ZenithLive 24

Investor Innovations Briefing

June 12, 2024

Experience
your world
your cloud
your enterprise
your access
your
workforce
your future
secured

Safe Harbor

FORWARD-LOOKING STATEMENTS

Unless otherwise noted, all numbers presented will be on an adjusted, non-GAAP basis. Reconciliation of GAAP to non-GAAP financial measures is in the appendix of this presentation.

This presentation has been prepared by Zscaler, Inc. ("Zscaler") for informational purposes only and not for any other purpose. Nothing contained in this presentation is, or should be construed as, a recommendation, promise or representation by the presenter or Zscaler or any officer, director, employee, agent or advisor of Zscaler. This presentation does not purport to be all-inclusive or to contain all of the information you may desire.

This presentation contains forward-looking statements. All statements other than statements of historical fact, including statements regarding our future financial and operating performance, including our financial outlook for the fourth quarter of fiscal 2024 and full year fiscal 2024, our planned products and upgrades, business strategy and plans and objectives of management for future operations of Zscaler are forward-looking statements. These statements involve known and a significant number of unknown risks, uncertainties, assumptions and other factors that could cause results to differ materially from statements made in this message, including any performance or achievements expressed or implied by the forward-looking statements. Moreover, we operate in a very competitive and rapidly changing environment, and new risks may emerge from time to time. It is not possible for us to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results or outcomes to differ materially from those contained in any forward-looking statements we may make, including but not limited to the ongoing effects of inflation and geopolitical events on our business, operations and financial results and the economy in general; our limited operating history; our ability to identify and effectively implement the necessary changes to address execution challenges; risks associated with managing our rapid growth, including fluctuations from period to period; our limited experience with new product and subscription and support introductions and the risks associated with new products and subscription and support offerings, including the discovery of software bugs; our ability to attract and retain new customers; the failure to timely develop and achieve market acceptance of new products and subscriptions as well as existing products and subscription and support; rapidly evolving technological developments in the market for network security products and subscription and support offerings and our ability to remain competitive; length of sales cycles; and general market, political, economic and business conditions. Additional risks and uncertainties that could affect our financial and operating results are included in our most recent filings with the Securities and Exchange Commission ("SEC"). You can locate these reports though our website at http://ir.zscaler.com or on the SEC website at www.sec.gov.

In some cases, you can identify forward-looking statements by terms such as "anticipate," "believe," "continues," "contemplate," "could," "estimate," "expect," "explore," "intend," "likely," "may," "plan," "potential," "predict," "project," "should," "target," "will" or "would" or the negative of these terms or other similar words. Zscaler based these forward-looking statements largely on its current expectations and projections about future events that it believes may affect its business. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements. All forward-looking statements in this message are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

Agenda

Expanding Our Platform Opportunity

Jay Chaudhry | Founder, Chairman, and CEO

Platform Innovations

Syam Nair | CTO and EVP of R&D

Raanan Raz | VP & GM, Data Analytics

Deepen Desai | Chief Security Officer

Moinul Khan | VP & GM, Data Protection

Naresh Kumar | VP, Product Management - Zero Trust Networking

Q&A

Break

Customer Journeys

Sanmina

Gray Television

Go-to-Market Strategy

Mike Rich | Chief Revenue Officer and President of Global Sales

Closing

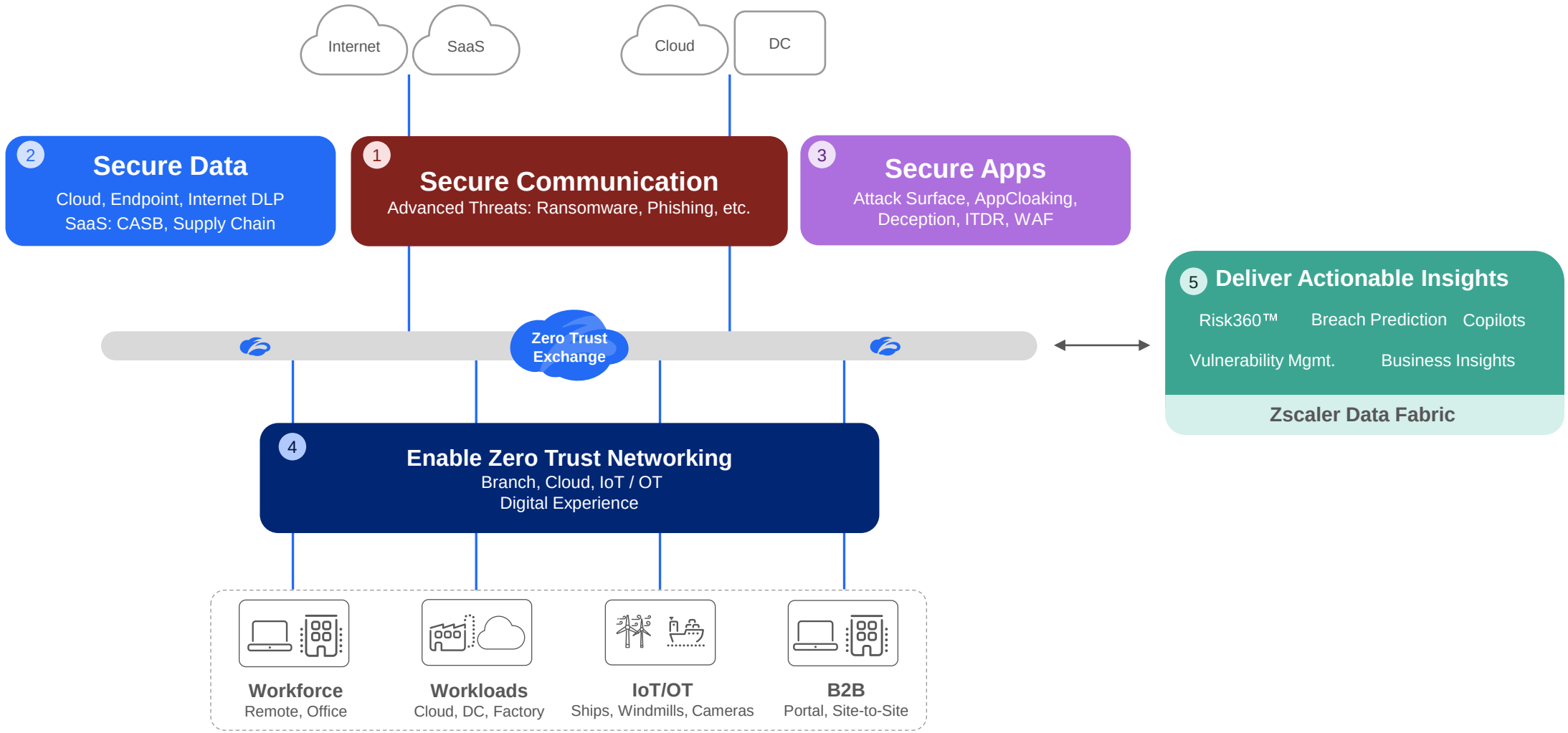
Jay Chaudhry | Founder, Chairman, and CEO

