

Wen Liu

Product Design Portfolio



ABOUT ME

Bio, Expertise, Work history

Self Intro



Wen Liu

From Senior UX Designer Promoted to
UX Design Lead/Design Expert at DiDi

8 Yrs Product Design Experience **First** Designer in the team

Sole Design Expert in department, oversee all aspects of design work

- Own the design vision, strategy, UX roadmaps, and product success
- Leading the development of UX processes with design decisions
- Proficiency in using data, interview and competitive analysis to define and solve complex problem
- Excel in building design systems to improve workflow and boost productivity

Tynker

06/2014 – 05/2015

Teacher's Portal
Kids' coding Platform

Cisco

06/2015 – 01/2020

Cisco Network Assurance Engine
Cisco Learning Network
Cisco Cloud Collaboration

DiDi

04/2020 – Present

EagleEye Endpoints Protection Platform
Cross-functional team Supports
Workshops, talents training, knowledge sharing

ABOUT ME

Roles and accomplishments

Responsibilities and Projects


Main Responsibilities

- EagleEye Endpoints Protection Platform **end to end UX enhancement**
- **Cross-functional team** products UX supports
- Holding **design workshops, talents training,** and **knowledge-sharing sessions**

Key Projects

- Build EagleEye entire **design system from scratch**
- Re-design the features related with **audit and control management**
- Cross-functional team support with **UX guidance, supervision, execution**
- Build UX of DiDi **D-Sec endpoint software**
- **Mentor, collaborate with contractor and interns** in multiple projects

Accomplishments at DiDi

75%

EagleEye clients' trial conversion rate
2019 18%, 2020 46%, 2021 62%, 2022 83%

\$6M

Generated revenue with UX Enhancement
in commercialization of the product

8.3

Product average NPS score
13 Clients sample, NPS value 64%

9

New clients acquisition

0-1

Build EagleEye design system

25+

New EagleEye features launched

1,000+

Related product page design

20+

Talent training project completed

ABOUT ME

PRODUCT INTRO

Product overview

EagleEye EPP

Users: **Enterprise Security Operators**

Internal + External Covered: **100K Endpoints**

Internal use

- Internal Security Tool

Commercialization

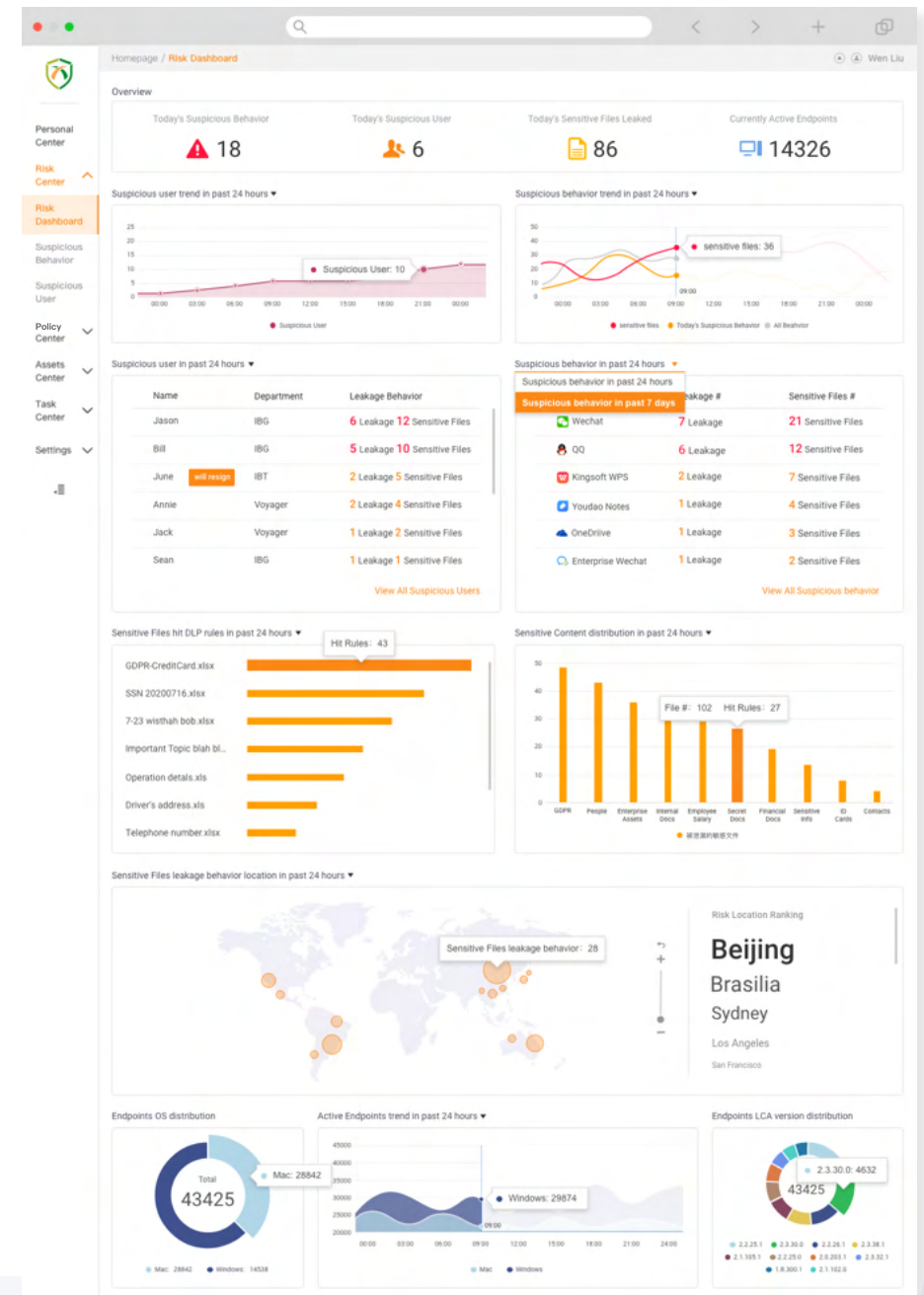
- Market – Approved
- Mature Product

Traditional DLP

- Risk Detection
- Security Audition

EPP Integrations

- TRAD. DLP Features
- Control Management
- Endpoints Security



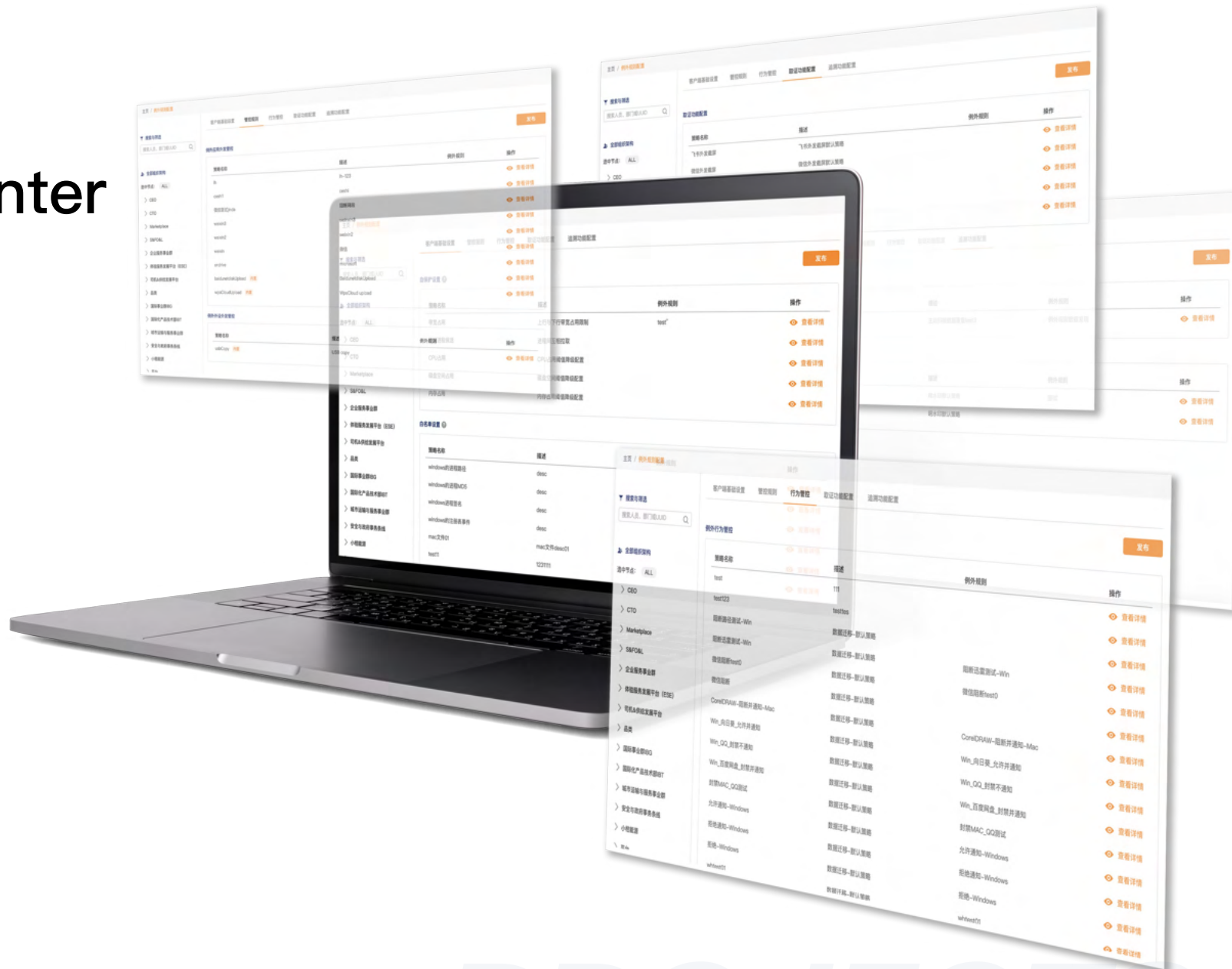
PROJECTS

User Experience Enhancement

EagleEye Policy Center

Re-Design

To effectively address complex problems and enhance user experience, it is crucial to gather and analyze data using established design methodologies. By doing so, it is possible to identify and implement improvements that will increase feature conversion rates, task success rates, and engagement rates.

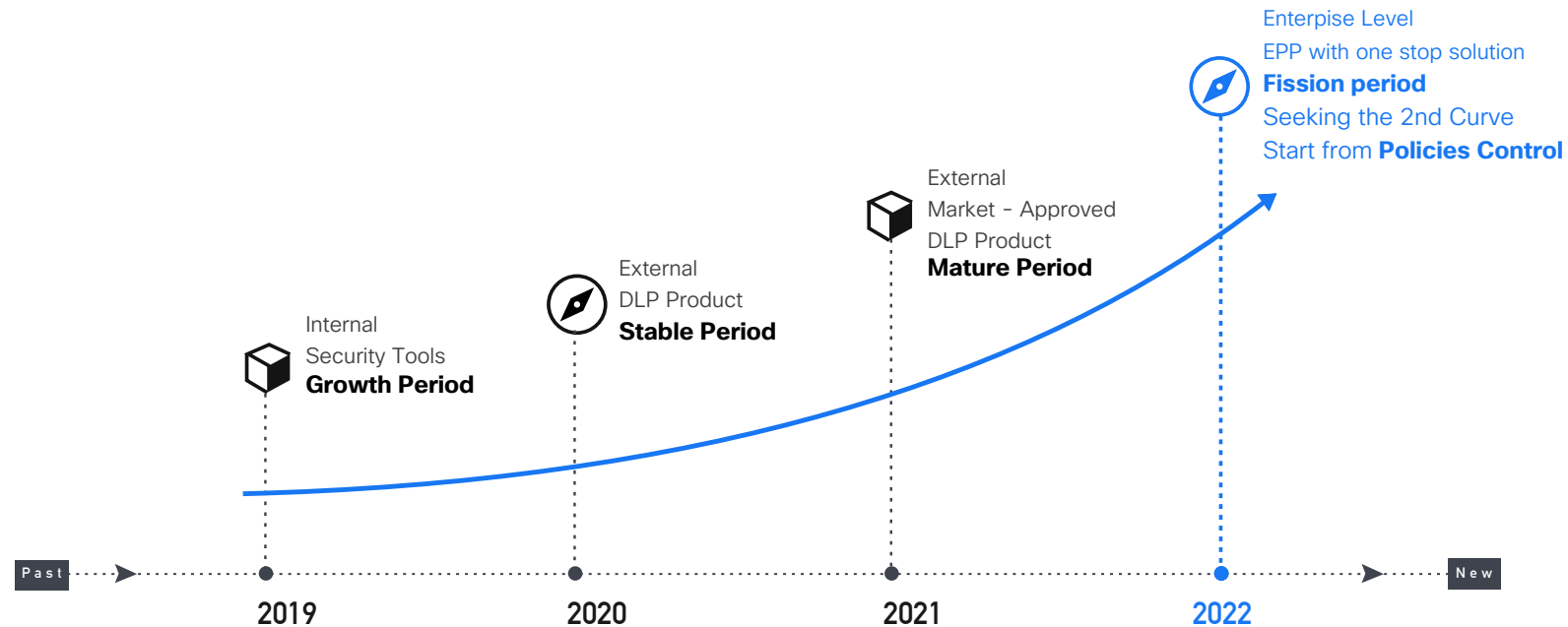


PROJECTS

BACKGROUND

Product observation and growth trend

Business and Users' Goal



BUSINESS GOAL ◦

- Trial **Conversion**
- Clients **Acquisition**
- Clients **Retention**
- Revenue **Growth**
- NPS **Increase**
- Market **Share**

USERS (SecOps) ' GOAL ◦

- **Efficiency** of Daily Task
- **Reliability** of Performance
- **Meet Flexibility** of Requirements
- **Lower Learning Cost**
- **Effectiveness** of Cost
- **Scalability** of Features
- **Continuous** improvement
- **Reduce** Insider Risk Rate
- **Improve** Security Awareness

USER INTERVIEW

Qualitative analysis from existing policy configuration features

User Feedbacks

SecOps	Position	User Scenarios	Pain Point
David Li	Director, Security Operations	<ul style="list-style-type: none">Assessing the impact of departmental policiesHigh-level review of security policies content and structure	Configuration process not start from department level
Kz Wu	Security Operations Manager	<ul style="list-style-type: none">Managing security policies and proceduresManaging insider threats, Identifying and protecting sensitive data	For All / For One interaction process is inconsistent
Bert Wu	Security Operations Administrator	<ul style="list-style-type: none">Developing app related policies and proceduresConfiguring multiple policy control management	Confused on content and feature, feeling useless
Vic Wong	Security Operations Administrator	<ul style="list-style-type: none">Developing app related policies and proceduresConfiguring multiple policy control management	Validation errors when edit, performance issue
Jason Zheng	Cyber Security Administrator	<ul style="list-style-type: none">Developing webapp related security policies and proceduresConfiguring webapp, app blocking control management	Frustrated on workflow, batch operation not userfriendly
Yaoxiong Zheng	IT Security Administrator	<ul style="list-style-type: none">Developing deivce security policies and proceduresConfiguring device basics, app, app process control management	Complex process on control management workflow
Alex Zhao	IT Security Administrator	<ul style="list-style-type: none">Developing deivce security policies and proceduresConfiguring device basics, external device control management	The workflow is very confusing, conflicts, validation errors
Jimmy Zhang	Information Security Administrator	<ul style="list-style-type: none">Developing forensics, watermark security policies and proceduresInvestigative multiple policy control management	Interactive confusion, no confidence to use on forensics features
Cherie Wong	Information Security Administrator	<ul style="list-style-type: none">Developing forensics, watermark security policies and proceduresInvestigative forensics, water mark control management	Too much info need to fill on form, hard to complete the daily task
Vicky Yu	Information Security Administrator	<ul style="list-style-type: none">Developing forensics, watermark security policies and proceduresInvestigative forensics control management	Batch operation with performance issue

DATA

Quantitative analysis from existing policy configuration features

Data (7 Days)

Collaborate with data scientists to ensure the data from internal analytics tools are accurate.

