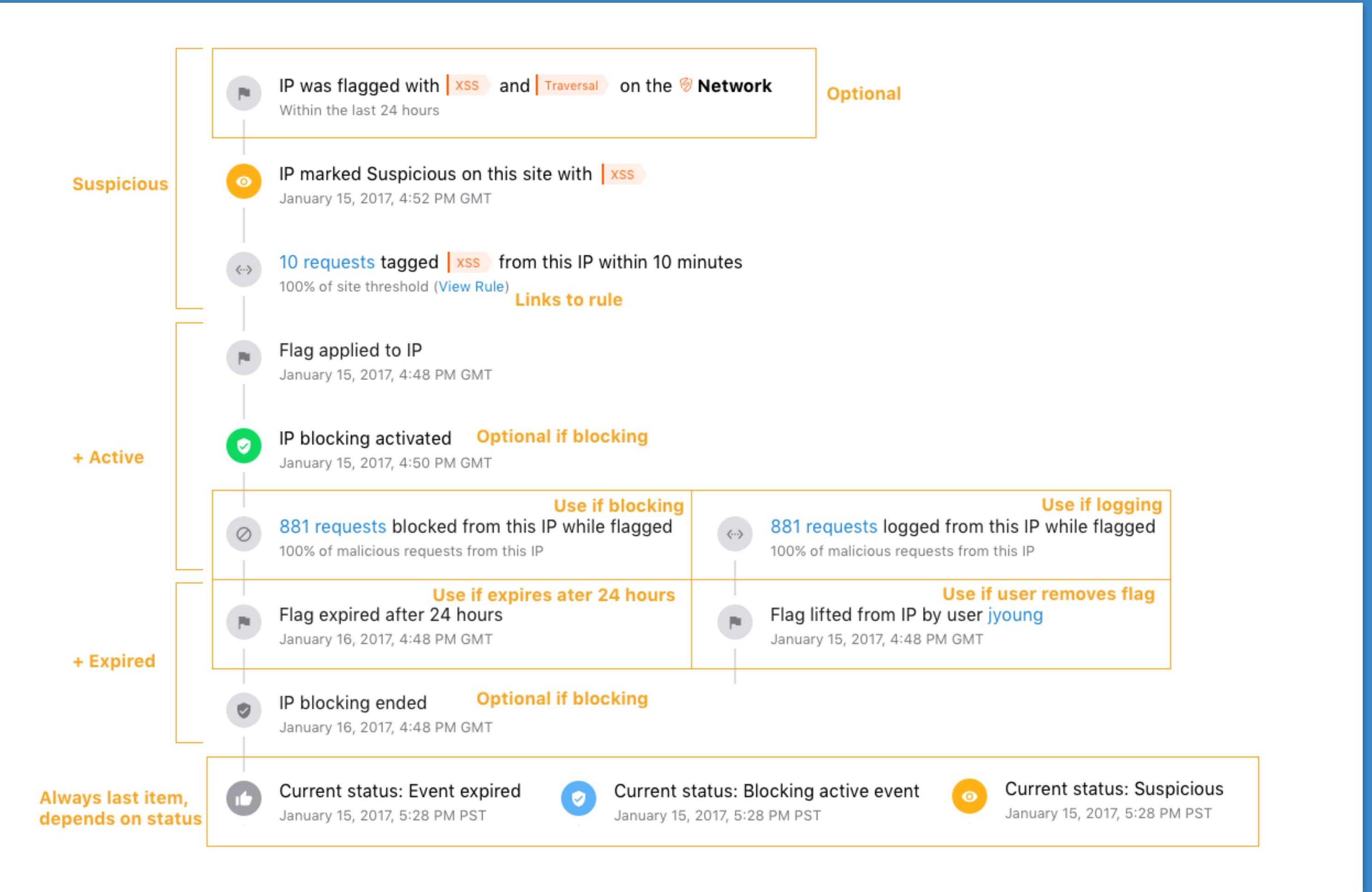
 80.11.22.33	ACTIVE
Traversal   XSS	6 hours ago
 72.221.42.17	EXPIRED
XSS	7 hours ago
 63.13.33.45	SUSPICIOUS
Login Attempt	8 hours ago