Q&A

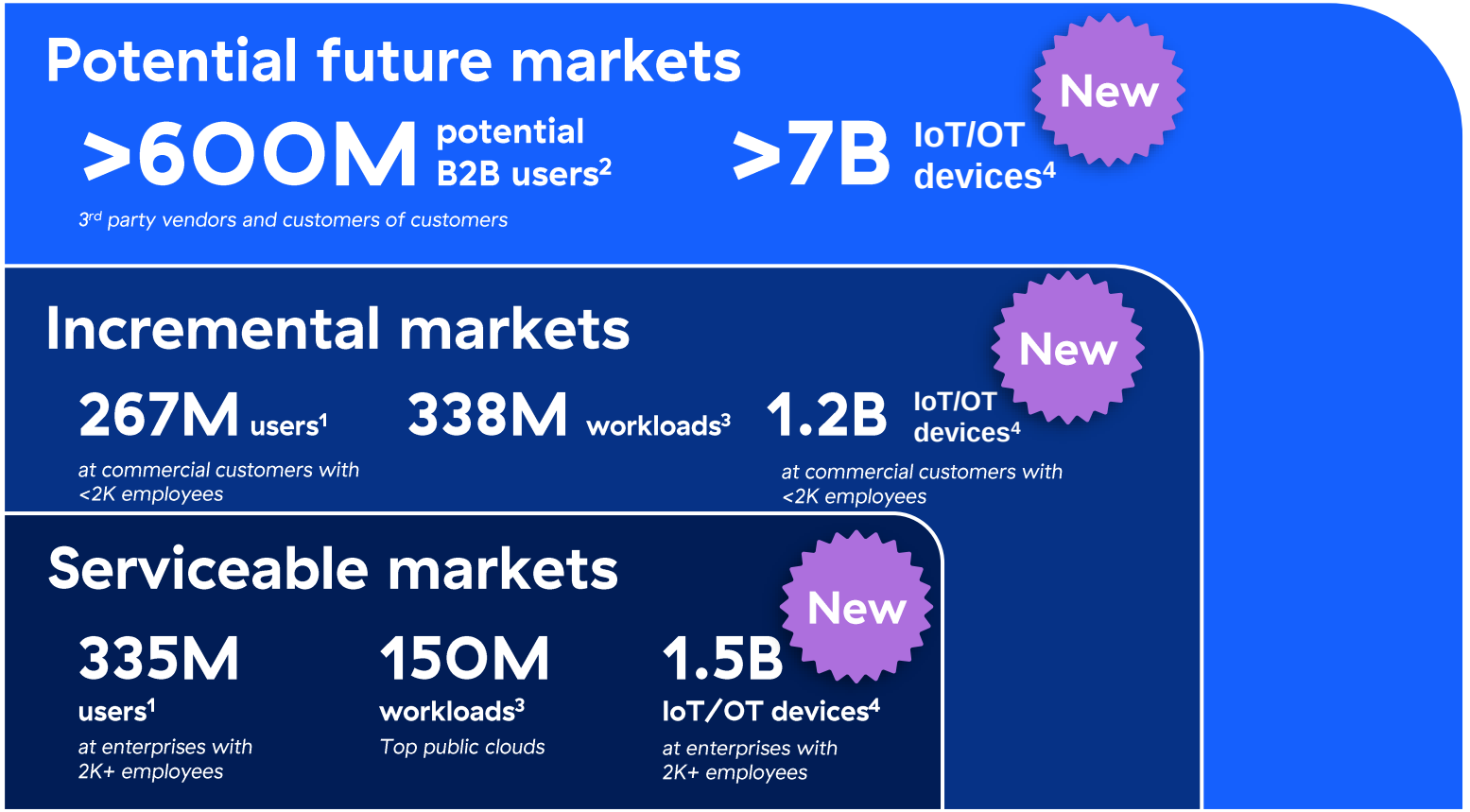
Expanding Our Platform Opportunity

Jay Chaudhry
Founder, Chairman, and CEO

Five comprehensive solutions built on an integrated platform



Expanding serviceable market to IoT/OT devices



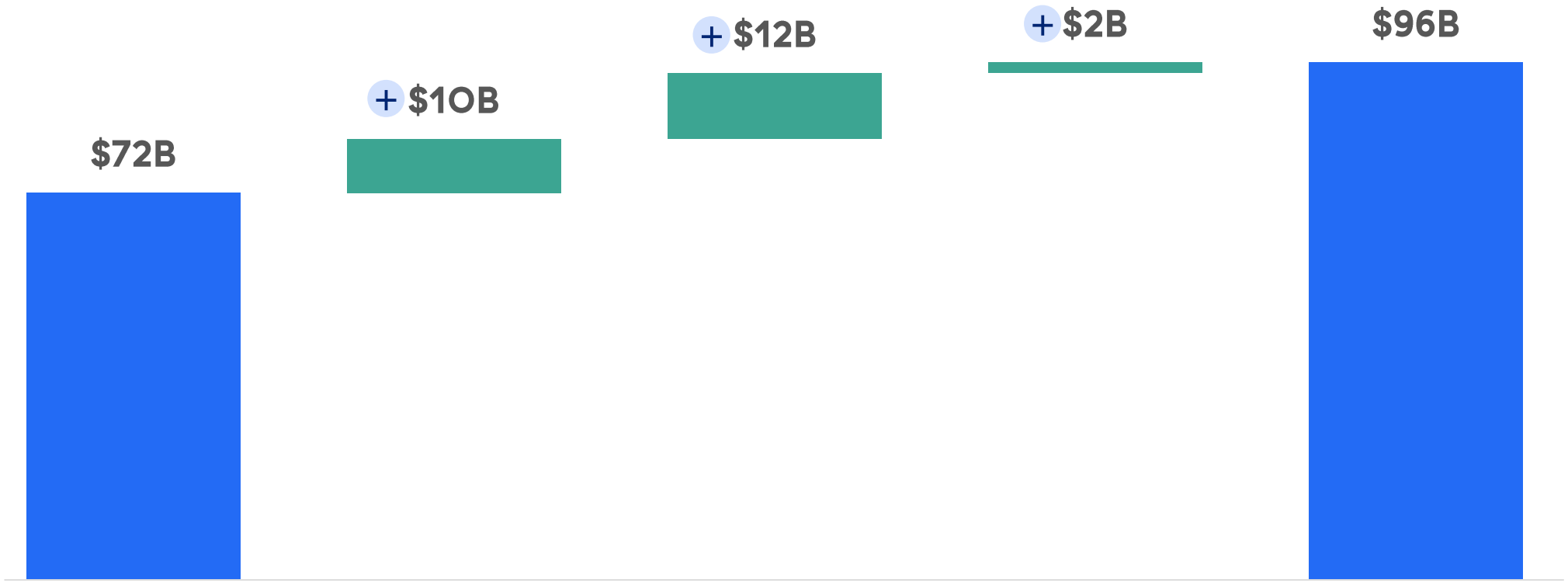
+

Zscaler Data Fabric

New

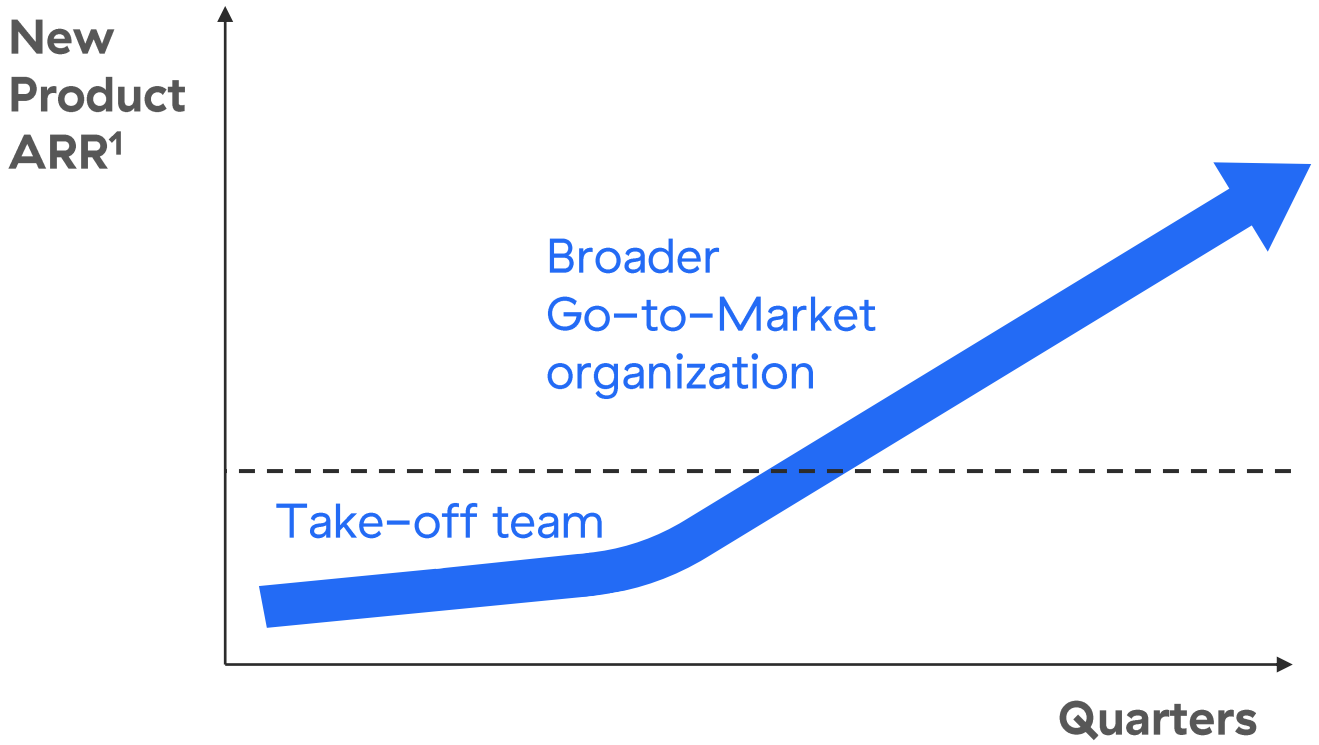
1. Based on Zscaler's analysis of worldwide organization and employee data from ZoomInfo.
2. Zscaler's estimate of potential B2B Users is based on assuming a similar number of users as total worldwide workforce. We consider B2B users to include third-party vendors and customers of our customer.
3. Based on Zscaler's analysis of workload market forecast for 2020 from 650 Research.
4. Based on Zscaler's analysis of IoT market forecast from Gartner.

Innovations are growing serviceable addressable market (SAM)



1) Presented at Zscaler Analyst Day 2021 (January 11, 2021)
2) ARPU is an assumed Average Revenue Per User for companies with 5,000 employees. Per device pricing is an assumed price for IoT/OT devices for companies with 2,000+ employees.
3) Users based on Zscaler's analysis of worldwide organization and employee data from ZoomInfo. Devices based on Zscaler's analysis of IoT market forecast from Gartner.