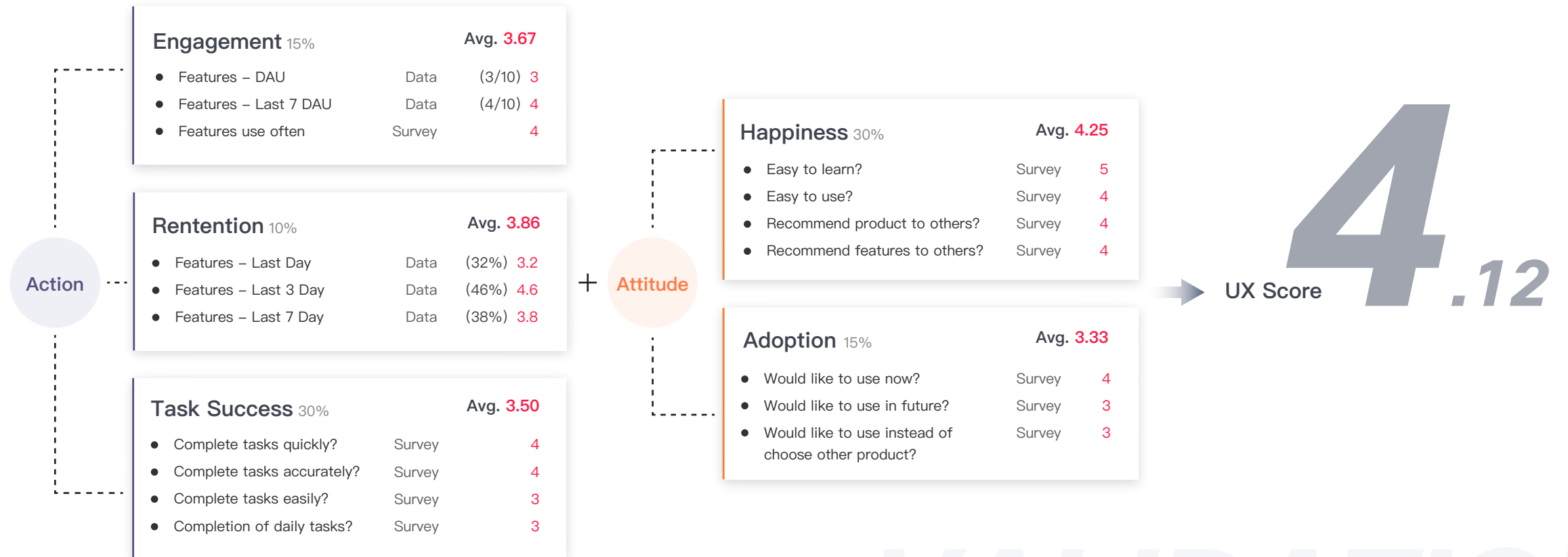
Metrics	Attribute	Data	Analysis
Task Completion Rate:	<ul style="list-style-type: none">Abandoned tasksRepeated tasks	<p>40% (poor)</p> <p>20% (fair)</p>	<p>Users are encountering difficulties</p> <p>Users are having difficulty understanding how to complete the process</p>
Time on Task:	<ul style="list-style-type: none">High average timeHigh standard deviation	<p>20 minutes (fair)</p> <p>10 minutes (fair)</p>	<p>Process is too complex or time-consuming</p> <p>The process is inconsistent or difficult to predict</p>
Error Rate:	<ul style="list-style-type: none">Frequency of errorsTypes of errors	<p>10 errors per user (fair)</p> <p>50% syntax errors (fair)</p>	<p>Users are encountering problems during the process of setting</p> <p>Program language used in the UI is confusing or unclear</p>
Click-Through Rate:	<ul style="list-style-type: none">Low click-through rate	<p>2% (fair)</p>	<p>Users are confused about content, lack clear CTA, unappealing UI design.</p>
Engagement Rate:	<ul style="list-style-type: none">Frequency of engagementDuration of engagement	<p>1 time per day (fair)</p> <p>2 minutes (poor)</p>	<p>Users are not finding the policy configuration feature useful or valuable</p> <p>Users are quickly losing interest or becoming frustrated with the process</p>

VALIDATION

UX Validation on existing policy configuration features

Survey Model

Use Google Heart Model with slightly change, send the survey to 10 SecOps and combine the data from data analytics tools to calculate.



VALIDATION

DEFINE

From user feedbacks, data and survey model

Defined Problem

- ✗ Policy controls were fragmented
- ✗ No policy view from Department
- ✗ Useless of All Device Configuration
- ✗ Complex workflow
- ✗ Performance issue with validation process

Home / Control Configuration

All Devices Configuration

All Devices will be configured, except special configured device.

Total 4

Content of Strategy	Strategy Type	Blocking mode	Configuration Status	Operate
Baidu Cloud Disk <small>Built-in</small>	Applications	<input checked="" type="radio"/> Network Block	<input type="checkbox"/>	
Kingsoft WPS <small>Built-in</small>	Applications	<input checked="" type="radio"/> Network Block	<input type="checkbox"/>	
Printer <small>Built-in</small>	External Devices	<input checked="" type="radio"/> File Printing Block	<input checked="" type="checkbox"/>	
USB Storage Devices <small>Built-in</small>	External Devices	<input type="radio"/> File Copy Block <input type="radio"/> File Encryption <input type="radio"/> Inject Prohibited	<input type="checkbox"/>	

Special Configuration

Special configuration devices, will according to issued actual configuration and not follow any default configuration.

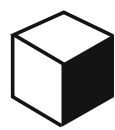
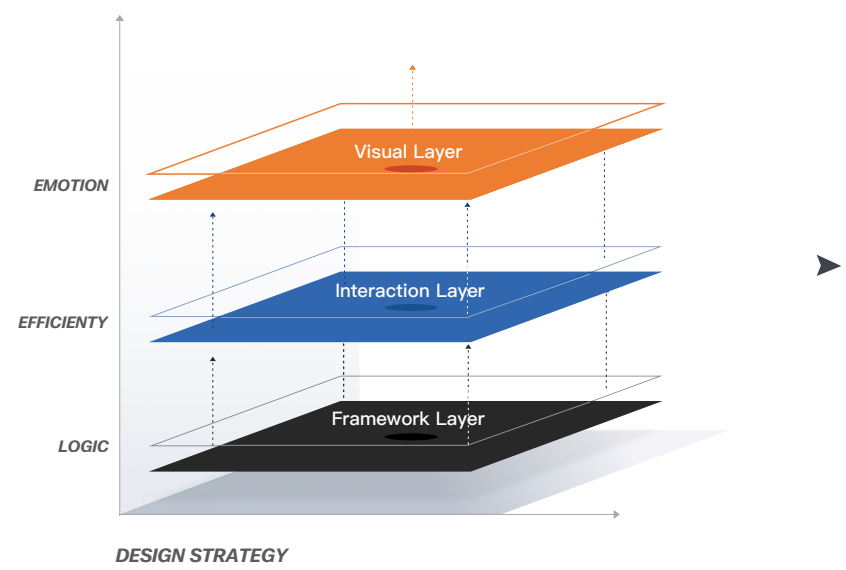
+ Add Special Configuration | Total 7

Device Or Device Group	Remarks	Operate User	Configuration Strategy	Operate Time	Operate
...VkoJVEdLSkxTIUxNk9JVEk3QkQ		tianqianqian	Apps: <input checked="" type="checkbox"/>	6/16/2021 17:33:50	<input type="checkbox"/> <input type="checkbox"/>
...DIUSIQ1BQU05SUIY0U1QzTUQ		Wentest	Apps: <input checked="" type="checkbox"/> External Devices: <input checked="" type="checkbox"/>	12/17/2020 10:47:24	<input type="checkbox"/> <input type="checkbox"/>
...DMJZCREVDMThQVknJRTJEOUo		jindatest	Apps: <input checked="" type="checkbox"/>	12/17/2020 10:43:07	<input type="checkbox"/> <input type="checkbox"/>
2TJUS1Bk4COU0A4A4E		jindatest		12/17/2020 10:20:20	<input type="checkbox"/> <input type="checkbox"/>

PROCESS

Use Product Thinking for a design solution

Methodology



01 Framework Update

Focus on the product logic to re-build security operation workflow, re-build information architecture to ensure operation easily and meet users' need

LOGIC



02 Efficiency Improvement

Improve basic source, set element priority and optimize display, simplify the workflow to enhance the operation experience

EFFICIENTLY



03 Design System Empowerment

Empowering design system is more effective internal collaboration, improving visual experience in security operation scenarios and enhances branding recognition

EMOTION

PROCESS

Why nobody uses All Device Configuration?

What is it?

An important carrier of the overall endpoints configuration

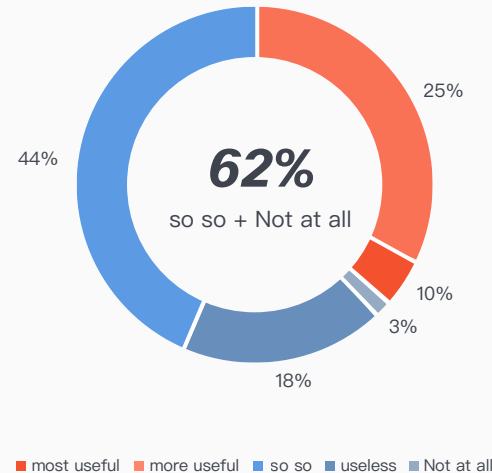
- On/Off behavior
- Conditions need to be accessed

Main channels for security operators and endpoints interaction

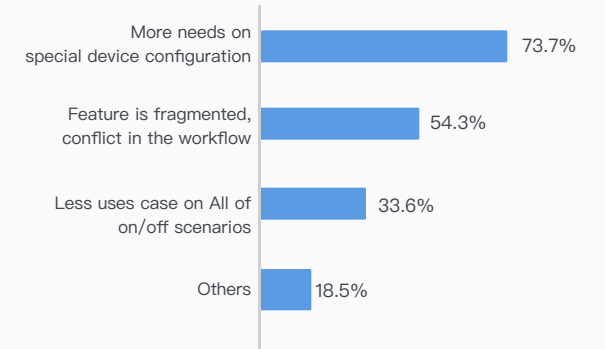
- Endpoints need to be managed in enterprise assets level
- An important configuration channel

How's the user feedbacks?

Current design usability Statistics from SecOps



Current design useless reason Survey from SecOps



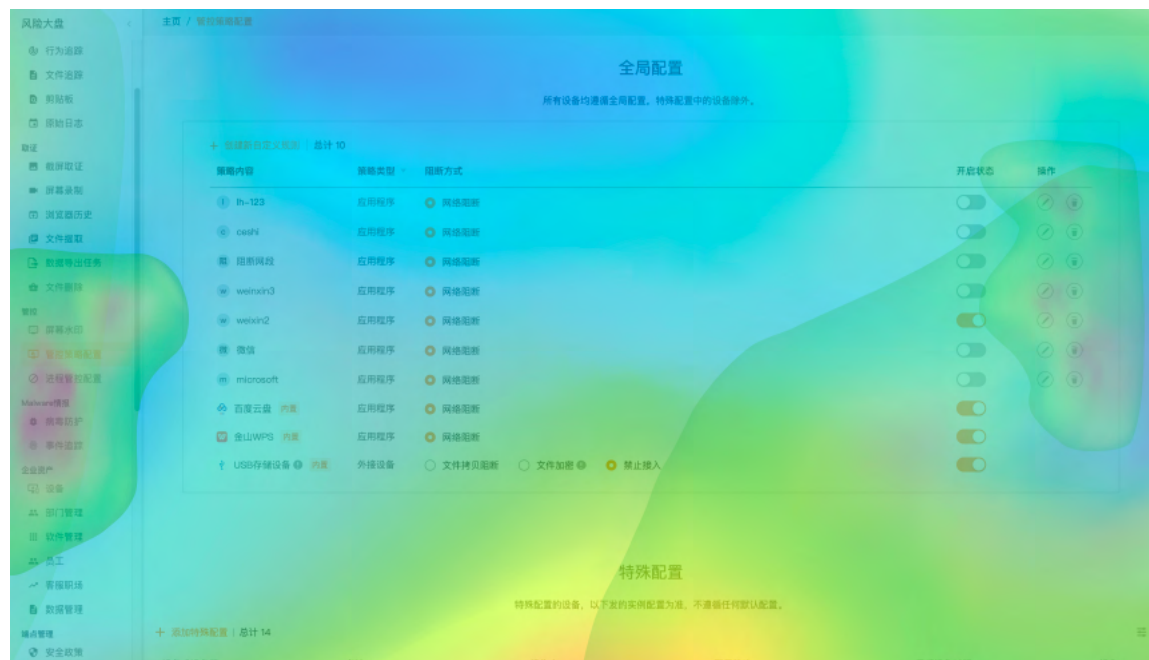
*The data from user interview and survey