## Attack timeline:

- Industry-first
- No competitors have this
- Makes variety of data easier to parse
- Narrative format makes Signal Sciences value explicit
- Complex feature at the nexus of business logic, UI, and backend data model

### Timeline





## Multiple changes during implementation

- During development, we adapted to the requirements of the legacy data model and strived to render it clearly to users
- (My notes to engineers are in orange)

Updates to Current Status when event is Active:	
<b>Blocking</b>	<b>Current status:</b> Blocking active event
<b>Logging</b>	<b>Current status:</b> Logging active event
<b>Agent mode = off</b>	<b>Current status:</b> Allowing all requests
<b>Whitelisted IP</b>	<b>Current status:</b> Allowing all requests from Whitelisted IP
<b>Blacklisted IP</b>	<b>Current status:</b> Blocking all requests from Blacklisted IP

# Results:

- Higher engagement rates via analytics and bug reports
- Qualitatively better usability
- Multiple marketing wins
- Highlighted during sales demos

# Missed opportunities:

- Event filter was de-prioritized
- Event map was de-prioritized
- Differences between design and production due to component library restrictions

The screenshot shows a web-based monitoring and security tool interface. At the top, there's a header with the company logo (Ben Corp), the site name (still-stream-15119.herokuapp.com), and navigation links for Help Center, Corp Tools, and My Profile.

The main content area has several sections:

- Events**: A list of recent events over the last 30 days. Each event entry includes the IP address, a status indicator (ACTIVE or EXPIRED), and a brief description of the event type (e.g., Attack Tooling, Login Attempt, Registration Attempt).