Expanding take-off teams to new product pillars



Take-off teams:

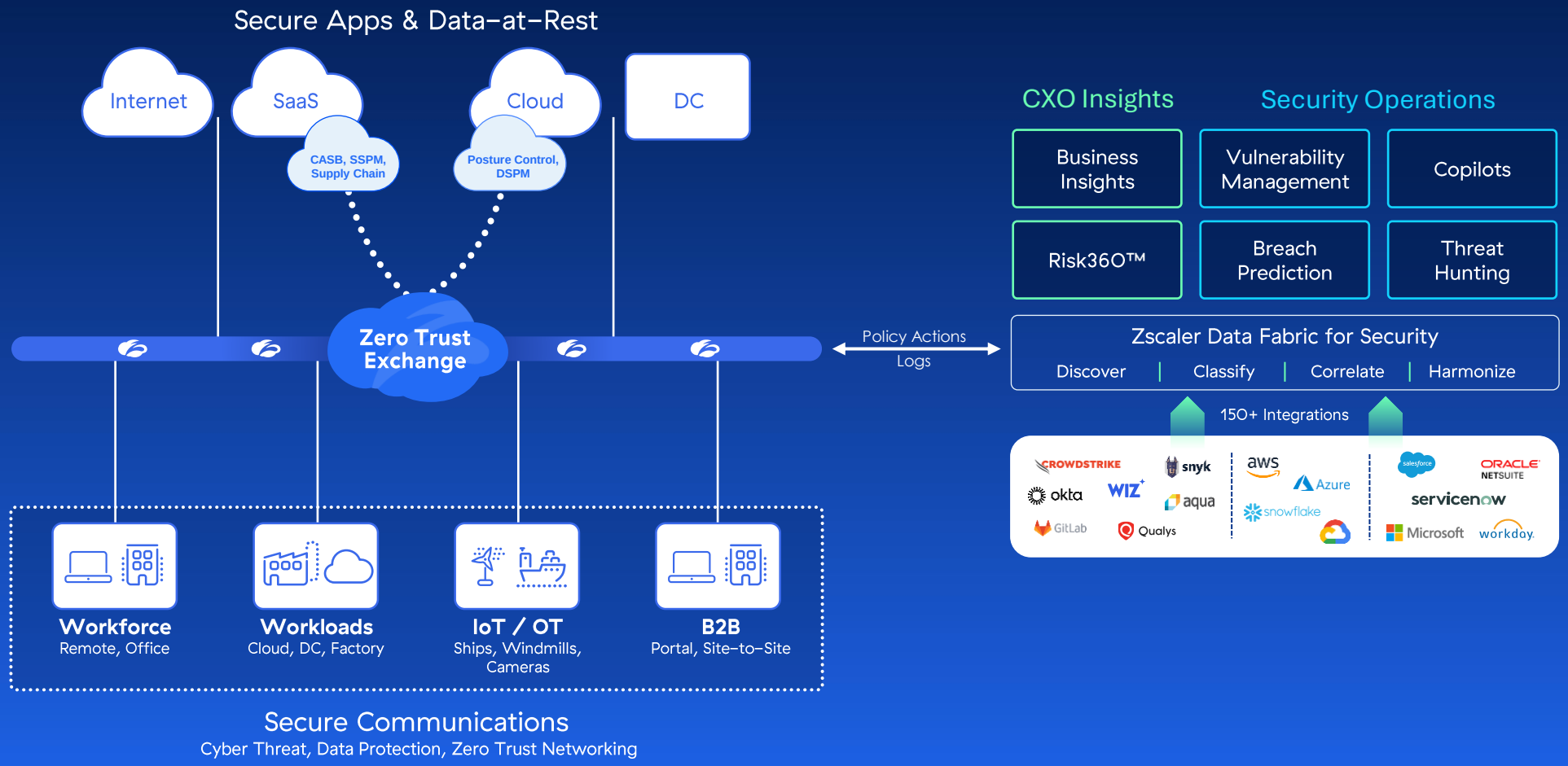
- Data Protection
- Zero Trust Networking
- AI Cloud Solutions

1. For illustrative purposes only

Platform Innovations

Syam Nair
CTO and EVP of R&D

Comprehensive and Integrated Platform



The world's only Data Fabric for Security®

Apps

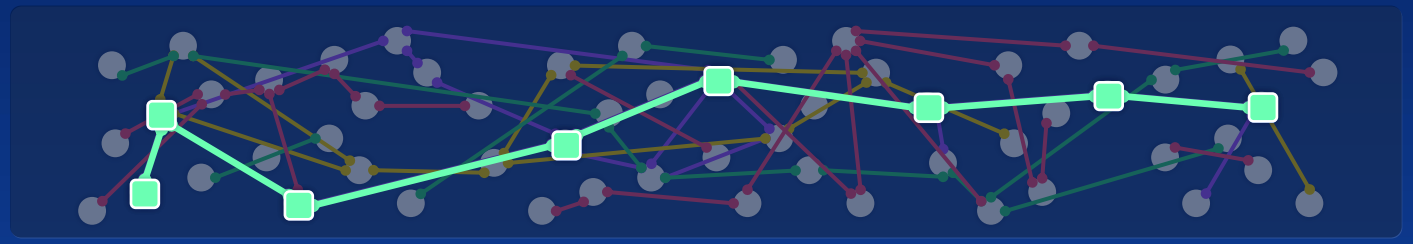
- Risk360
- UVM
- Breach Predictor
- Copilot
- Managed Threat Hunting
- Detection & Response

Smart Detections
Incident Response
Security Graph

Data Fabric & AI Services
Training, modeling, inference

Data Fabric for Security

Discover | Classify | Correlate | Harmonize



Identity, Attributes, Behavior, Device, Content, Destination, Network, Findings

Data Sources (Logs)