LOGIC

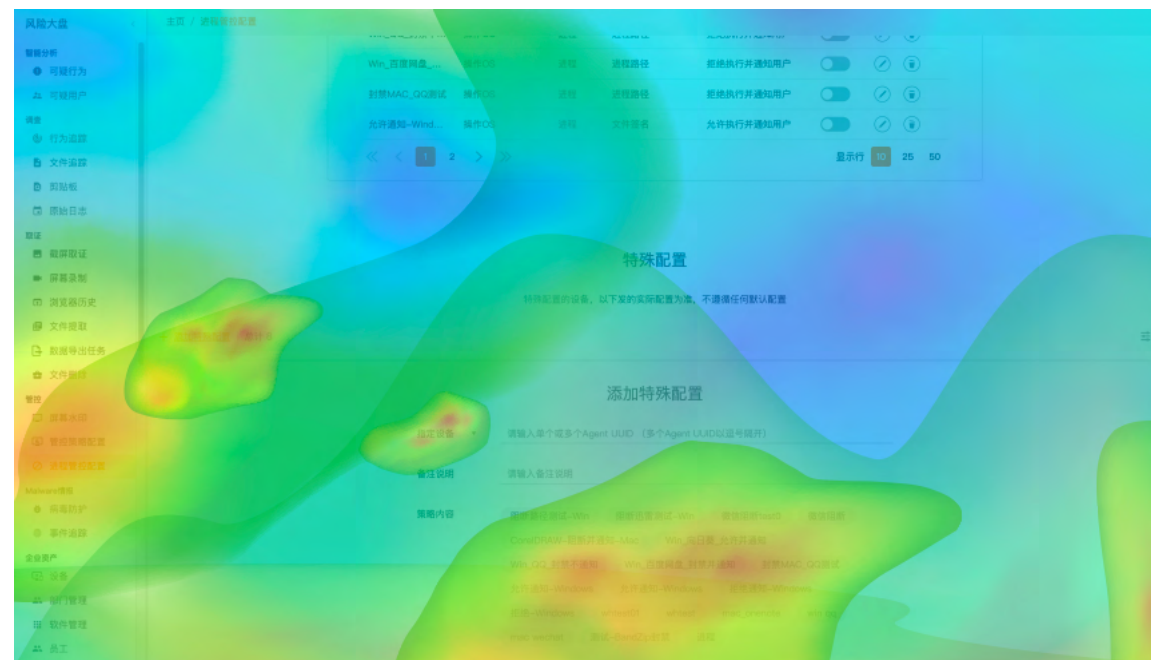
Visual analysis from Heat-Mapping tool

Heat Map References

- All Device Configuration feature is useless, page section conversion rate is low
- Users may open couples of the same page in one browser by interacting at Nav
- Users are encountering scrolling issue



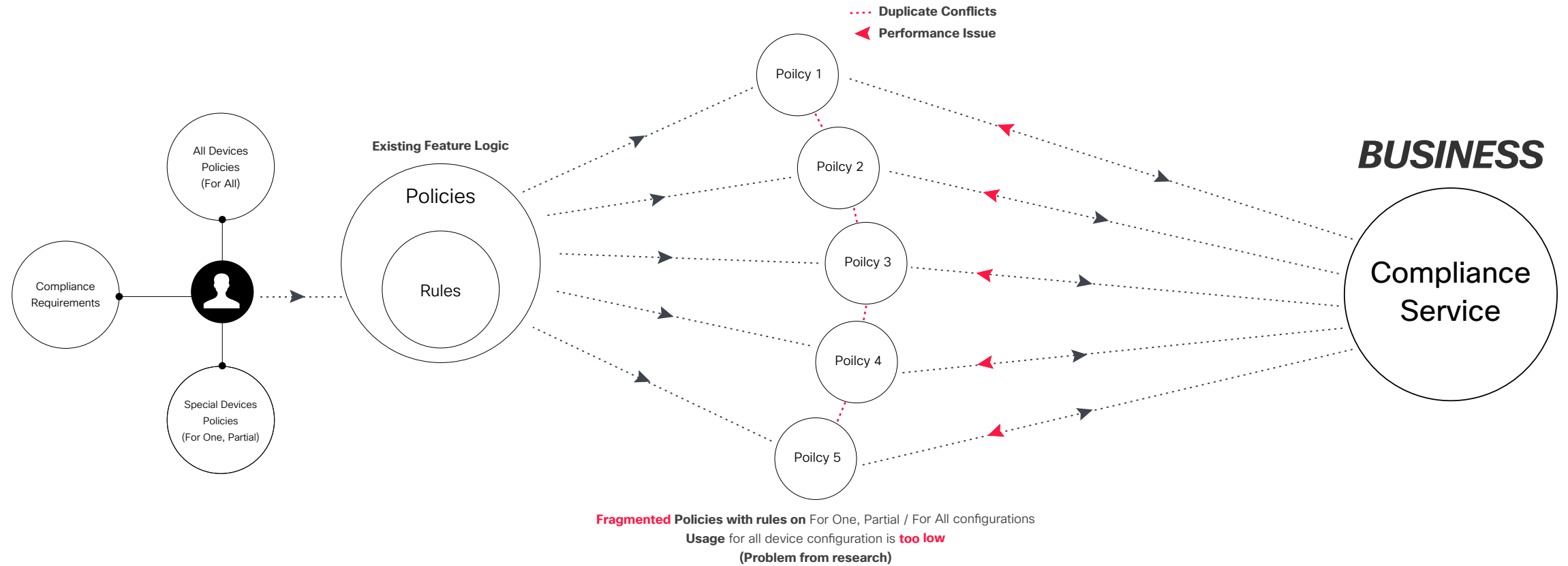
Landing page before scrolling



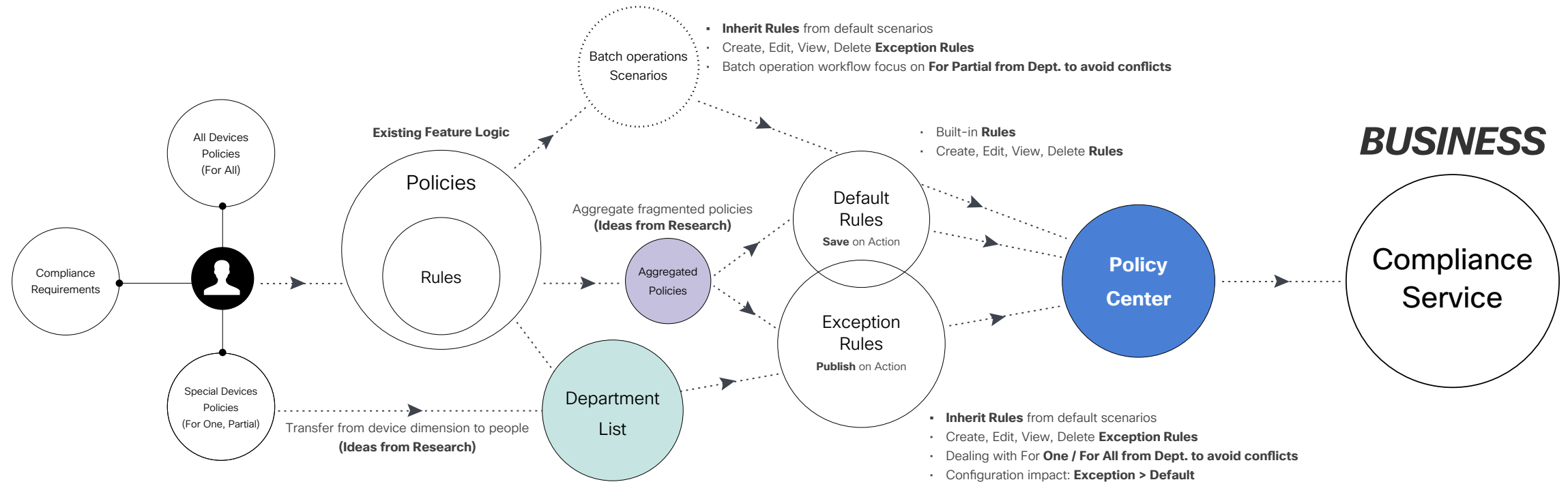
Landing page after scrolling

RESEARCH

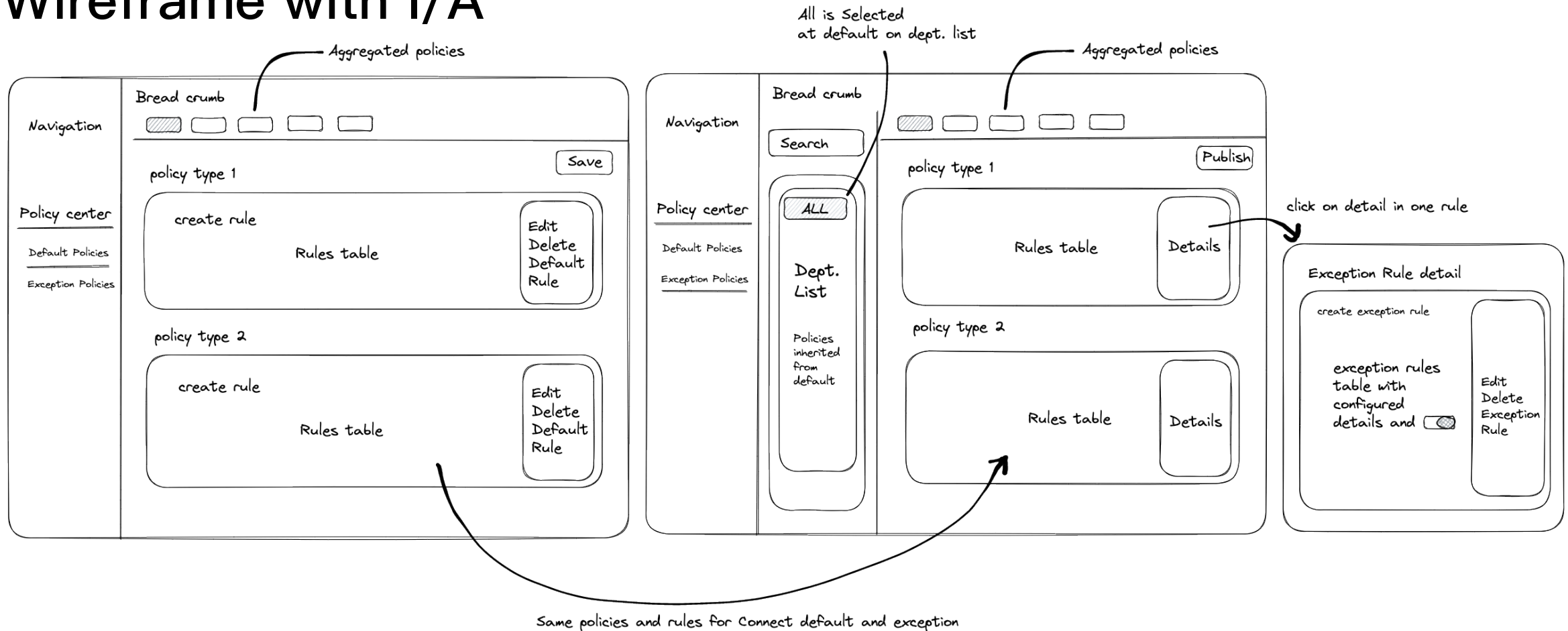
Existing Framework



New Framework Design Thinking



Wireframe with I/A



Interaction Enhancement

GOAL

All → **Default**

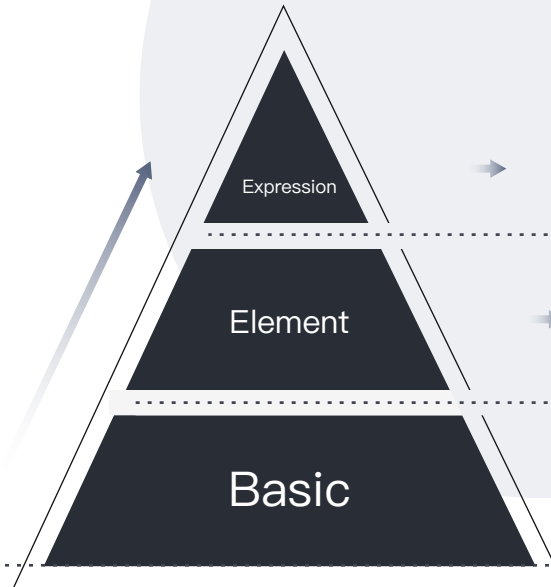
Special → **Exception**

Make the **Workflow** with

High Efficiency



Product Thinking



- **Optimize display, information at a glance**

Shows the unity of relevance and highlights the key content

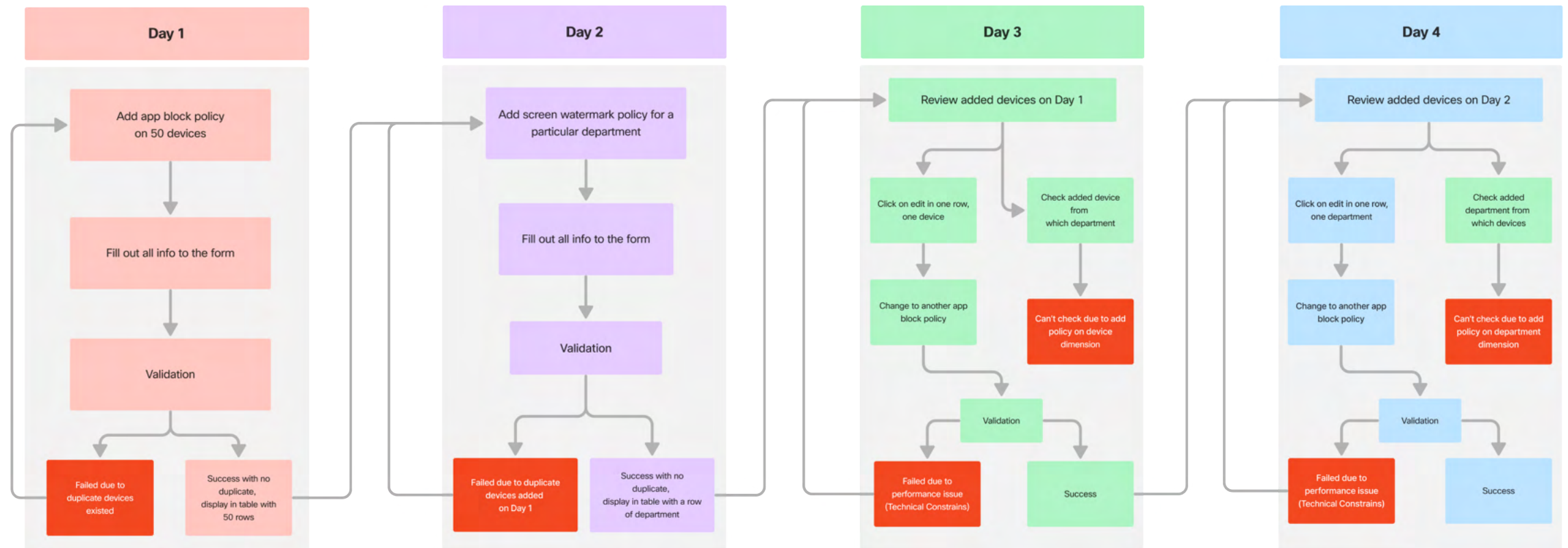
- **Set Element priority, publish with caution**