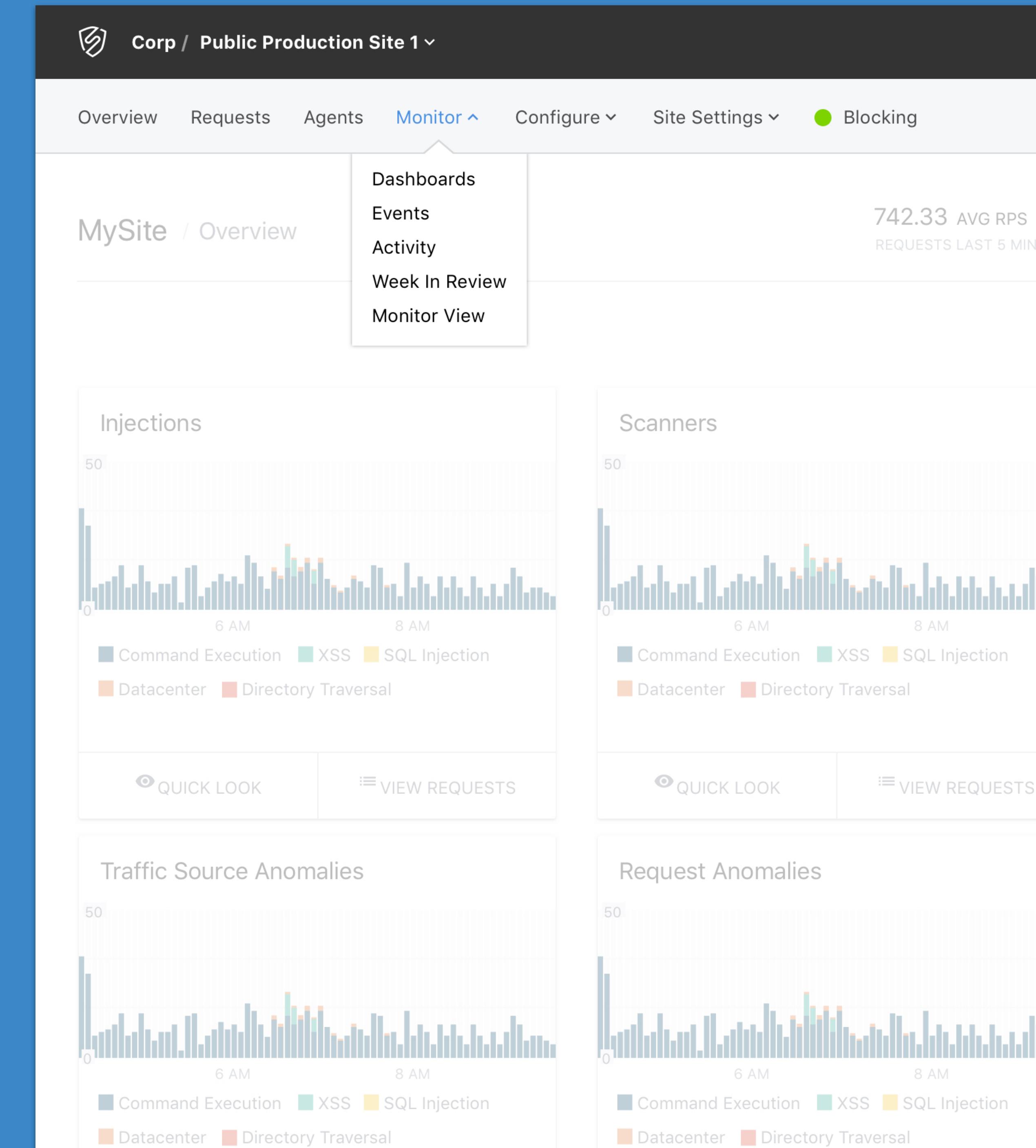
IP Address	Status	Event Type	Timestamp
192.168.0.100	ACTIVE	Attack Tooling	3 minutes ago
192.168.0.204	EXPIRED	Attack Tooling	yesterday
192.168.0.203	EXPIRED	Login Attempt	yesterday
192.168.0.205	EXPIRED	Attack Tooling	15 days ago
192.168.0.204	EXPIRED	Login Attempt	15 days ago
192.168.0.207	EXPIRED	Attack Tooling	18 days ago
192.168.0.206	EXPIRED	Registration Attempt	18 days ago
192.168.0.205	EXPIRED	Registration Attempt	18 days ago
192.168.0.205	EXPIRED	Registration Attempt	21 days ago
192.168.0.204	EXPIRED	Login Attempt	21 days ago
- Blocking requests from flagged IP**: A detailed view for the flagged IP 192.168.0.100. It shows the status as ACTIVE, the IP as 192.168.0.100, and the signal as Attack Tooling. It also states that 51 requests were blocked while flagged. A note indicates requests will be monitored for 23 hours until June 2, 2018, at 4:10 PM PDT.
- Timeline**: A chronological log of events for the flagged IP. Each item includes an icon, a description, and a timestamp.
  - IP marked Suspicious on this site with Attack Tooling (June 1, 2018, 4:10 PM PDT)
  - 51 requests tagged from this IP with Attack Tooling within 1 minute (100% of site threshold)
  - Flag applied to IP (June 1, 2018, 4:10 PM PDT)
  - Blocking malicious attacks from this IP (Site in Blocking mode)
  - 51 requests blocked from this IP while flagged (Blocking 100% of malicious requests)
  - Current status: Blocking active event**
- Details**: A summary section showing the IP ADDRESS as 192.168.0.100.

# Case study #2

# Navigation redesign

I redesigned Signal Sciences' management console navigation.

- Reorganized menu items into more intuitive groupings
- Improved access to most-used features
- Redesigned to reflect how Signal Sciences organizes customer properties
- Identified highest-value enterprise “power users”
- Prepared dashboard to scale for enterprise
- Established new analytics tracking standards



# Problems:

- Items were crammed into non-intuitive menus
- Most-visited pages were hard to find and access
- Wasn't clear whether the user was in the “site” context or the “corp” context
- Difficult and slow to switch between customer sites

The screenshot shows a complex web interface with a navigation bar at the top. The navigation bar includes links for Dashboards, Configurations (with a dropdown menu), Blocking, Support, Docs, Adobe, Behance, and a date range selector set to 'LAST 6 HOURS'. A red arrow points from the 'Configurations' link to its dropdown menu, which lists many items: Agents, Whitelist/Blacklist, Flagged IPs, Members, Data Privacy, Integrations, Header Links, Signals, Custom Rules, Custom Rules V2, Custom Tags, and Custom Alerts. Another red arrow points from the 'Behance' link in the top navigation to the 'ACTIVE INTEGRATIONS' section, which displays 5 active integrations. A third red arrow points from the 'Injections' chart area to the 'Scanners' section, which contains a histogram and the text 'Way too many items. How do I find what I'm looking for?'. The overall layout is cluttered and lacks a clear user flow.