zscaler

Communication Logs: **400 Billion Daily Transactions / 500T Signals**

Users | Workloads | B2B | IoT/OT

CROWDSTRIKE | snyk | WIZ | Qualys. | Microsoft Sentinel | aqua | splunk> | okta

Demo: Unified Vulnerability Management

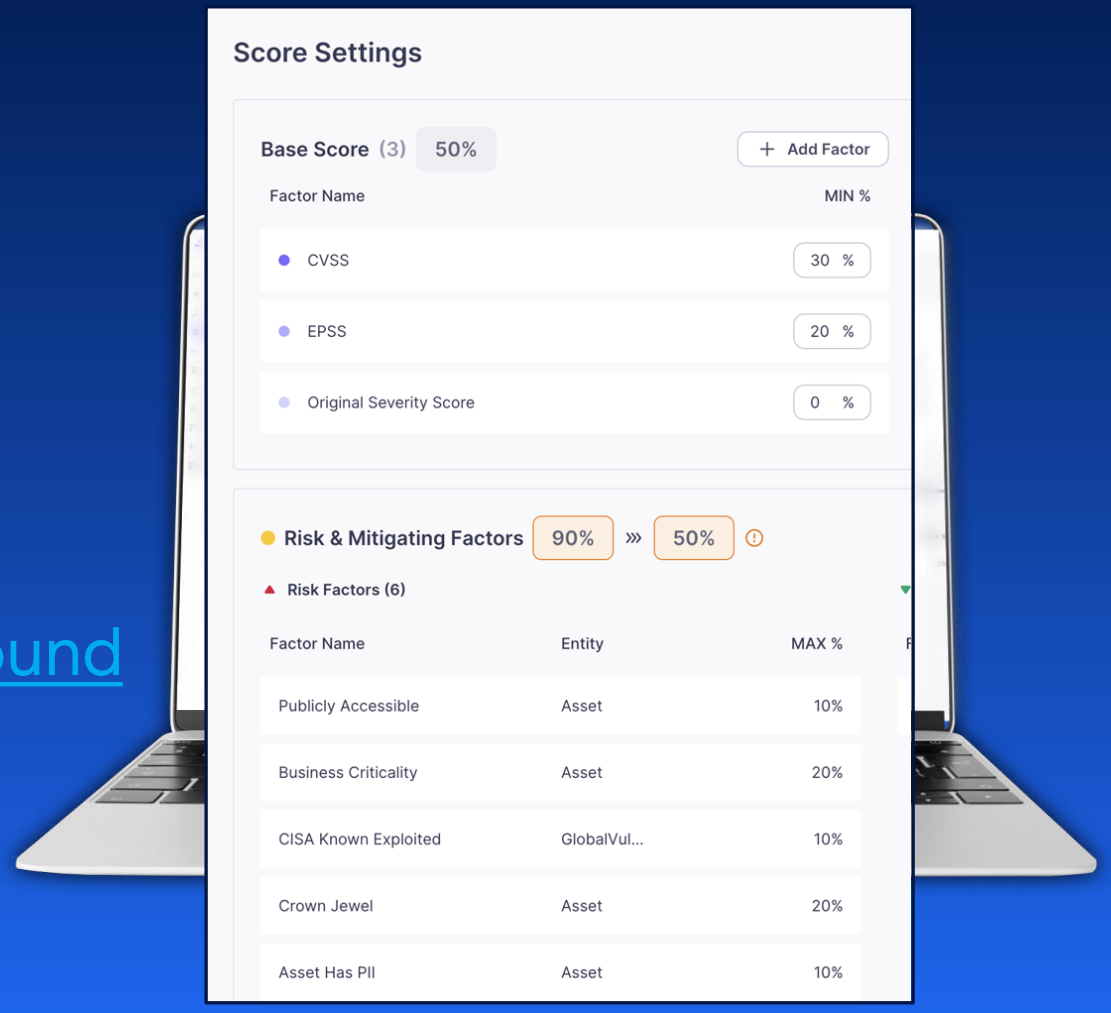
Raanan Raz
VP & GM, Data Analytics

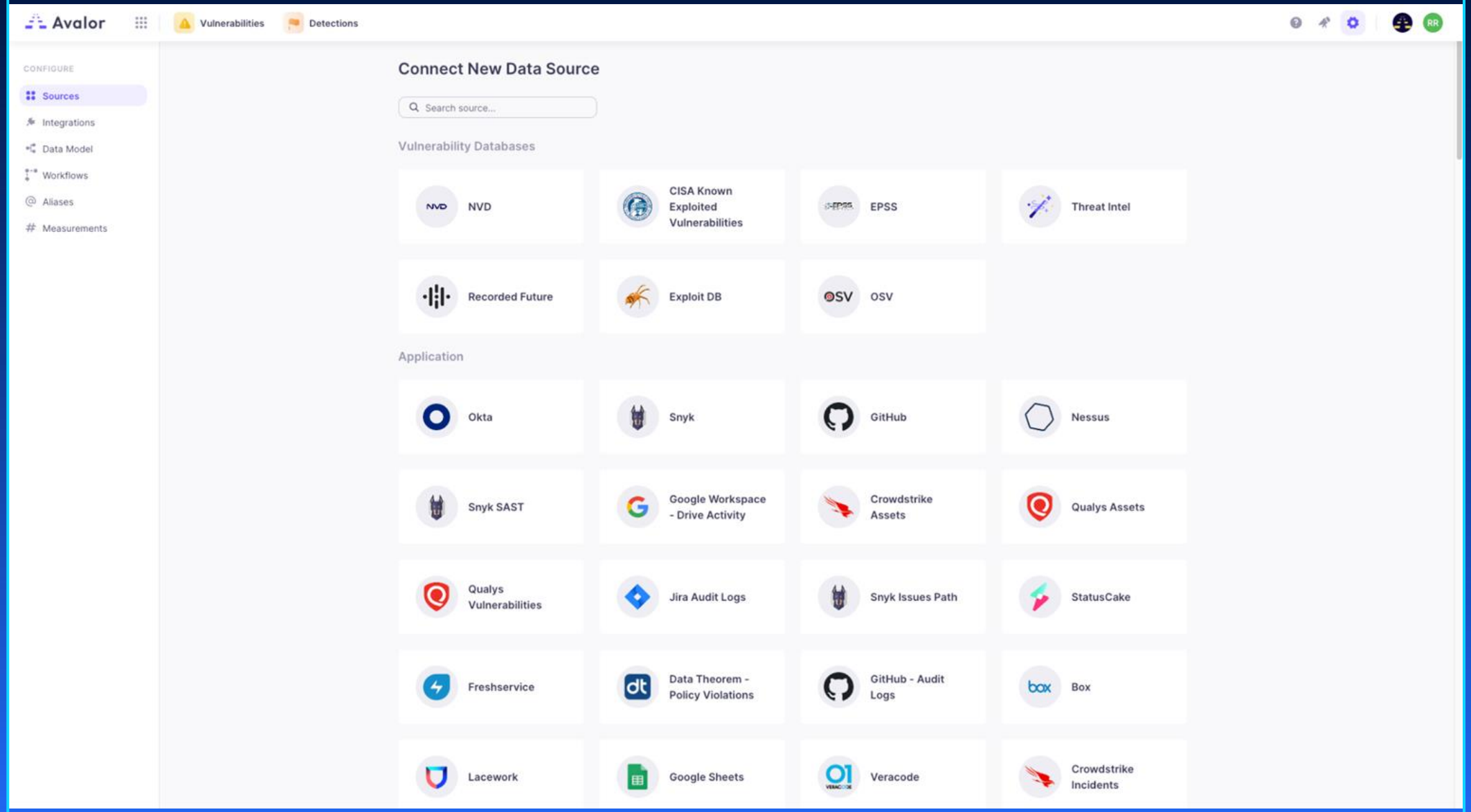