Specify Configuration, ensure the priority

- **Improve Basic source, unified management**

Integrate multiple configurations, establish the function logic

Existing Workflow

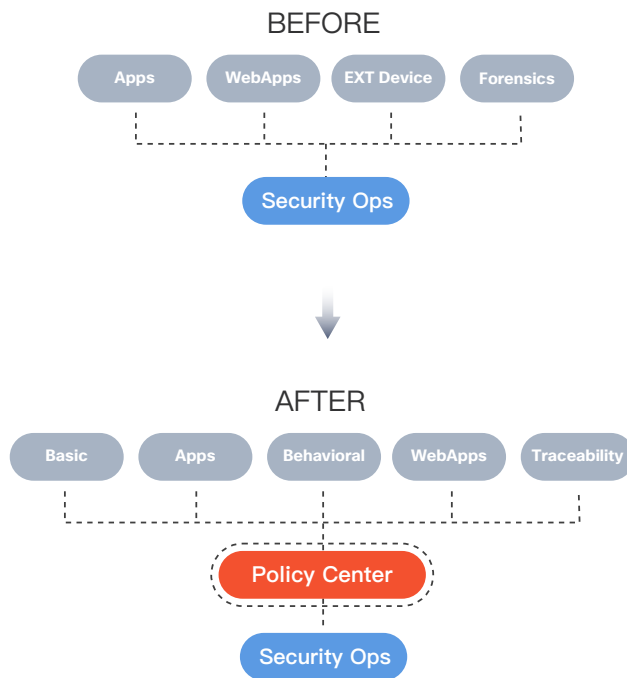


EFFICIENTY

Efficiency Improvements

Basic and Element

01 Improve Basic source, unified management



02 Set Element priority, clear for IA expression

Priority

P0/ **Critical**
Policies
Department

Clickable Elements of Defaults and Exceptions

Tab with Aggregated Policies | Department List | Search →

P1/ **Major**
Call to Action in
Landing of DEF, EXC

Create | Edit | Delete | EXC. Details | Save | Publish →

P2/ **Minor**
Call to Action in
EXC. Details

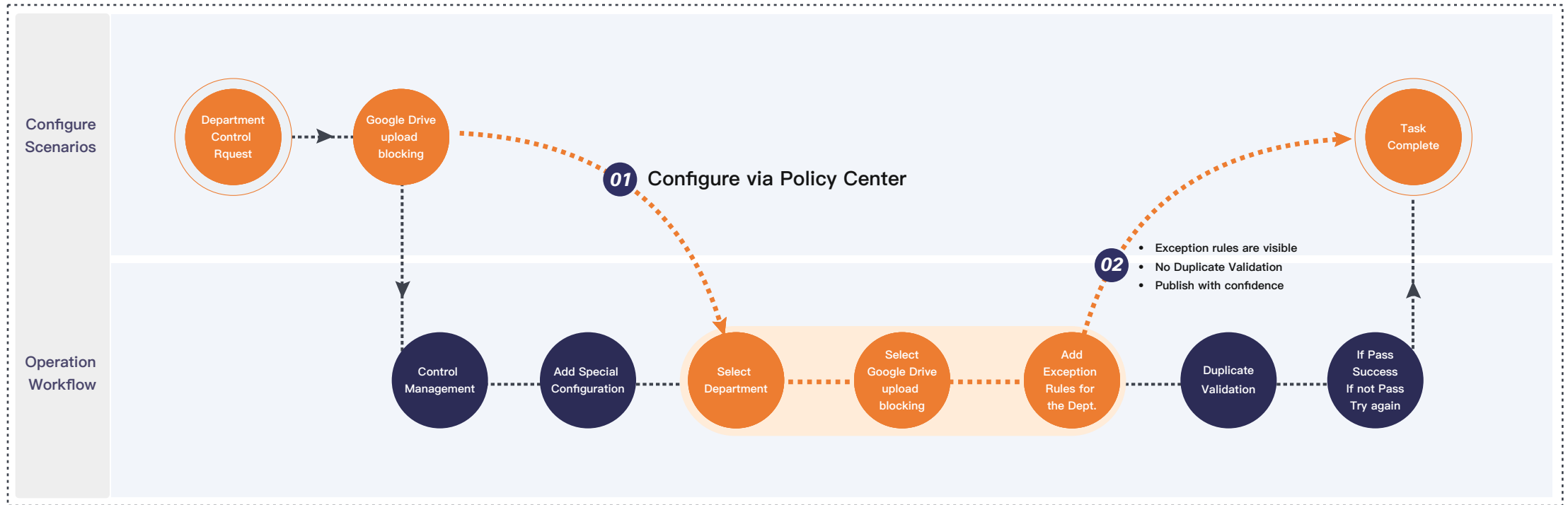
Create | Edit | Delete | Prioritize | On/Off Switch →

EFFICIENCY

Efficiency Improvements

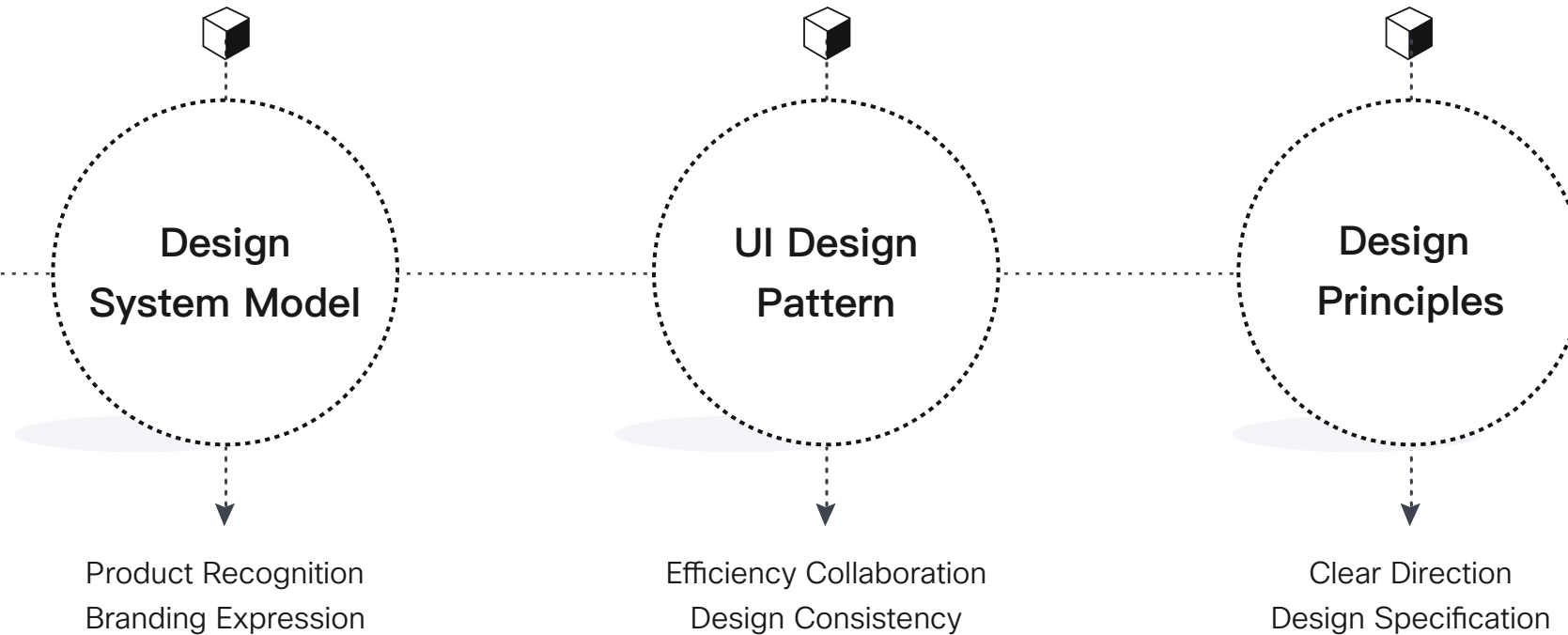
Simplified Workflow

Before 7 → After 3





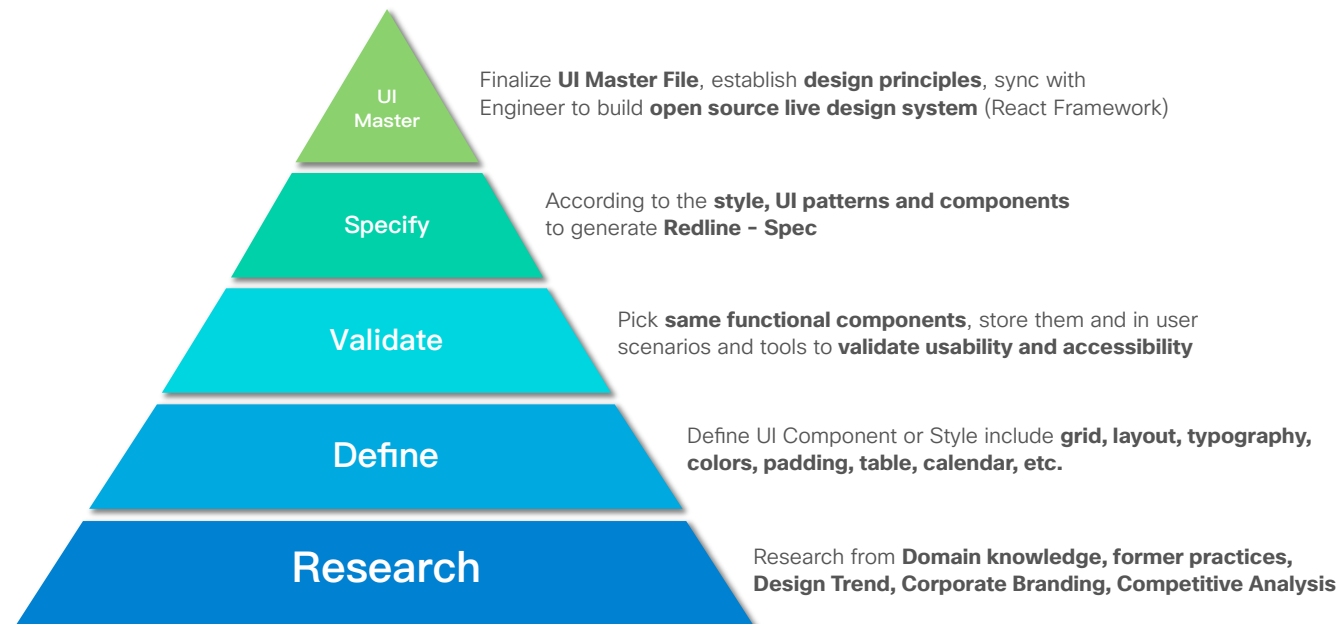
Design System in Operation Scenarios



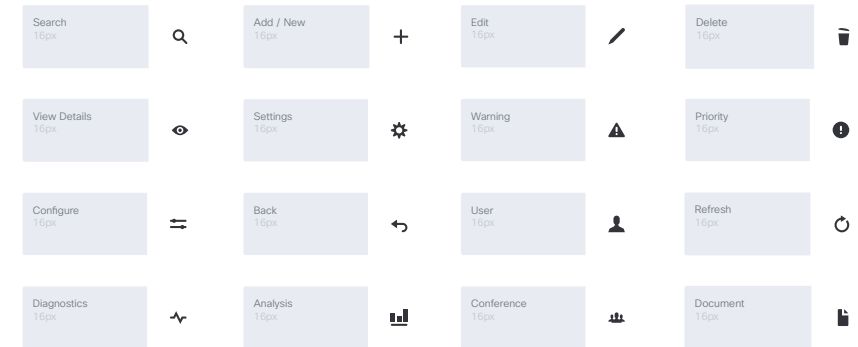
EMOTION

Design System Empowerment

Design System Model



Major Icons



Colors

Severity Palette



High Severity Palette



Standard Palette

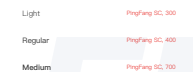


Font Guide

General Font Styling



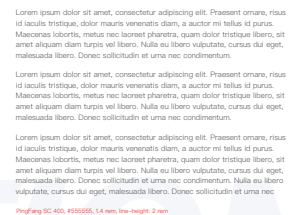
General Font Weight



Heading Font Size



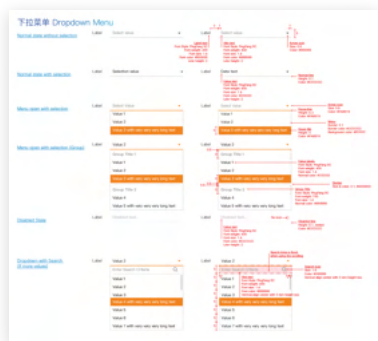
Default Body Font



EMOTION

Design System Empowerment

UI Design Pattern



Home / Policies Center / Exception Policies
Wen Liu

Search Filter

All Departments

- > CEO
- > CTO
 - > SSTG
 - > Business Sec
 - > Foundation Sec
 - wanghaokun
 - wenliu
 - liu haoeric**
 - Yangzhongnan
 - > Info Sec
 - > SSTG Office
 - > S&FO&L
 - > Enterprise Service Group
 - > Experience Service Platform
 - > Driver&Vendor Platform
 - > Goods Category
 - > IBG
 - > IBT
 - > Voyager
 - > S & G Business line

Endpoints Basic
Apps Leakage
Behavior Control
WebApps Leakage
✔ Exception Rule has been created

Publish

Self - Protection

Default Rules	Description	Exception Rules	Action		
Process Test Built-in	protection test	Self Test, CPU Test, RAM Test	Details		
+ Create an Exception Rule					
Exception Rule	Coverage	On/Off State	Remark	Operator	Action
Self Test	Device Source: Enterprise Assets OS: Windows	<input type="checkbox"/>	Test	Wenliu	↻ 🔒 ↑ ↓
CPU Test	Device Source: Enterprise Assets OS: Mac	<input checked="" type="checkbox"/>	Test1	Wenliu	↻ 🔒 ↑ ↓
RAM Test	Device Source: Enterprise Assets	<input type="checkbox"/>	Test2	Wenliu	↻ 🔒 ↑ ↓

DISK Protection Built-in	All Disk process enabled		Details
CPU	All CPU usage peak limit	MacOS-BigSur	Details
RAM Control	All RAM usage limit	Low-End Device	Details

White - List

Default Rules	Description	Exception Rules	Actions
360	360 white - list		Details
Mac Updates	Mac Updates white - list	Mac-Update	Details
IDEA	IDEA Strategy white - list	IDEA-Rule	Details

EMOTION

Design System Empowerment

Design Principles

Clear **Direction** for Implementation



Establish **Design Specifications** (Redline-Spec)



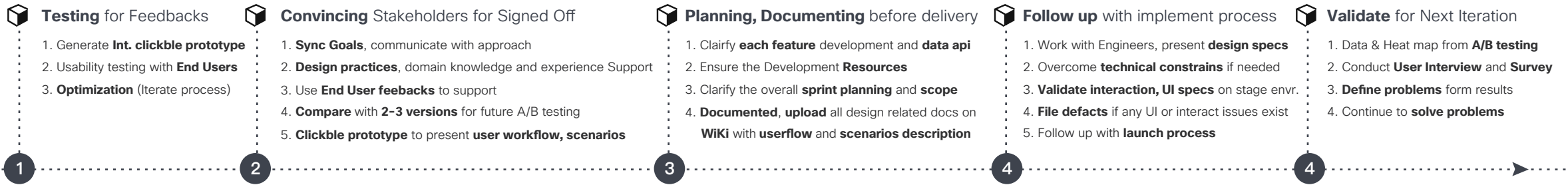
Deliver with **Hi-Fidelity** Mockups



Ensure Product **Standardization**



Teamwork, Dreamwork



GOAL

Let End Users (SecOps) find the solution

Based on the usability testing result/note, validate and optimize the solution

Testing note: **User need batch operations**

Rule Name	Rule Type	Set Rule	Effective Target	Remark	Type	Operator	Date & Time	Action
Low End	Control	Google Drive	Foundation Sec	low end managment	Bulk	haokun	2021-07-04 06:25:07	🔍 🗑️
USB	Control	USB Storage	bogontype123	02/20 meeting	BPM	Admin	2021-07-02 05:20:56	🔍 🗑️
Win Mark	Watermark	Dark Watermark	All	All watermark Contr...	Manual	haokun	2021-03-18 02:58:25	🔍 🗑️
Low End	Control	Google Drive	Foundation Sec	low end managment	Bulk	haokun	2021-07-04 06:25:07	🔍 🗑️
USB	Control	USB Storage	bogontype123	02/20 meeting	BPM	Admin	2021-07-02 05:20:56	🔍 🗑️
Win Mark	Watermark	Dark Watermark	All	All watermark Contr...	Manual	haokun	2021-03-18 02:58:25	🔍 🗑️
Low End	Control	Google Drive	Foundation Sec	low end managment	Bulk	haokun	2021-07-04 06:25:07	🔍 🗑️
USB	Control	USB Storage	bogontype123	02/20 meeting	BPM	Admin	2021-07-02 05:20:56	🔍 🗑️
Win Mark	Watermark	Dark Watermark	All	All watermark Contr...	Manual	haokun	2021-03-18 02:58:25	🔍 🗑️

COLLABORATION

Convincing Stakeholders

Articulating Design Decisions



The screenshot shows a web application interface for 'Exception Policies'. A modal window titled 'Rule Details - "Process Test"' is open, displaying a table of exception rules. The table has columns for Exception Rule, Coverage, On/Off State, Remark, Operator, and Action. The rules listed are Self Test, CPU Test, and RAM Test.