Behance Overview

Injections

50

Scanners

Way too many items.  
How do I find what I'm looking for?

742.33 AVG RPS  
REQUESTS LAST 5 MIN

60 187 14  
AGENT HEALTH

LAST 6 HOURS

ACTIVE INTEGRATIONS

5 # pd ...  
ACTIVE INTEGRATIONS

Flagged IPs  
IPs that have triggered decisions

94.242.221.621  
100% of the XSS threshold  
ACTIVE

23 min ago

Are these categories meaningful?  
Am I viewing the corp or site context?

<input type="checkbox"/>	Event Label <span>?</span>	Total Events <span>?</span>	↓	Unique Events <span>?</span>	Event Value <span>?</span>	Avg. Value <span>?</span>
		7,217 % of Total: 26.40% (27,333)		4,197 % of Total: 29.48% (14,236)	0 % of Total: 0.00% (4)	0.00 Avg for View: <0.01 (-100.00%)
<input type="checkbox"/>	1. overview-link	1,659 (22.99%)		809 (19.28%)	0 (0.00%)	0.00
<input type="checkbox"/>	2. agents-link	1,345 (18.64%)		580 (13.82%)	0 (0.00%)	0.00
<input type="checkbox"/>	3. requests-link	1,036 (14.35%)		495 (11.79%)	0 (0.00%)	0.00
<input type="checkbox"/>	4. whitelist-blacklist-link	339 (4.70%)		223 (5.31%)	0 (0.00%)	0.00
<input type="checkbox"/>	5. signals-link	306 (4.24%)		168 (4.00%)	0 (0.00%)	0.00
<input type="checkbox"/>	6. events-link	247 (3.42%)		150 (3.57%)	0 (0.00%)	0.00
<input type="checkbox"/>	7. dashboards-link	242 (3.35%)		189 (4.50%)	0 (0.00%)	0.00
<input type="checkbox"/>	8. custom-alerts-link	209 (2.90%)		132 (3.15%)	0 (0.00%)	0.00
<input type="checkbox"/>	9. members-link	208 (2.88%)		135 (3.22%)	0 (0.00%)	0.00
<input type="checkbox"/>	10. corp-link	165 (2.29%)		131 (3.12%)	0 (0.00%)	0.00