Focus on Using Data, Not Compiling It

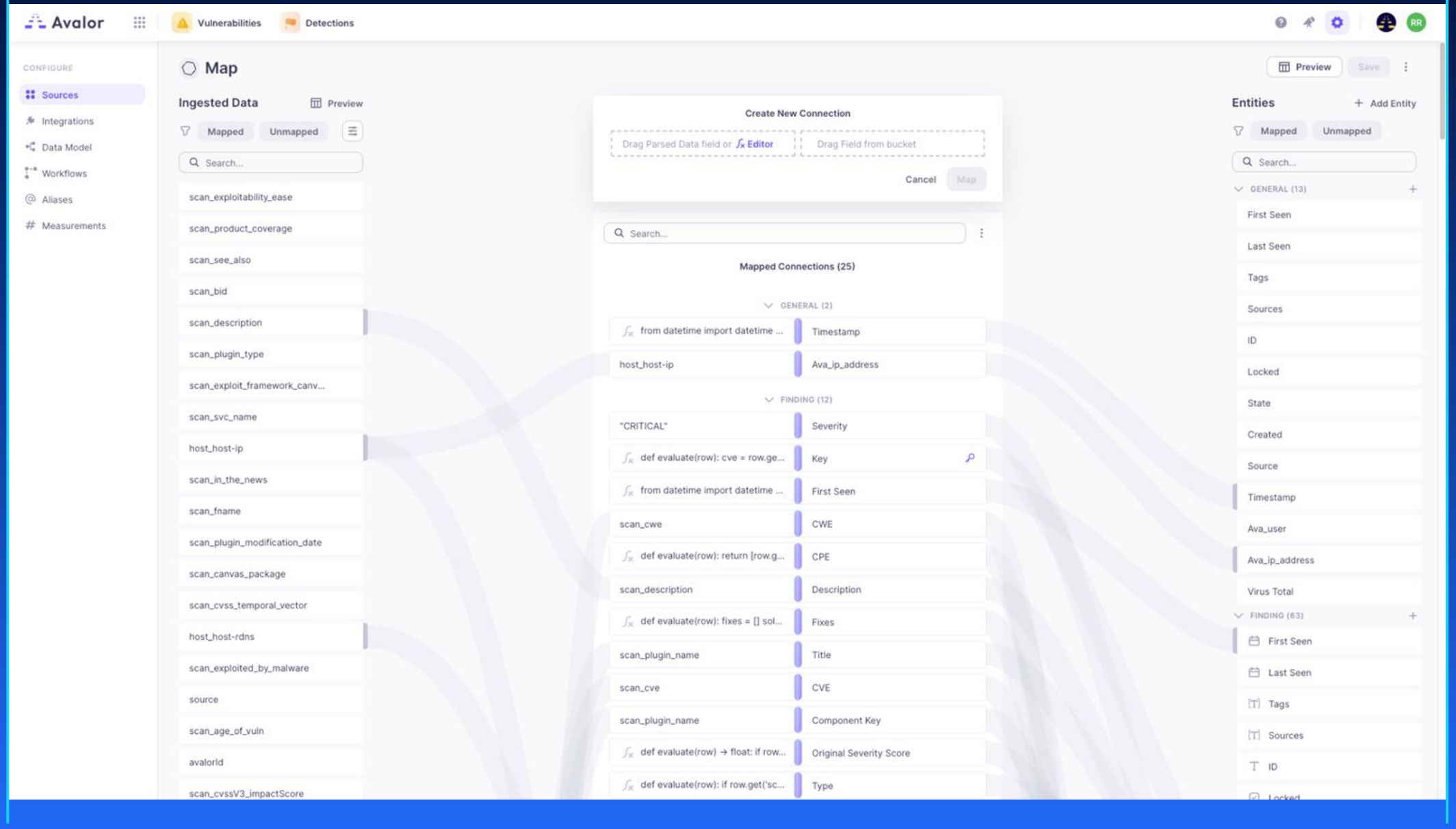
HIGH RISK

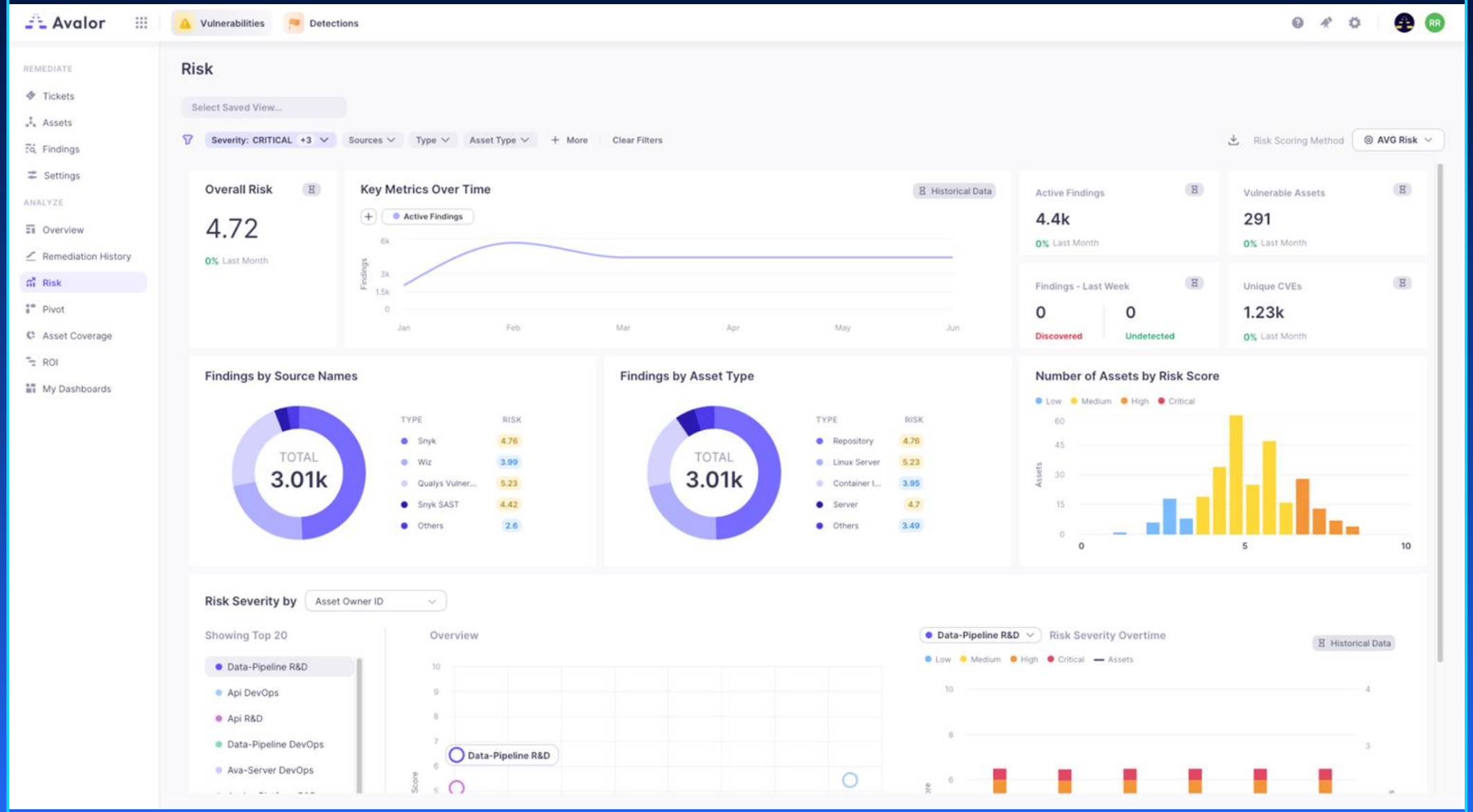
LOW RISK

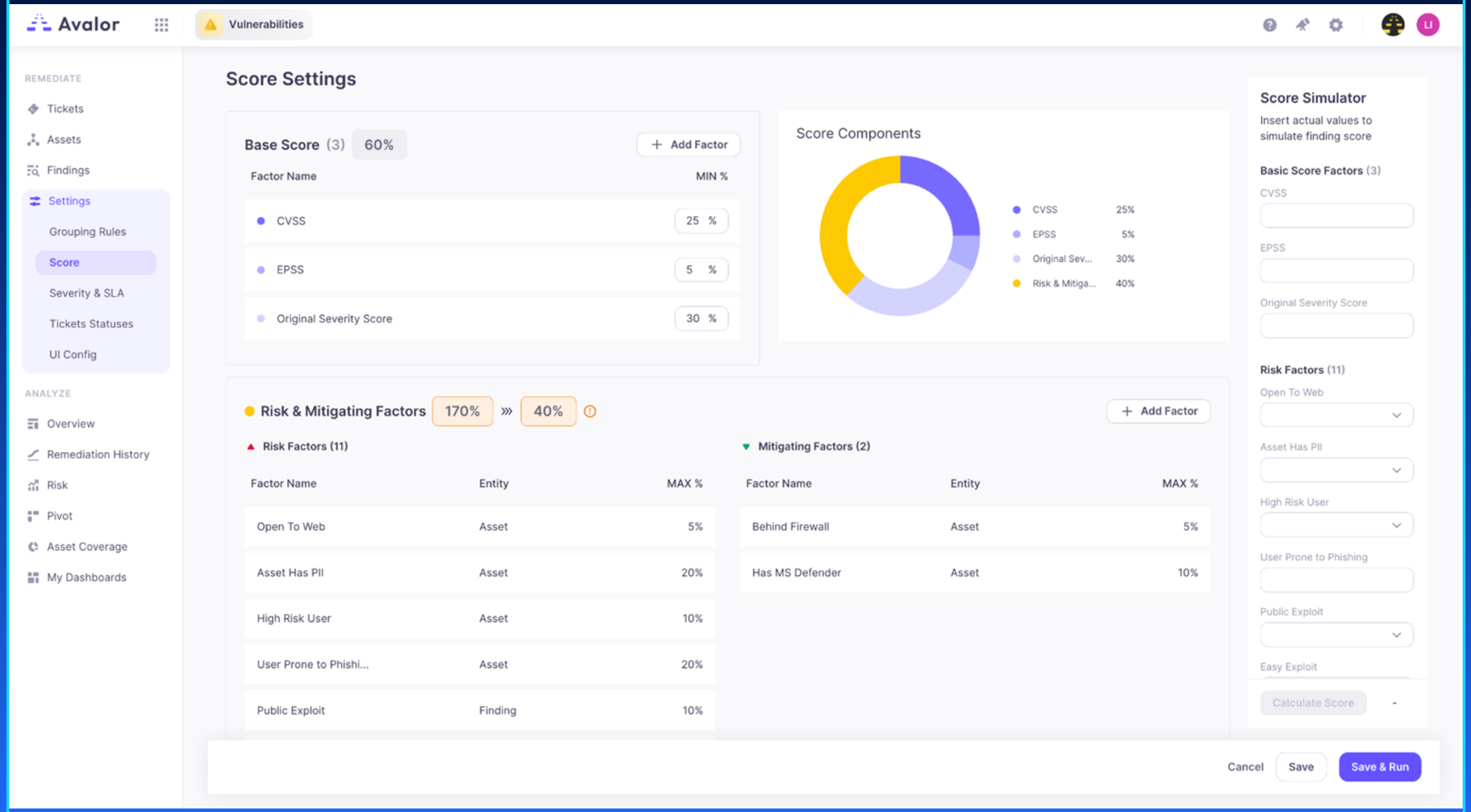
- User clicks on phishing links
- Has access to PII
- Has a known exploit
- Is exposed to the internet
- CVE with CVSS 7.0 found
- Asset has EDR
- In a dev environment