Exception Rule	Coverage	On/Off State	Remark	Operator	Action
Self Test	Device Source: Enterprise Assets OS: Windows	<input type="checkbox"/>	Test	Wenliu	🔍 🔊 ⬇️ ⬆️
CPU Test	Device Source: Enterprise Assets OS: Mac	<input checked="" type="checkbox"/>	Test1	Wenliu	🔍 🔊 ⬇️ ⬆️
RAM Test	Device Source: Enterprise Assets	<input type="checkbox"/>	Test2	Wenliu	🔍 🔊 ⬇️ ⬆️

Stakeholder Expected: Display a **Rule Details Model** after User click on **Details**

The screenshot shows the same web application interface. The 'Process Test' row in the 'Self - Protection' table is expanded to show a detailed view of the rule. The expanded view includes a table with columns for Exception Rule, Coverage, On/Off State, Remark, Operator, and Action.

Exception Rule	Coverage	On/Off State	Remark	Operator	Action
Self Test	Device Source: Enterprise Assets OS: Windows	<input type="checkbox"/>	Test	Wenliu	🔍 🔊 ⬇️ ⬆️
CPU Test	Device Source: Enterprise Assets OS: Mac	<input checked="" type="checkbox"/>	Test1	Wenliu	🔍 🔊 ⬇️ ⬆️
RAM Test	Device Source: Enterprise Assets	<input type="checkbox"/>	Test2	Wenliu	🔍 🔊 ⬇️ ⬆️

My Approach: Expand a row for **Rule Details** after User click on **Details (Proceed Version ✓)**

VALIDATION

UX Validation

Data result after launch

After 7 days of launch, collaborate with data scientists to ensure the data from internal analytics tools are accurate.

Metrics	Attribute	Data	Analysis
Task Completion Rate:	<ul style="list-style-type: none">Abandoned tasksRepeated tasks	<p>5% (good)</p> <p>2% (good)</p>	<p>Users are able to use the feature without any problems</p> <p>Users are understanding how to complete the process</p>
Time on Task:	<ul style="list-style-type: none">High average timeHigh standard deviation	<p>7 minutes (excellent)</p> <p>2 minutes (excellent)</p>	<p>Process is easy or efficiency</p> <p>The process is consistent or easy to predict</p>
Error Rate:	<ul style="list-style-type: none">Frequency of errorsTypes of errors	<p>1 error per user (excellent)</p> <p>10% syntax errors (good)</p>	<p>Users are encountering less problems during the process of setting</p> <p>Program language used in the UI is confusing or unclear</p>
Click-Through Rate:	<ul style="list-style-type: none">Low click-through rate	<p>20% (excellent)</p>	<p>Users are clear with content, easy to find CTA, UI design is intuitive</p>
Engagement Rate:	<ul style="list-style-type: none">Frequency of engagementDuration of engagement	<p>4 times per day (excellent)</p> <p>10 minutes (excellent)</p>	<p>Users are easy to find the policy configuration feature with useful or valuable</p> <p>Users are interest or more like to interact with the process</p>

VALIDATION

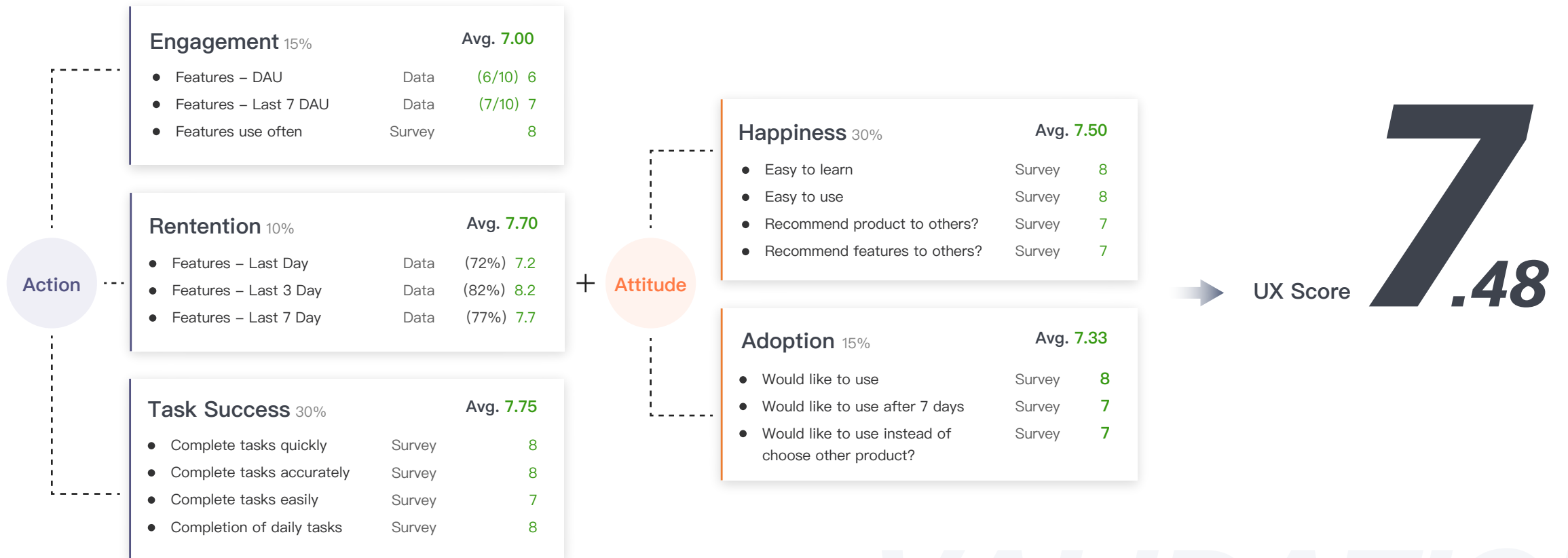
VALIDATION

UX Validation result after new policy configuration features launched

Survey Model

After 7 days of launch, send the survey to 10 SecOps and combine the data from data analytics tools to calculate.

UX Value  **33.6%**

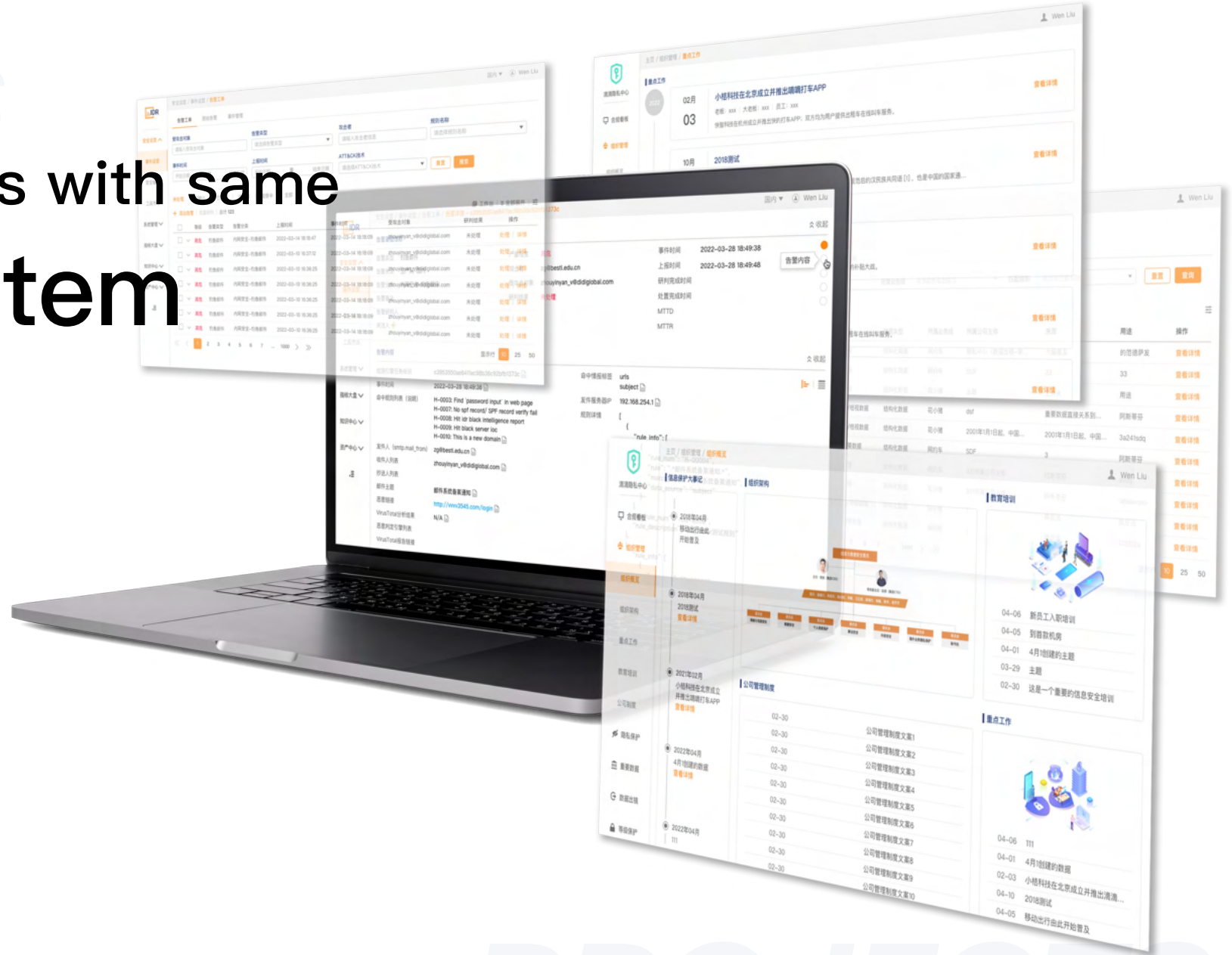


VALIDATION

PROJECTS

Empowering others with same Design System

Applying design system empowerment on other products allows for the seamless integration of design elements and principles, resulting in a cohesive user experience and strengthening the overall brand identity. Fostering a shared understanding and language across cross-functional teams and disciplines.



PROJECTS

EMPOWERMENT

Design System for Cross-Functional Teams

DiDi Privacy Center

Background:

- Compliance Requirement need to build from scratch

Goal:

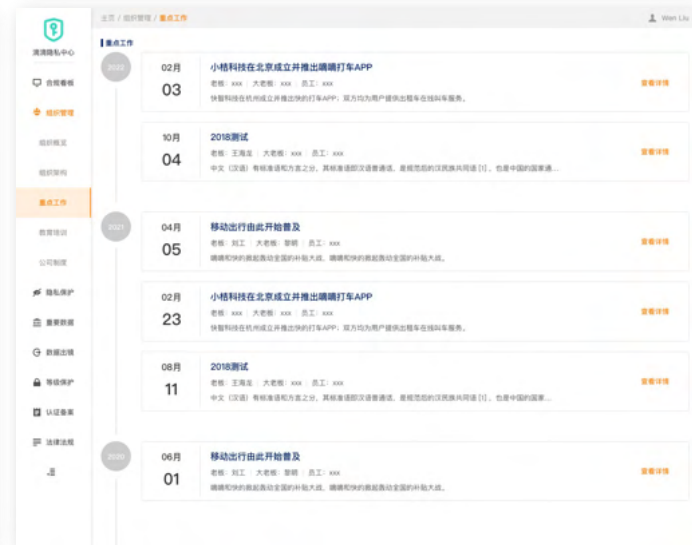
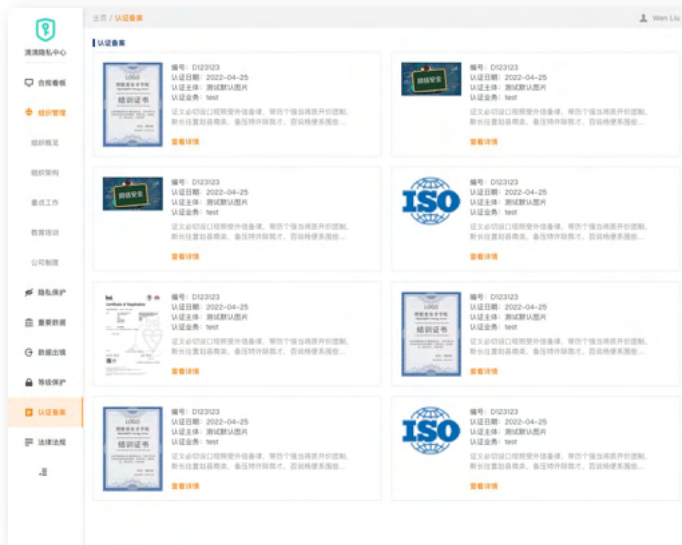
- Clickable Prototype for an **efficient, scalable, and user-friendly** privacy center

Action:

- Empower EagleEye Design System with reusable UI components and design patterns
- Collaborate with cross-functional teams to ensure the design system effectively
- Test and validate the usability through user research

Result:

- Achieve a **cohesive, consistent, and on-brand** privacy center design
- Improve user experience metrics such as **engagement and adoption rates**
- Align with **evolving user needs and business goals**.