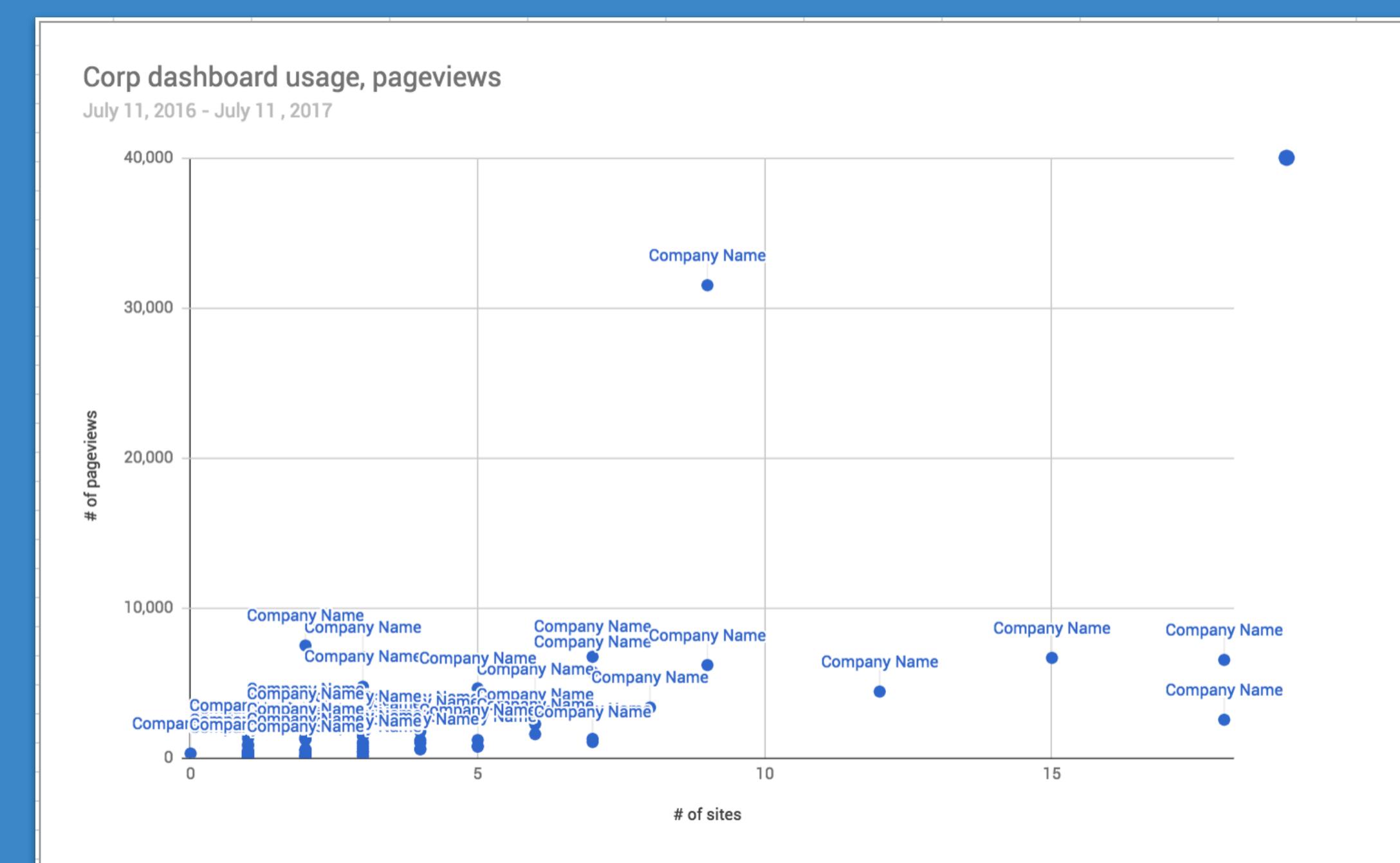
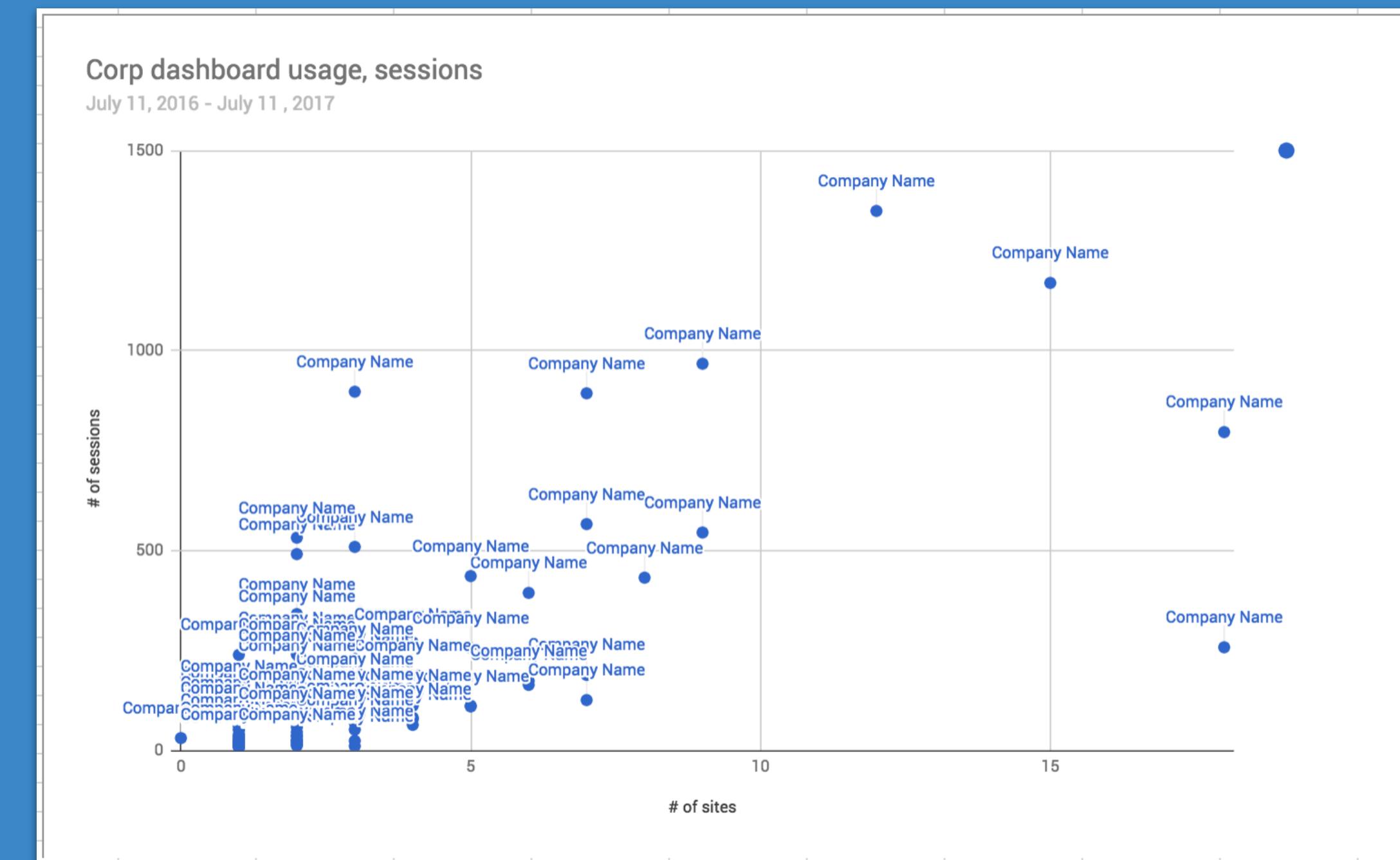