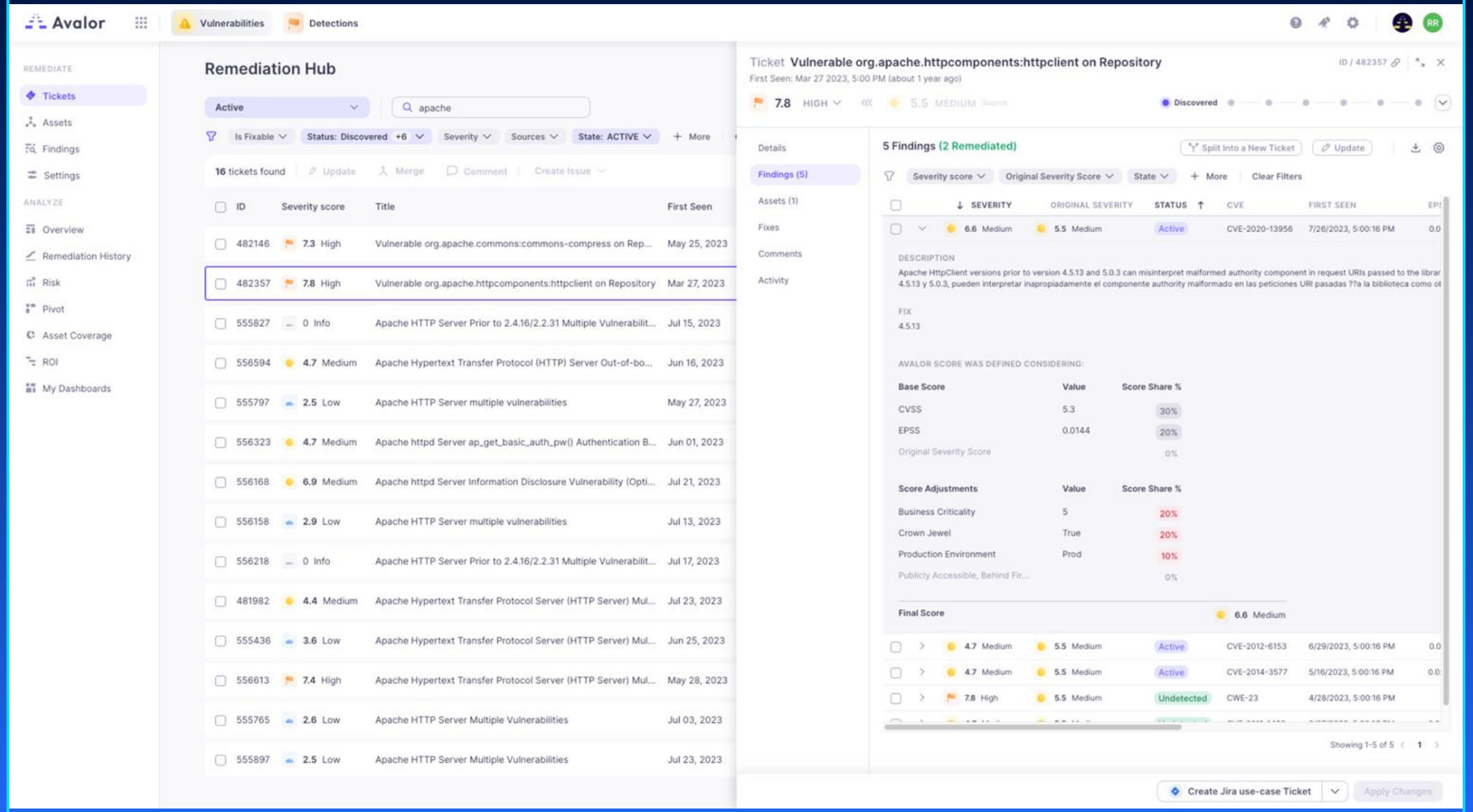


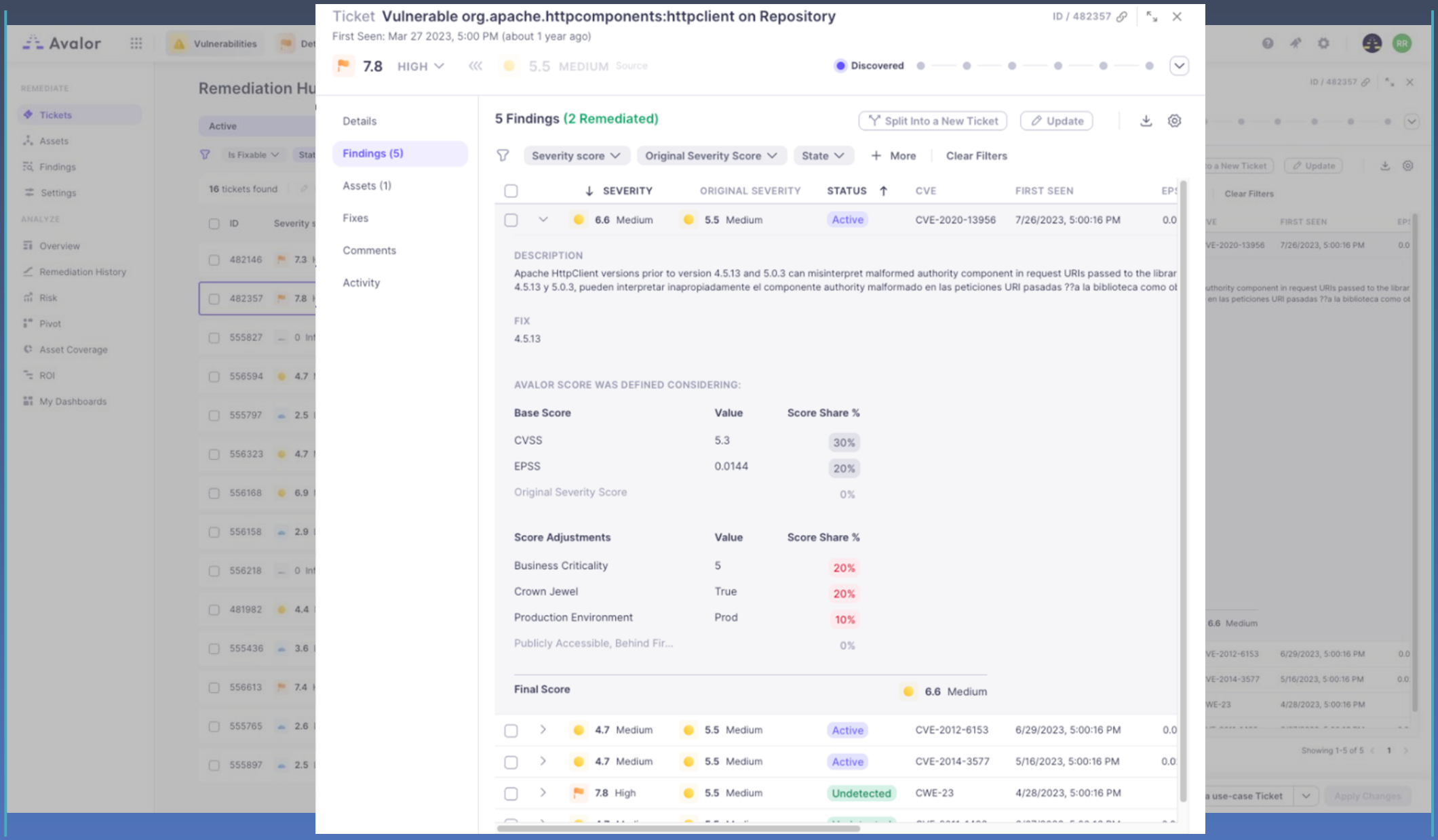

Avalor
Vulnerabilities
Detections
RR
CONFIGURE
Sources
Integrations
Data Model
Workflows
Aliases
Measurements
Connect New Data Source
Search source...
Vulnerability Databases
NVD
CISA Known Exploited Vulnerabilities
EPSS
Threat Intel
Recorded Future
Exploit DB
OSV
Application
Okta
Snyk
GitHub
Nessus
Snyk SAST
Google Workspace - Drive Activity
Crowdstrike Assets
Qualys Assets
Qualys Vulnerabilities
Jira Audit Logs
Snyk Issues Path
StatusCake
Freshservice
Data Theorem - Policy Violations
GitHub - Audit Logs
Box
Lacework
Google Sheets
Veracode
Crowdstrike Incidents