EMPOWERMENT

EMPOWERMENT

Design System for Cross-Functional Teams

Anti Intrusion IDR Platform

Background:

- The current design has **inconsistencies and usability issues**

Goal:

- Applying EagleEye Design System for **better consistency, usability, and scalability.**

Action:

- Empower EagleEye Design System** with reusable UI components and design patterns
- Working closely with cross-functional teams** to ensure its effective implementation
- Validate the effectiveness** of the design system through user research and A/B testing.

Result:

- Increase user satisfaction and engagement**, resulting in conversion rates and task success rates
- Establish a **cohesive and consistent brand identity** across the platform
- Align with **evolving user needs and business goals.**

The screenshot displays the IDR platform interface with the following sections:

- 告警基础信息 (Alert Basic Information):** A table showing alert details such as 告警类型 (钓鱼邮件), 严重程度 (高危), 事件时间 (2022-03-28 18:49:38), 告警来源 (生产网-国内), 攻击者 (zg@besti.edu.cn), 上报时间 (2022-03-28 18:49:48), 告警分类 (内网安全-钓鱼邮件), 受攻击对象 (zhouyinyan_v@didiglobal.com), 研判完成时间, 告警备注, 研判结果 (未处理), 处置完成时间, 告警研判人, 关注人 (+), MTTD, and MTTR.
- 告警内容 (Alert Content):** A detailed view of the alert, including 检测引擎任务标识 (c3953550ae8411ec98b36c92bfb1373c), 事件时间 (2022-03-28 18:49:38), 命中规则列表 (说明) (H-0003: Find 'password input' in web page, H-0007: No spf record/ SPF record verify fail, H-0008: Hit idr black intelligence report, H-0009: Hit black server loc, H-0010: This is a new domain), 发件人 (smtp.mail_from) (zg@besti.edu.cn), 收件人列表 (zhouyinyan_v@didiglobal.com), 抄送人列表, 邮件主题 (邮件系统备案通知), 恶意链接 (http://www3545.com/login), VirusTotal分析结果 (N/A), 恶意判定引擎列表, VirusTotal报告链接, and 页面截屏.
- 事件溯源 (Event Tracing):** A table showing event details for 2022-03-28 18:49:38 | 高危 | 钓鱼邮件. The table includes columns for 等级 (高危), 告警类型 (钓鱼邮件), 告警分类 (内网安全-钓鱼邮件), 事件时间 (2022-03-14 18:18:09), 处理完成时间, 告警研判人, 研判结果 (未处理), and 操作 (详情).
- 安全运营标准 (Security Operation Standards):** A table with columns for 事件标签 (Phasellus a quam elementum, scelerisque nulla ac, tincidunt nisi.), 常见误报 (Lorem ipsum dolor sit amet, consectetur adipiscing elit.), 告警描述 (lobortis sagittis eget ac nibh. Pellentesque sit amet diam sit amet eros), 处理流程 (Aliquam sit amet fringilla turpis. Morbi ac augue erat. Nullam nec lorem), 关注要点 (nibh. Phasellus pellentesque, metus vitae accumsan gravida, 业务术语 (Morbi rutrum, odio ac pulvinar egestas, metus mauris), and 告警示例 (Etiam tincidunt orci sit amet lorem elementum pulvinar. Duis nisi felis).
- 告警分析路径 (Alert Analysis Path):** A flow diagram showing the process: 异常引擎检测 (Anomaly Engine Detection) -> 事件路由网关 (Event Routing Gateway) -> 溯源分析引擎 (Tracing Analysis Engine).



MENTORING

Talent Development

EagleEye

Large screen

Data Visualization

-  **Mentored and collaborated with intern** to successfully complete projects from **conception to launch**.
-  **Enhanced product competitiveness** and **increased client conversion** rates during commercialization.



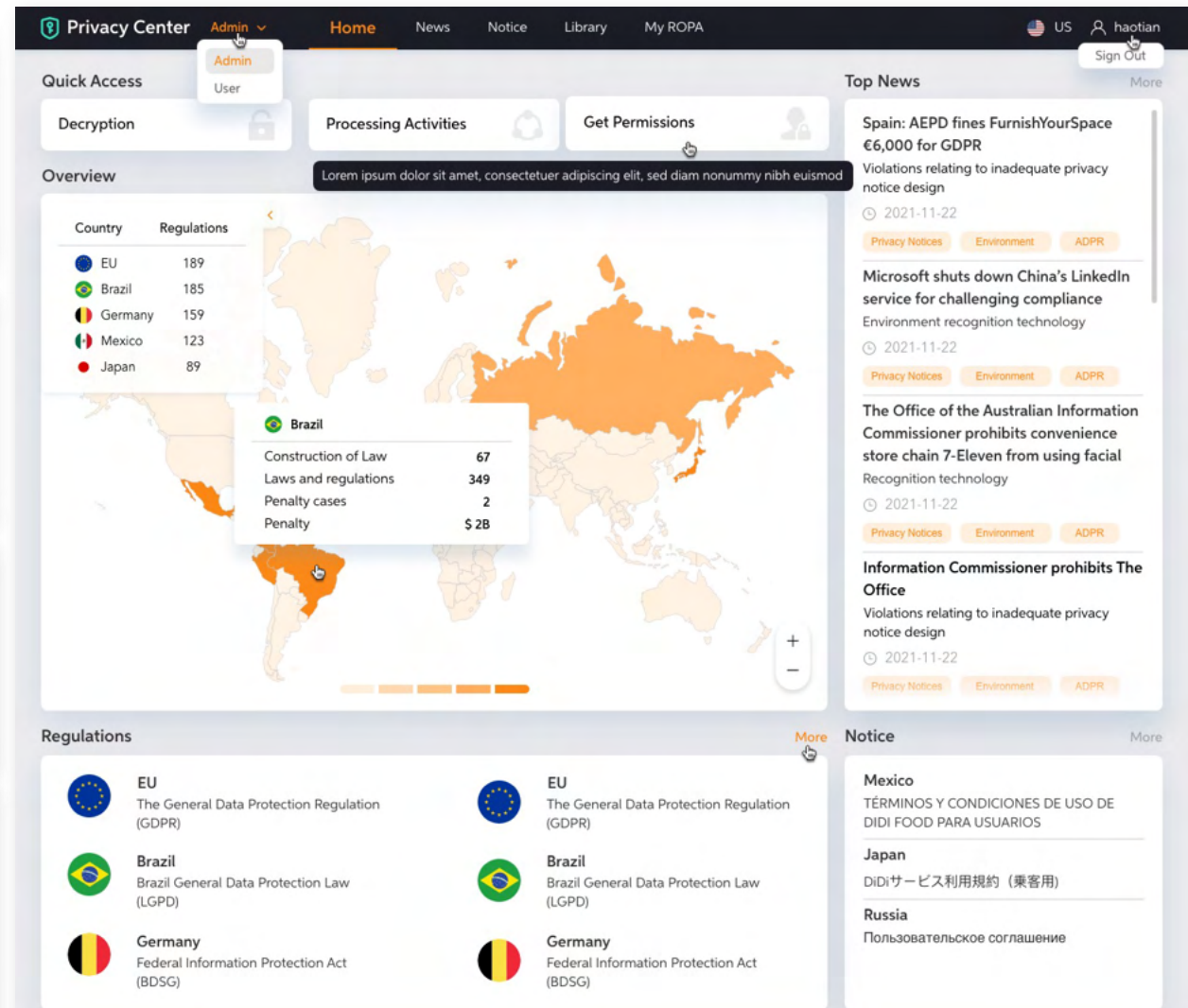
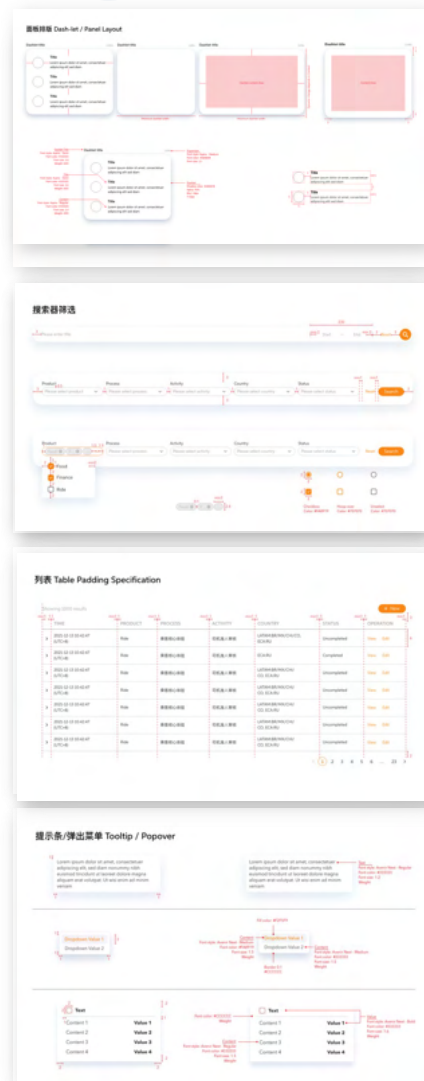
MENTORING

Talent Development

DiDi Intl. Privacy Platform

Provided mentorship to intern while collaborating on the complete re-design the entire platform for global internal customers.

Concluded design patterns and specification, resolved UX issues to achieve a consistent and intuitive design that increased task success, adoption, and engagement rates and met user needs.



Influence on PMs

“Wen Liu not only can complete the visual design excellently, but also has a deep accumulation of product interaction friendliness and security product design logic. He has a good sense of service and actively helped me solve many problems in the product design of Eagle Eye”

EagleEye Sr Product Manager
SSTG/Foundation Product/
Endpoint Sec



“With complete design ideas and comprehensive abilities, have great enthusiasm and strong initiative for design work, and have a strong sense of service. He can think deeply about improving the overall design level of the system.”



SSO Center – Product Lead
SSTG/Info Sec/Engineering Platform/
Sec Architecture

“Thanks to Wen Liu for supporting the IDR platform project, helping the platform to standardize a unified visual style, improving the platform user experience, and adding support for internationalization. Looking forward to the continued cooperation in the subsequent platform UI improvements”



Anti-Intrusion IDR – Product Lead
SSTG/Info Sec/Cyber Sec/
Anti-Intrusion

“From the international privacy platform to the domestic privacy center product build, Wen not only has continuous high-quality design output, but also led the team to build UI design specifications to provide strong support for compliance work, and all teams are very recognized.”



Privacy Center – Product Manager
SSTG/Info Sec/Engineering Platform/
Sec Architecture

■ Design Showcase

Cisco Network Assurance Engine Prototype



Dashboard

Epoch Trend

Smart Events by Severity



Critical	Major	Minor	Warning	Info	Total
314	998	54	294	675	2,335

Category	Critical	Major	Minor	Warning	Info	Total
Tenant Endpoint	196	187	0	4	224	611
Real Time Change Analysis	0	376	15	127	74	592
Tenant Forwarding	50	191	21	161	108	531
Resource Security	66	238	18	1	261	584
Resource Utilization	0	0	0	1	4	5
System	2	6	0	0	4	12
Compliance	0	0	0	0	1	2

Unhealthy Count by Resource



App Profiles 29 / 180	Bridge Domains 24 / 85	Contracts 10 / 50	Endpoints 31 / 295	Endpoint Group (EPG) 132 / 1,529	External Routes 22 / 186
External Routed Networks (L3Outs) 20 / 226	Interfaces 32 / 245	Internal Subnets 167 / 189	Leaf 2 / 4	Tenants 19 / 226	VRFs 24 / 380

Endpoints by Leaf



Leaf	Unhealthy EPs	Total EPs
candid5-leaf1	185	189
candid5-leaf2	18	21
candid5-leaf3	7	7
candid5-leaf4	5	5

[View endpoint issues on all leaves](#)

Routes by Leaf



Leaf	Internal...	External...	Total...
candid5-leaf1	1,092	101	1,190
candid5-leaf2	1,038	0	1,038
candid5-leaf3	611	99	710
candid5-leaf4	345	15	360

[View route counts on all leaves](#)

Policy CAM by Leaf



Leaf	% Used
candid5-leaf1	0.68%
candid5-leaf2	0.46%
candid5-leaf3	0.28%
candid5-leaf4	0.00%

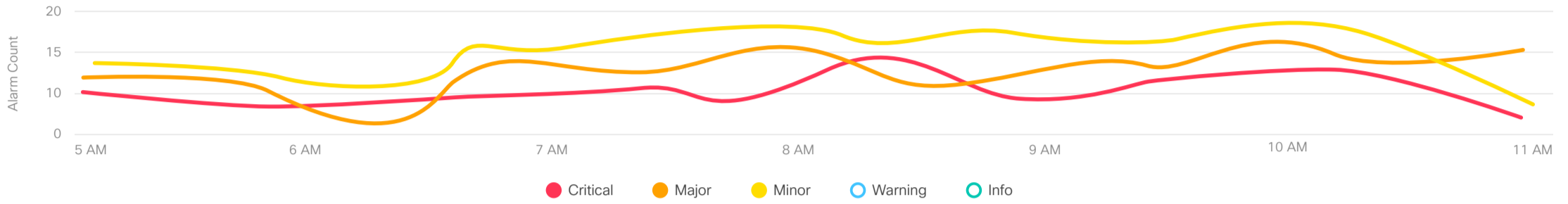
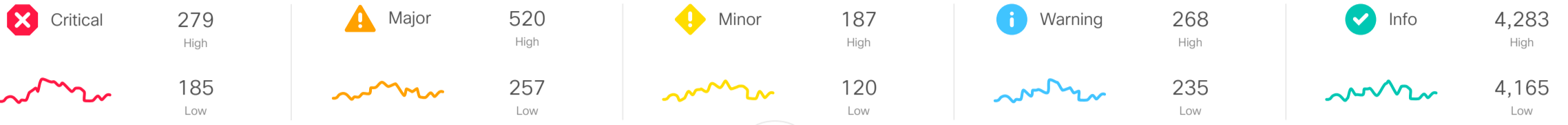
[View policy CAM usage on all leaves](#)