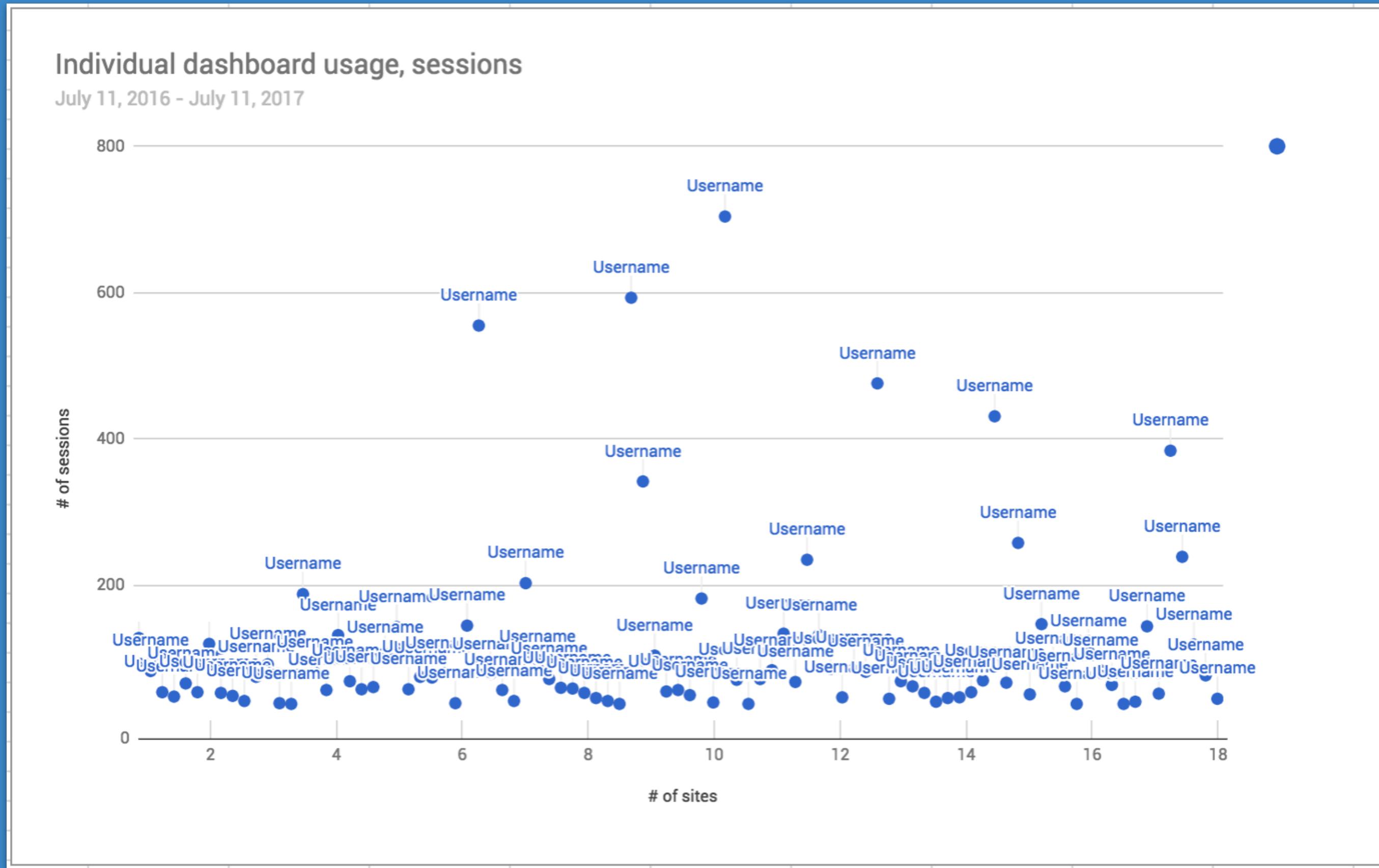
## Identified most-used pages