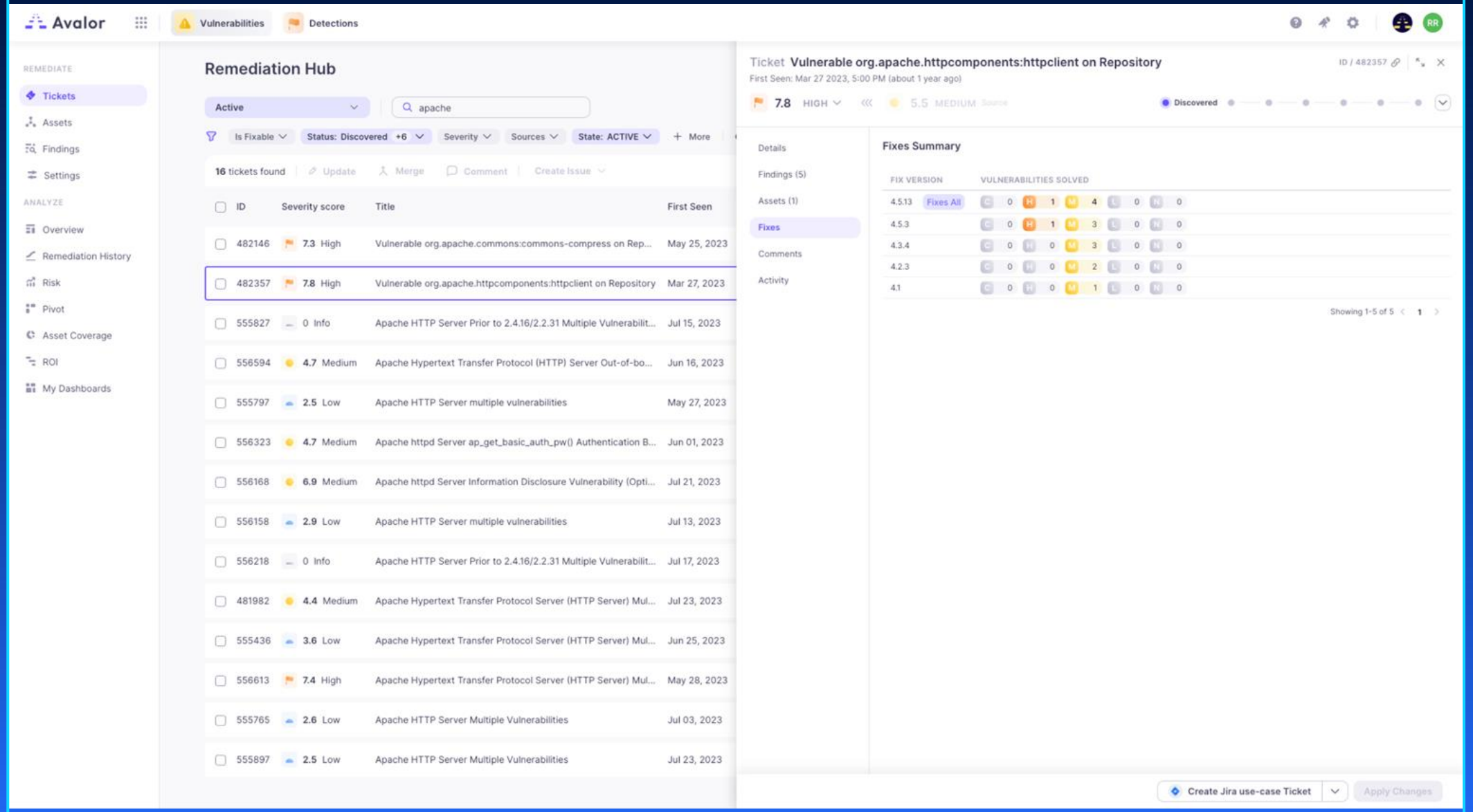

Avalor
Vulnerabilities
Detections
RR
CONFIGURE
Sources
Integrations
Data Model
Workflows
Aliases
Measurements
Map
Preview
Save
Ingested Data
Preview
Mapped
Unmapped
Search...
scan_exploitability_ease
scan_product_coverage
scan_see_also
scan_bid
scan_description
scan_plugin_type
scan_exploit_framework_canv...
scan_svc_name
host_host-ip
scan_in_the_news
scan_fname
scan_plugin_modification_date
scan_canvas_package
scan_cvss_temporal_vector
host_host-rdns
scan_exploited_by_malware
source
scan_age_of_vuln
avalorId
scan_cvssV3_impactScore
Create New Connection
Drag Parsed Data field or Editor
Drag Field from bucket
Cancel
Map
Search...
Mapped Connections (25)
GENERAL (2)
from datetime import datetime ...
Timestamp
host_host-ip
Ava_ip_address
FINDING (12)
"CRITICAL"
Severity
def evaluate(row): cve = row.ge...
Key
from datetime import datetime ...
First Seen
scan_cwe
CWE
def evaluate(row): return [row.g...
CPE
scan_description
Description
def evaluate(row): fixes = [] sol...
Fixes
scan_plugin_name
Title
scan_cve
CVE
scan_plugin_name
Component Key
def evaluate(row) → float: if row...
Original Severity Score
def evaluate(row): if row.get('sc...
Type
Entities
Add Entity
Mapped
Unmapped
Search...
GENERAL (13)
First Seen
Last Seen
Tags
Sources
ID
Locked
State
Created
Source
Timestamp
Ava_user
Ava_ip_address
Virus Total
FINDING (63)
First Seen
Last Seen
Tags
Sources
ID
Locked

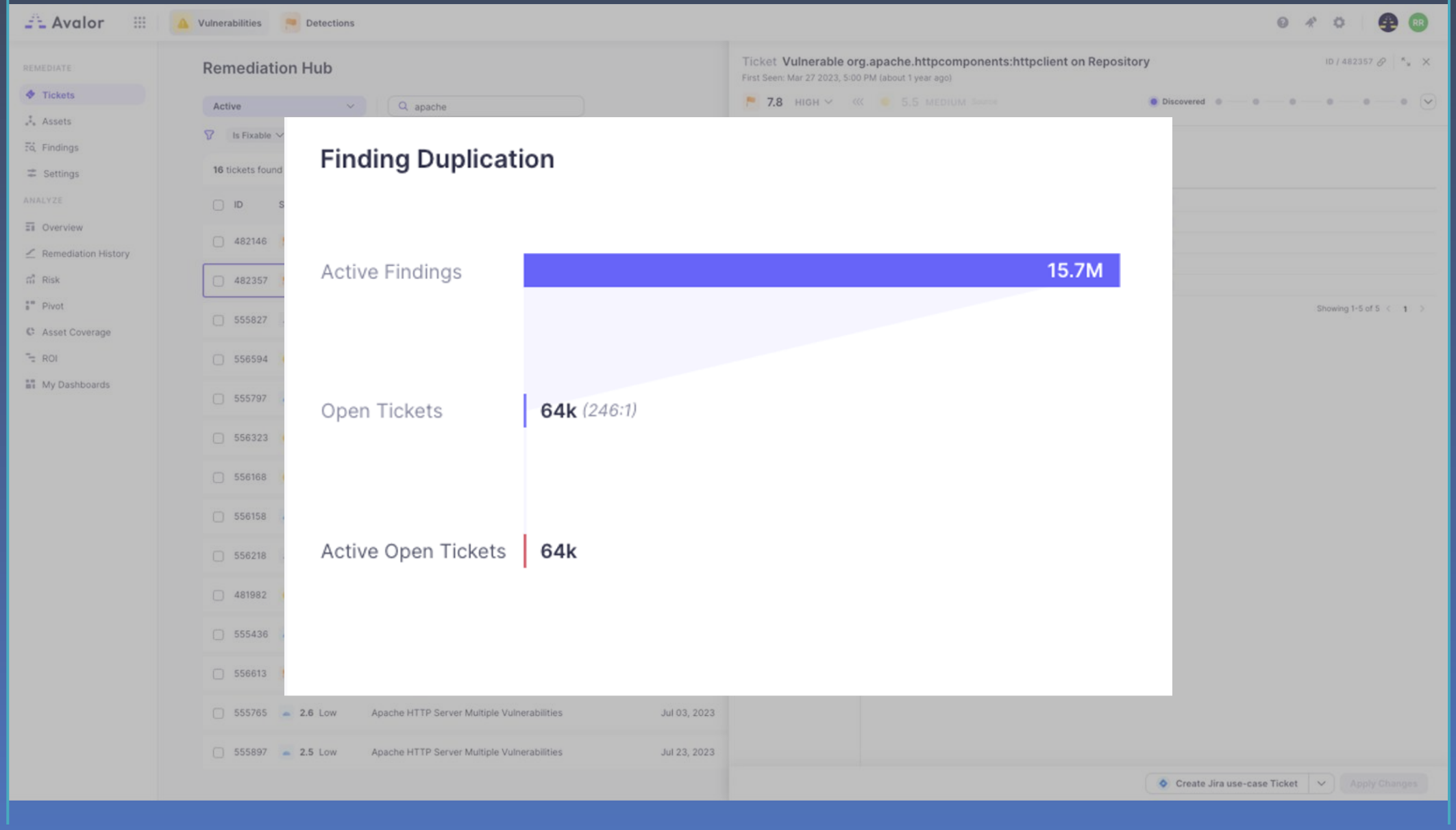

Avalor
Vulnerabilities
Detections
REMEDIATE
Tickets
Assets
Findings
Settings
ANALYZE
Overview
Remediation History
Risk
Pivot
Asset Coverage
ROI
My Dashboards
Risk
Select Saved View...
Severity: CRITICAL +3
Sources
Type
Asset Type
More
Clear Filters
Risk Scoring Method
AVG Risk
Overall Risk
4.72
0% Last Month
Key Metrics Over Time
Historical Data
Active Findings
6k
3k
1.5k
0
Findings
Jan
Feb
Mar
Apr
May
Jun
Active Findings
4.4k
0% Last Month
Vulnerable Assets
291
0% Last Month
Findings - Last Week
0
Discovered
0
Undetected
Unique CVEs
1.23k
0% Last Month
Findings by Source Names
TOTAL
3.01k
TYPE
RISK
Snyk 4.76
Wiz 3.99
Qualys Vulner... 5.23
Snyk SAST 4.42
Others 2.6
Findings by Asset Type
TOTAL
3.01k
TYPE
RISK
Repository 4.76
Linux Server 5.23
Container I... 3.95
Server 4.7
Others 3.49
Number of Assets by Risk Score
Low
Medium
High
Critical
Assets
60
45
30
15
0
0
5
10
Risk Severity by
Asset Owner ID
Showing Top 20
Data-Pipeline R&D
Api DevOps
Api R&D
Data-Pipeline DevOps
Ava-Server DevOps
Overview
Score
Data-Pipeline R&D
Data-Pipeline R&D
Risk Severity Overtime
Historical Data
Low
Medium
High
Critical
Assets