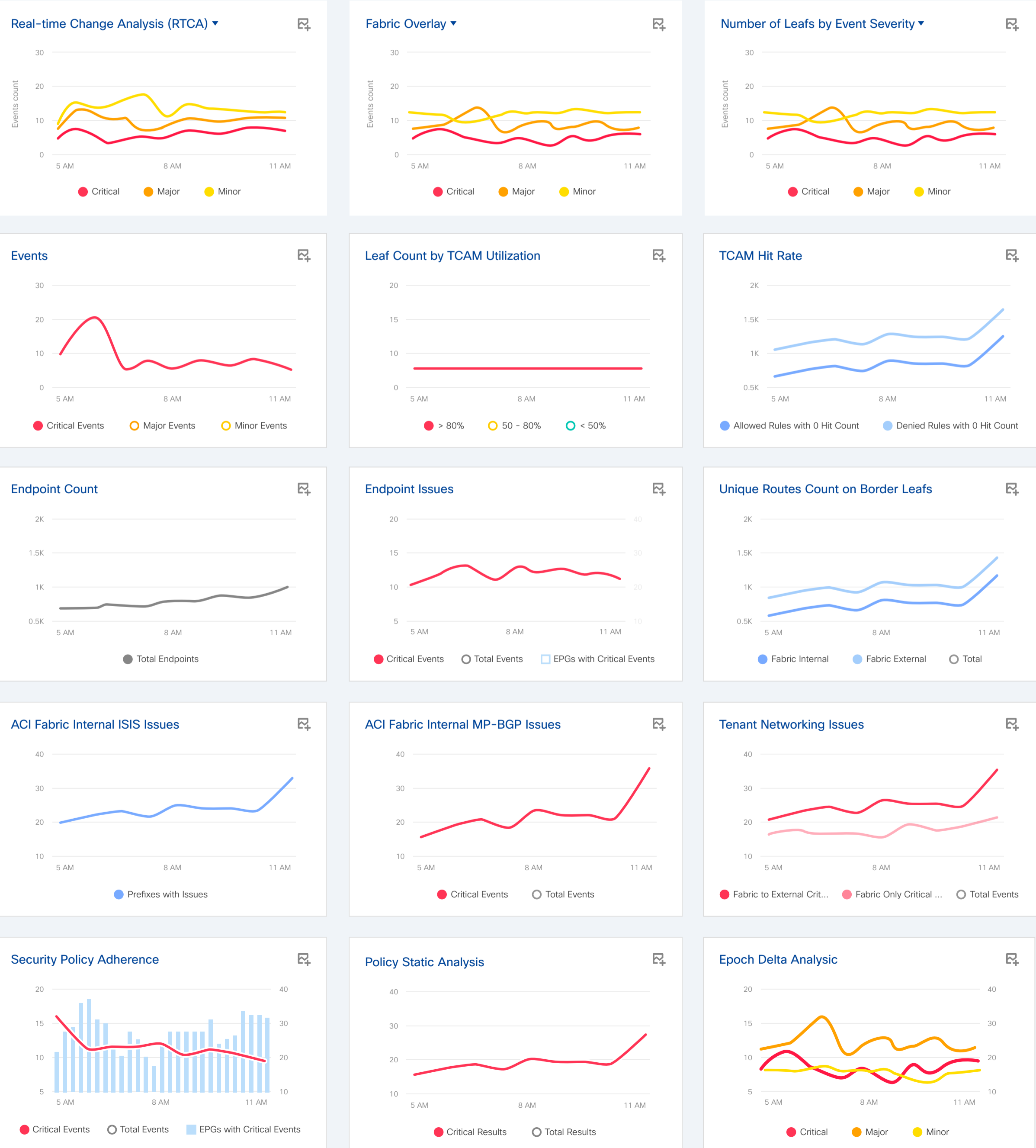
Dashboard

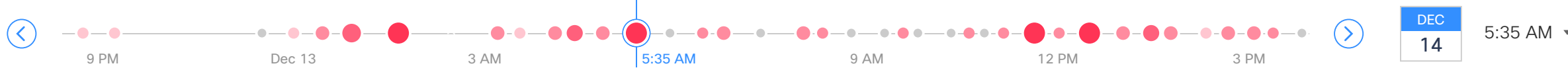
Epoch Trend

Events Trend

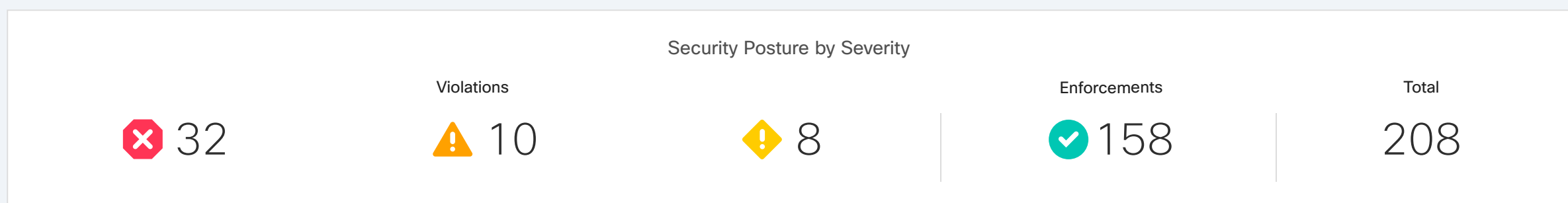


Event Analysis





Analyze / Policy / Security Adherence ★



Security Posture by Policy Type

Type	Violations	Enforcements
Deny Policy	✖ 32	✔ 90
Allow Policy	⚠ 10	✔ 34
Deny Log Policy	⚠ 3	✔ 22
Allow Log Policy	⚠ 5	✔ 12

Root Causes for Security Violations

Root Cause	Leaf Count with Violations
Controller-Leaf Out of Sync	5 of 20 Leafs
Leaf-Hardware Out-of-Sync	4 of 20 Leafs
Both root causes	2 of 20 Leafs

Top Leafs by Security Violations

Leaf	BizPriority	Violations
rtp1-ac0...w1011	P1	✖ ⚠ ⚠
rtp1-ac0...w1101	P1	✖ ⚠ ⚠
rtp1-aa1...w3911	P1	✖ ⚠ ⚠
rtp1-aw...w3914	P2	✖ ⚠ ⚠
rtp1-au0...w1112	P2	✖ ⚠ ⚠

[View violations on 12 of 20 Leafs](#)

Top Tenants by Security Violations

Tenant	BizPriority	Violations
Pepsi	P1	✖ ⚠ ⚠
Coke Cola	P1	✖ ⚠ ⚠
Target	P1	✖ ⚠ ⚠
Intuit	P2	✖ ⚠ ⚠
Macy's	P2	✖ ⚠ ⚠

[View violations on 7 of 18 tenants](#)

Top Application Profiles by Security Violations

Application Profile	BizPriority	Violations
lae2_ga3	P1	✖ ⚠ ⚠
platfora-1-poc	P1	✖ ⚠ ⚠
metr...-storage-ap	P1	✖ ⚠ ⚠
platfora-1-poc	P2	✖ ⚠ ⚠
simdmz-l3Out	P2	✖ ⚠ ⚠

[View violations on 14 of 26 application profiles](#)

Top EPGs by Security Violations

EPG	BizPriority	Violations
lae2inp	P1	✖ ⚠ ⚠
platfora-1-app	P1	✖ ⚠ ⚠
nas-mc-np...-01-epg	P1	✖ ⚠ ⚠
platfora-1-app	P2	✖ ⚠ ⚠
infra-osinfra-extNet	P2	✖ ⚠ ⚠

[View violations in 17 of 30 EPGs](#)

Top EPG Pair by Security Issues

Source EPG	Destination EPG	BizPriority	Violations
lae2inp	hadoop-1-cluster	P1	✖ ⚠ ⚠
platfora-1-app	fn-d-lae2inp-extNet	P1	✖ ⚠ ⚠
nas-mc-nprd-svm-01-epg	infra-osinfra-extNet	P1	✖ ⚠ ⚠
platfora-1-app	nas-internal-prd-svm-03-epg	P2	✖ ⚠ ⚠
infra-osinfra-extNet	aci-test-dmz-epg	P2	✖ ⚠ ⚠

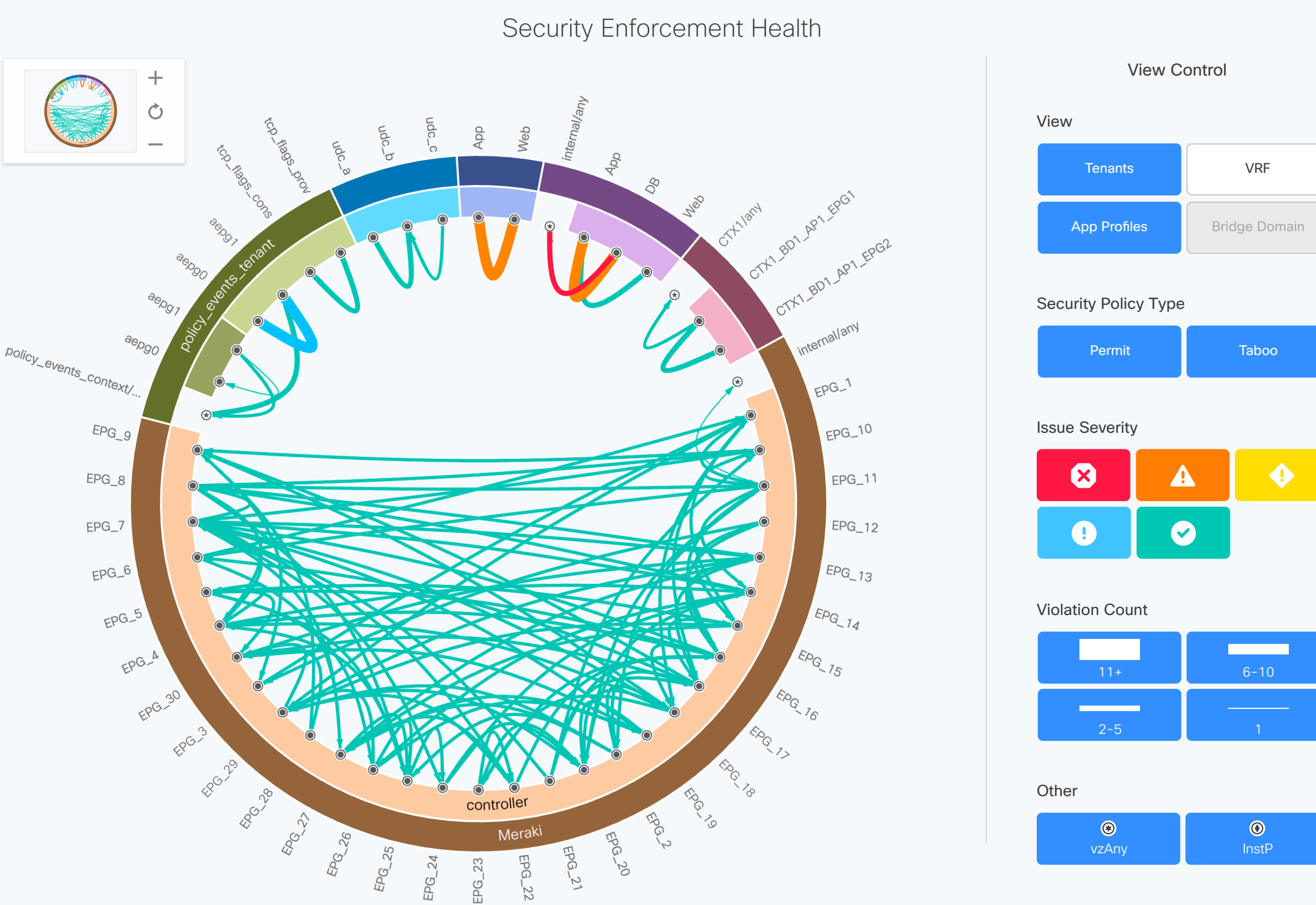
[View violations in 12 of 128 EPG pairs](#)

Least Used Security Policies by Hit Count

Provider EPG	Provider EPG	Leaf	Contract	Filter	W/In 1 Hr.	W/In 1 Day	W/In 1 Wk.	W/In 1 Mo.	Cumulative
platfora-1-app	platfora-6-app	rtp1-ae07-fab1-sw...	tn-regress5/brc-infra-...	flt-dst-syslog-filter	0	0	0	0	0
platfora-2-app	platfora-7-app	rtp1-ac09-fab1-sw...	tn-regress5/brc-infra-...	flt-udp-rpc	0	0	0	0	0
platfora-3-app	platfora-8-app	rtp1-aa10-fab1-sw...	tn-regress5/brc-infra-...	icmp	0	0	0	0	0
platfora-4-app	platfora-9-app	rtp1-aw10-fab1-sw...	tn-regress5/brc-infra-...	flt-dst-tcp-filter	0	0	0	0	0
platfora-5-app	platfora-10-app	rtp1-au09-fab1-sw...	tn-regress5/brc-infra-...	flt-dst-syslog-filter	0	0	0	0	0

[View all 128 Leafs](#)

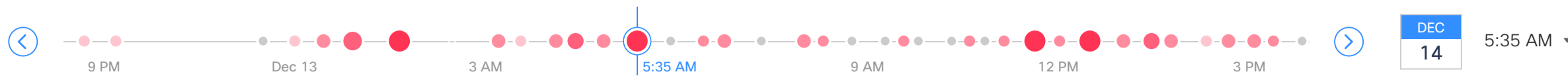
LEAF candid-leaf1 x
TENANT uni/tn-policy_events_tenant x
LEAF candid-leaf1 x
TENANT uni/tn-policy_events_tenant x
Reset



Tenant Security Events

10 total events

Severity	Event Code	Description	Provider EPG	Consumer EPG
✔	APPLIANCE_WEB_SERVICES_OPERATION_NORMAL	Infrastructure resources operating normally	DB	internal/any
⚠	APPLIANCE_DATABASE_REACHING_LIMIT	Database has reached a key utilization threshold	epg1-valid	ctx0/any
✖	CLUSTER_OPERATING_BEYOND_CAPACITY	Cluster is operating at a lower capacity in comp...	DB	App
✔	APPLIANCE_INFRA_RESOURCE_OPERATION_NORMAL	Infrastructure resources operating normally	DB	App
✔	APPLIANCE_DATABASE_OPERATION_NORMAL	Infrastructure resources operating normally	DB	App
✖	CLUSTER_OPERATING_BEYOND_CAPACITY	Cluster is operating at a lower capacity in com...	DB	App
✔	APPLIANCE_DATABASE_OPERATION_NORMAL	Infrastructure resources operating normally	DB	App



LEAF candid-leaf1 x TENANT uni/tn-policy_events_tenant x LEAF candid-leaf1 x TENANT uni/tn-policy_events_tenant x Reset