- Established analytics tracking standards to capture data
- *page-name, component-action, target-component*

Navigation Bar					
<a href="#">Dashboard</a> <a href="#">Overview</a> <a href="#">Dashboards</a> <a href="#">Search</a> <a href="#">Monitor View</a> <a href="#">Events</a> <a href="#">Activity</a> <a href="#">Week in Review</a>	<a href="#">Configurations</a> <a href="#">Whitelist/Blacklist</a> <a href="#">Flagged IPs</a> <a href="#">Members</a> <a href="#">Data Privacy</a> <a href="#">Integrations</a> <a href="#">Header Links</a> <a href="#">Signals</a> <a href="#">Members</a> <a href="#">Custom Rules</a> <a href="#">Custom Rules V2</a> <a href="#">Custom Tags</a> <a href="#">Custom Alerts</a>	<a href="#">Non-blocking toggle</a>	<a href="#">Help Center</a> <a href="#">Guides &amp; FAQ</a> <a href="#">API Docs</a> <a href="#">Support</a>	<a href="#">[Corp name]</a> <a href="#">Reports</a> <a href="#">Manage Sites</a> <a href="#">Manage Users</a>	<a href="#">[Site name]</a> <a href="#">Reports</a> <a href="#">Manage Sites</a> <a href="#">Manage Users</a>

# Re-grouped features

Label	Description
Overview	Your home base where you can find site-based graphs of requests and attack trends, alerts, and links to more detailed information.
Graphs of Signals	A collection of graphs that each visualize a tag's prevalence across all traffic.
Requests	View and search through a list of all requests to your site.
Monitor View	A read-only mode to visualize high-level request and attack data meant for displaying on large monitors.
Events	A list of events across the dashboard, like a notification of a suspicious IP being flagged.
Activity	A list of all activity across the dashboard, like flagged IPs and changes to settings by a user.
Week In Review	A report of traffic and attack trends across your site for the last 7 days.
Agents	A list of all agents on your servers and their current status.
Whitelist/Blacklist	View and edit a list of all IPs whose traffic has been permanently blocked or allowed.
Flagged IPs	A list of specific IPs which are currently being monitored for malicious traffic.
Members	Add and view users that have administrative privileges on a site.
Data Privacy	Edit what data from your requests is visible or redacted prior to being sent to our platform.
Integrations	Connect to third-party services like Slack or Jira in order to view notifications and information.
Header Links	Set up links to cross-reference our request data in other third-party services you use.
Signals	View the rules that determine how requests are tagged and what actions are taken by our platform.
Custom Tags	Create custom tags to categorize specific request types.
Custom Alerts	Create custom alerts based on the presence and rate of custom tags.
Turn Blocking Mode On and Off	Toggle Blocking Mode on and off with a single click.
Guides & FAQ	See guides for installing, using, and troubleshooting our platform.
API Docs	In-depth technical instructions on connecting to and using our platform's API.

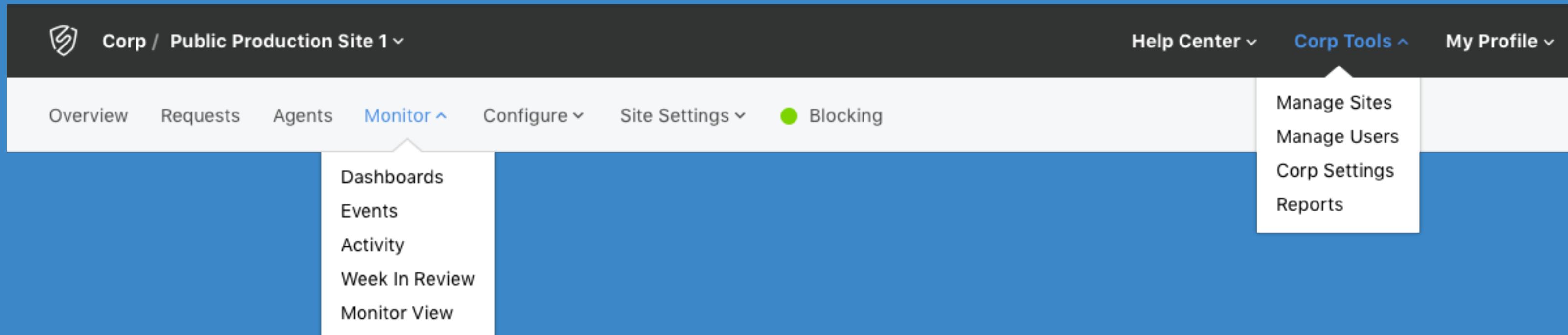
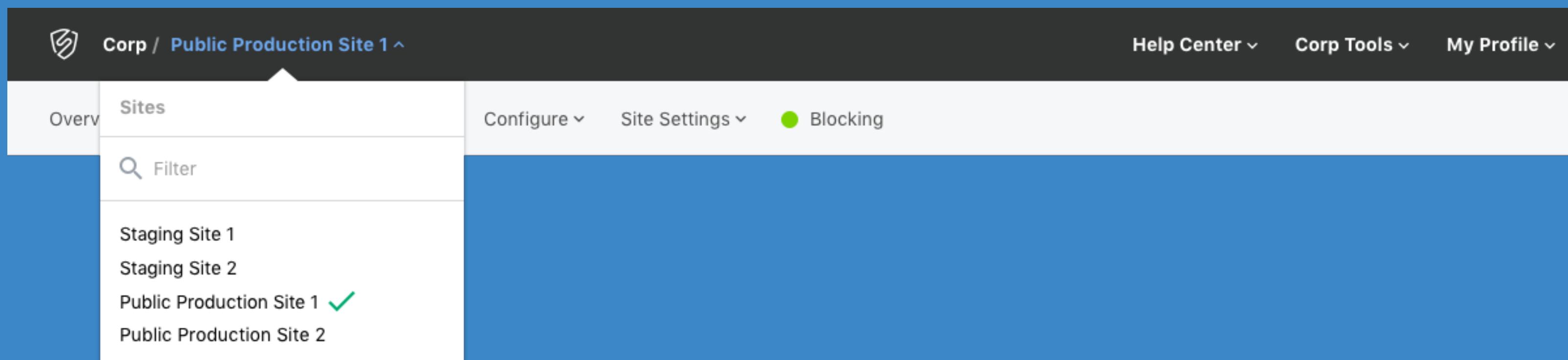


# Identified “power users” to test with

- (Customer names redacted)

# Results:

- Introduced two-level nav that aligns with property hierarchy:  
top-level is corp-level features, bottom level is site-level features
- Moved most-used items, like Requests, to the front
- Re-organized remaining nav items into new categories that reflect purpose
- New site switcher is explicit about corp/site hierarchy and includes on-the-fly filter



# Thanks!



November 2019

Website: [jbarr.co](http://jbarr.co)

Email: [justin@jbarr.co](mailto:justin@jbarr.co)