Security Enforcement Health

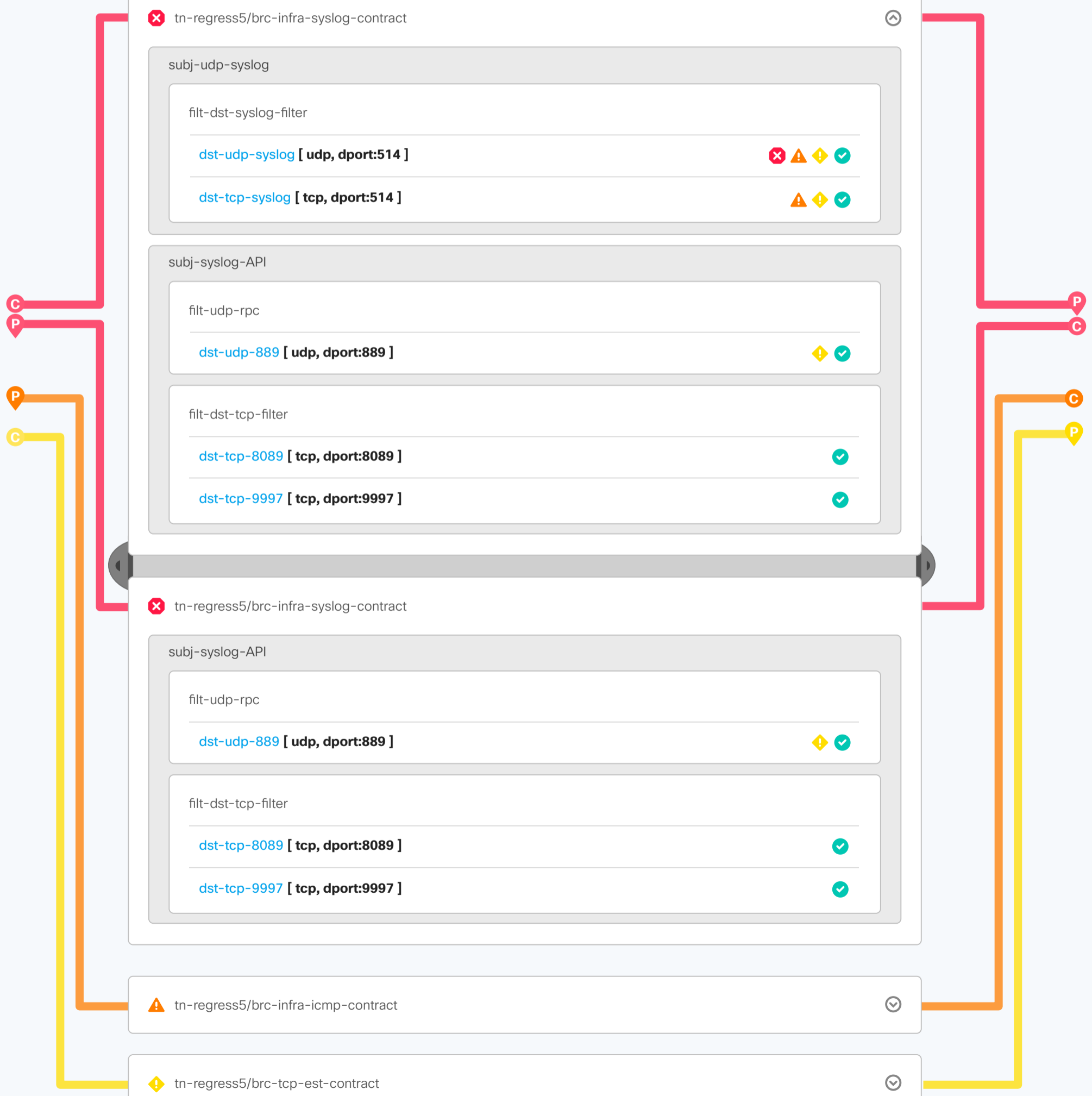
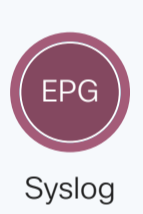
Back

tn-regress5/brc-infra-syslog-contract

- subj-udp-syslog
 - filt-dst-syslog-filter
 - dst-udp-syslog [udp, dport:514]
 - dst-tcp-syslog [tcp, dport:514]
 - subj-syslog-API
 - filt-udp-rpc
 - dst-udp-889 [udp, dport:889]
 - filt-dst-tcp-filter
 - dst-tcp-8089 [tcp, dport:8089]
 - dst-tcp-9997 [tcp, dport:9997]

tn-regress5/brc-infra-icmp-contract

tn-regress5/brc-tcp-est-contract





Epoch Delta / Epoch Delta Analysis ★

Epoch Delta Analysis

Delta Analysis Analysis Management

Delta Analysis 1

Earlier Epoch: 04/04/2018 1:46:30 PM PDT

Later Epoch: 04/05/2018 5:56:30 PM PDT

Time Range: 1 day 4 hr 10 min 00 sec

Dashboard | Health Delta | **Policy Delta** | State Delta | Capacity Delta | Operator Delta

Added Deleted Modified Unchanged

Q Search in policy i

Affected Resources (8)

- Tenant A
 - BD AA
 - BD AB
 - EPG 1
 - 2** EPG 2
 - EPG
 - uni/tn-david-any-zero-cases/ap-n...
 - [Cross launch to APIC](#)
 - 1 Added, 1 Deleted
 - ✖ 7 ⚠ 23 ⚠ 2
 - EPG 3
 - Contract 11
 - Contract 12

Policy Viewer

[Export policy](#) ■ ■

0 of 0 ^ ▼

```

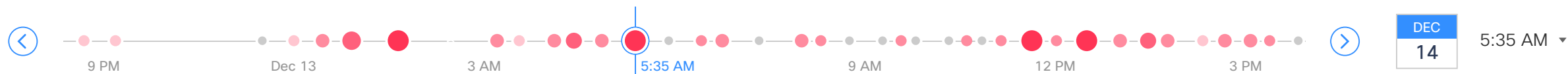
1 <?xml version="1.0" ?>
2 <polUni dn="uni" nameAlias="" >
3   <dbgDebugP descr="" dn="uni/dbg" name="" nameAlias="" />
4   <l2extDomP dn="uni/l2dom-navtestdom" name="navtestdom"
5   nameAlias="" ownerKey="" ownerTag="" >
6     <infraRsVlanNs dn="" tDn="uni/infra/vlanns-[navtestvlanpool_]_stat-
7   ic" />
8   </l2extDomP>
9   <l2extDomP dn="uni/l2dom-l2dom_epdemo" name="l2dom_epdemo"
10  nameAlias="" ownerKey="" ownerTag="" >
11     <infraRsVlanNs dn="" tDn="uni/infra/vlanns-[ep-
12  demo_vlan_pool]-static" />
13   </l2extDomP>
14   <l2extDomP dn="uni/l2dom-l2dom_P" name="l2dom_P" nameAlias=""
15   ownerKey="" ownerTag="" >
16     <infraRsVlanNs dn="" tDn="uni/infra/vlanns-[Ext-vlans]-static" />
17   <l2extDomP dn="uni/l2dom-l2dom_global" name="l2dom_global"
18   nameAlias="" ownerKey="" ownerTag="" >
19     <infraRsVlanNs dn="" tDn="uni/infra/vlanns-[vlanPool_global]-stat-
20   ic" />
21   </l2extDomP>
22   <bbbUserEp descr="" dn="uni/userext" name="" nameAlias="" owner-
23   Key="" own
24   <aaaUserRole descr="" dn="" name="read-all"
25   nameAlias="" ownerKey="" ownerTag="" privType="readPriv" />
26   <aaaUserRole descr="" dn="" name="aaa" nameAlias=""
27   ownerKey="" ownerTag="" privType="readPriv" />
28   HighSet="100.000000" warnLowReset="0.000000" warnLowSet="0.000000" />
29   </statsColl>
30   mal="0.000000" propId="compRcvdErrPktsDropRate" warnHighRe-
31   set="9.000000"
32
33   <lldplfPol adminRxSt="disabled" adminTxSt="disabled" descr=""
34   dn="" name="lldpOff" nameAlias="" ownerKey="" ownerTag="" />

```

Audit Log

● 10 ● 21 ● 15

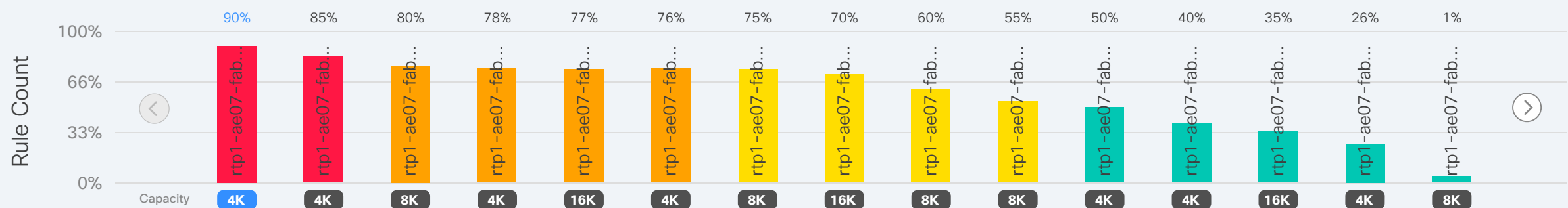
- 04/04/2018 1:46:30.017 PM PDT Dhruv Jain
 - RsBd added
 - uni/tn-epoch_delta_test_1/ap-policy-diff/epg-EPG1/rsbd
 - matchT:AtleastOne, prio:unspecified, tnVzBrCPName:
 - [Cross launch to APIC](#)
- 04/04/2018 1:46:30.017 PM PDT Dhruv Jain
 - RsBd added
 - uni/tn-epoch_delta_test_1/ap-policy-diff/epg-EPG1/rsbd
 - No chang set
 - [Cross launch to APIC](#)



Policy CAM Analysis

Enter search criteria Reset

[View all 128 leafs](#)



Associated Policies for rtp1-ae07-fab1-sw1011

Provider Tenant	Consumer Tenant	Provider EPG	Consumer EPG	Contract	Filter
Macy's_1 12,810 / 61,000	lae2inp 2,890 / 12,810	hadoop-1-cluster 2,842 / 12,810	internal 2,835 / 12,810	infra-icmp-contract 2,875 / 12,810	icmp 2,845 / 12,810
Intuit 12,810 / 61,000	platfora-1-app 2,718 / 12,810	fnd-lae2inp-extNet 2,793 / 12,810	internal 2,787 / 12,810	infra-tcp-est-contract 2,732 / 12,810	tcp-est-filter 2,657 / 12,810
Target 12,810 / 61,000	nas-mc-...01-epg 2,675 / 12,810	infra-osinfra-extNet 2,610 / 12,810	shared 2,647 / 12,810	prod-inter-db-contract 2,642 / 12,810	dst-...-1500-2000-filter 2,493 / 12,810
Pepsi 12,810 / 61,000	platfora-1-app 2,432 / 12,810	nas-internal-03-... 2,532 / 12,810	policy_events_context 2,574 / 12,810	test-udp-rpc 2,413 / 12,810	src-udp-889-filter 2,375 / 12,810
Other 12,810 / 61,000	Other 2,822 / 12,810	Other 2,786 / 12,810	Other 2,823 / 12,810	Other 2,794 / 12,810	Other 2,810 / 12,810

Manage Compliance

Object Selectors (12)
Traffic Selectors (7)
Compliance Requirements (6)
Compliance Requirement Sets (4)

[+ Create New Object Selector](#)

Create New Obejct Selector

Object Selector Name

Description (Optional)

Object Selector Type

Included EPGs

Include EPGs in

that are also in

Include EPGs in

[Add Included EPGs](#)

Excluded EPGs (Optional)

Exclude EPGs in

that are also in

[Add Excluded EPGs](#)

EPGs Matching the Object Selector Criteria

12 EPGs total

EPG Name ▾	DN
Filter	Filter
amb2_epg1	uni/tn-amb/ap-amb2-AP/epg-amb2_epg1
amb2_epg2	uni/tn-amb/ap-amb2-AP/epg-amb2_epg2
amb2_epg3	uni/tn-amb/ap-amb2-AP/epg-amb2_epg3
ctx1-bd1-epg1	uni/tn-bell01/ap-ctx1-ap1/epg-ctx1-bd1-epg1
ctx1-bd1-epg2	uni/tn-bell01/ap-ctx1-ap1/epg-ctx1-bd1-epg2
ctx1-bd2-epg1	uni/tn-bell01/ap-ctx1-ap1/epg-ctx1-bd2-epg1
ctx1-bd2-epg2	uni/tn-bell01/ap-ctx1-ap1/epg-ctx1-bd2-epg2
dhcp-Client1	uni/tn-common/ap-dhcpAP1/epg-dhcp-Client1
dhcp-Client2	uni/tn-common/ap-dhcpAP1/epg-dhcp-Client2
dhcp-Server	uni/tn-common/ap-dhcpAP1/epg-dhcp-Server

< 1 2 >

Rows 10 25 50 100

Cancel
Save

12 Object Selectors | ☰ | ⚙️

Obejct Selector Name	Obejct Selector Type	Associated Requirements	Description
Filter	Filter ▾	Filter	
⚙️ Selector 1	EPG	Req4 Req5 Req3 View All 11	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed hendrerit nulla a lectus vulputate, volutpat condimentum quam egestas. Sed id neque sed nulla tincidunt egestas maximus vitae felis.
⚙️ Selector 2	EPG	Req7 Req3 Req2 View All 12	Pellentesque quis ligula auctor, bibendum ipsum nec, pellentesque enim. Etiam vestibulum diam sem, ut mattis nulla finibus at. Proin erat lorem, vehicula a lectus sed, commodo lobortis quam.
⚙️ Selector 3	EPG	Req4 Req5 Req3 View All 13	Proin a quam quis lectus blandit congue vitae sed orci. Cras bibendum consequat turpis, id pellentesque purus volutpat vehicula. Etiam iaculis justo vitae sem sollicitudin, vitae euismod enim elementum.
⚙️ Selector 4	BD	Req4 Req8	Fusce elementum dignissim diam, id volutpat tortor. Aliquam vitae quam luctus, fringilla augue quis, pulvinar diam. Duis quis lorem

Assurance Groups

+ Create New Assurance Group | Schedule

Sort by Scheduled

15 total Assurance Groups

Current running order (4 Active Assurance Groups)



Analysis interval is 15 minutes. (Approximately 60 minutes to run one cycle)

Control buttons: Delete, Close, Stop

Live Analysis Assurance Group 1 [Refresh] [Settings]	Live Analysis Assurance Group 5 [Checkmark] [Settings]	Live Analysis Assurance Group 7 [Checkmark] [Settings]	Live Analysis Assurance Group 14 [Checkmark] [Settings]
Live Analysis Assurance Group 2 [Refresh] [Settings]	Live Analysis Assurance Group 3 [Checkmark] [Settings]	Offline Analysis Assurance Group 4 [Refresh] [Settings]	Offline Analysis Assurance Group 6 [Refresh] [Settings]
Live Analysis Assurance Group 8 [Checkmark] [Settings]	Live Analysis Assurance Group 9 [Checkmark] [Settings]	Live Analysis Assurance Group 10 [Checkmark] [Settings]	Live Analysis Assurance Group 11 [Checkmark] [Settings]
Live Analysis Assurance Group 12 [Checkmark] [Settings]	Offline Analysis Assurance Group 13 [Refresh] [Settings]	Live Analysis Assurance Group 15 with a ... [Checkmark] [Settings]	Live Analysis Assurance Group 16 with a ... [Checkmark] [Settings]



Thank You