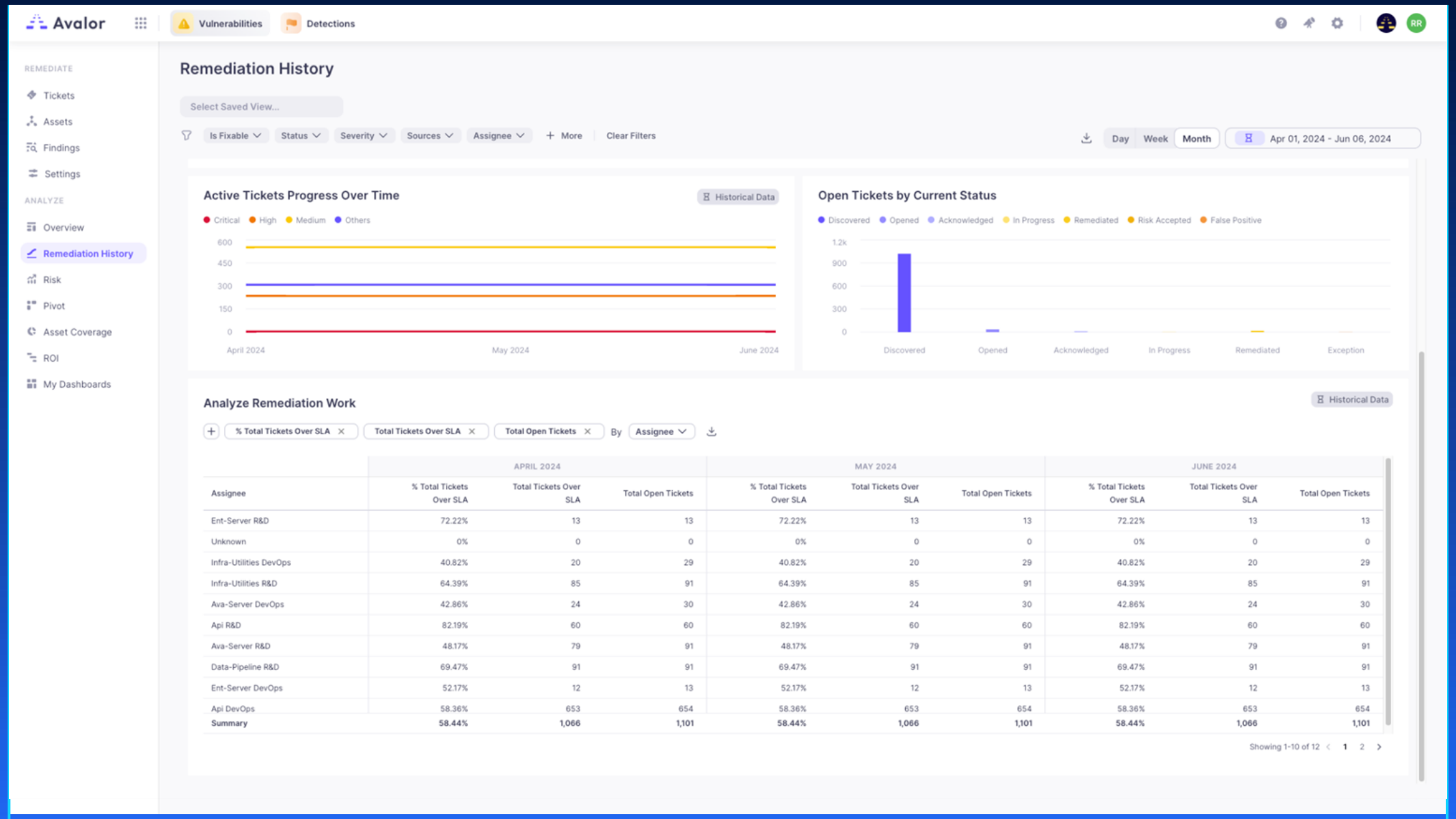

Avalor
Vulnerabilities
LI
REMEDIATE
Tickets
Assets
Findings
Settings
Grouping Rules
Score
Severity & SLA
Tickets Statuses
UI Config
ANALYZE
Overview
Remediation History
Risk
Pivot
Asset Coverage
My Dashboards
Score Settings
Base Score (3) 60%
Add Factor
Factor Name
MIN %
CVSS 25 %
EPSS 5 %
Original Severity Score 30 %
Score Components
CVSS 25%
EPSS 5%
Original Sev... 30%
Risk & Mitiga... 40%
Risk & Mitigating Factors 170% 40%
Add Factor
Risk Factors (11)
Mitigating Factors (2)
Factor Name
Entity
MAX %
Open To Web Asset 5%
Asset Has PII Asset 20%
High Risk User Asset 10%
User Prone to Phishi... Asset 20%
Public Exploit Finding 10%
Behind Firewall Asset 5%
Has MS Defender Asset 10%
Score Simulator
Insert actual values to simulate finding score
Basic Score Factors (3)
CVSS
EPSS
Original Severity Score
Risk Factors (11)
Open To Web
Asset Has PII
High Risk User
User Prone to Phishing
Public Exploit
Easy Exploit
Calculate Score
Cancel
Save
Save & Run

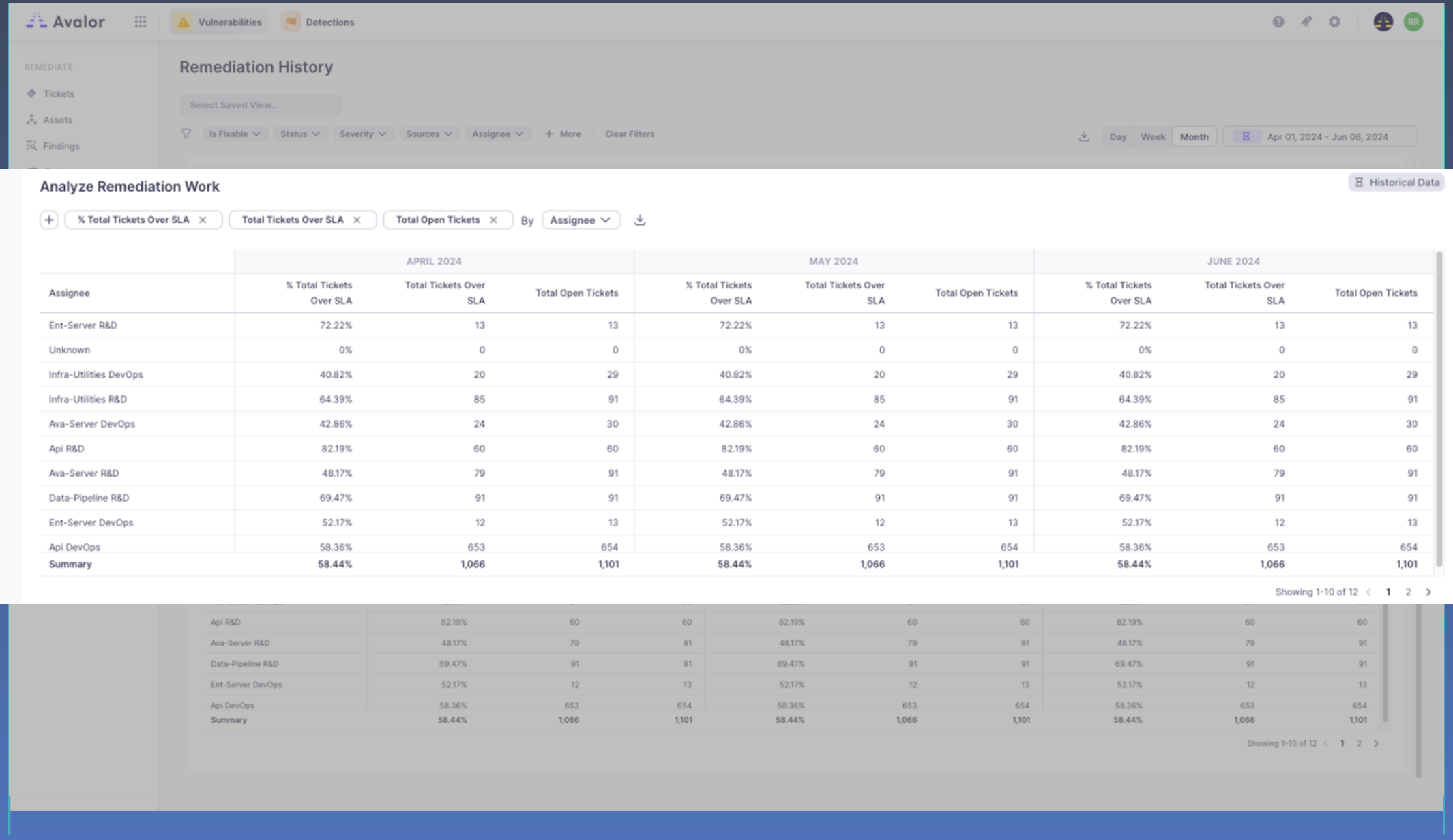

Avalor
Vulnerabilities
Detections
REMEDIATE
Tickets
Assets
Findings
Settings
ANALYZE
Overview
Remediation History
Risk
Pivot
Asset Coverage
ROI
My Dashboards
Remediation Hub
Active
apache
Is Fixable
Status: Discovered +6
Severity
Sources
State: ACTIVE
More
16 tickets found
Update
Merge
Comment
Create Issue
ID
Severity score
Title
First Seen
482146 7.3 High Vulnerable org.apache.commons:commons-compress on Rep... May 25, 2023
482357 7.8 High Vulnerable org.apache.httpcomponents:httpclient on Repository Mar 27, 2023
555827 0 Info Apache HTTP Server Prior to 2.4.16/2.2.31 Multiple Vulnerabilit... Jul 15, 2023
556594 4.7 Medium Apache Hypertext Transfer Protocol (HTTP) Server Out-of-bo... Jun 16, 2023
555797 2.5 Low Apache HTTP Server multiple vulnerabilities May 27, 2023
556323 4.7 Medium Apache httpd Server ap_get_basic_auth_pw() Authentication B... Jun 01, 2023
556168 6.9 Medium Apache httpd Server Information Disclosure Vulnerability (Opti... Jul 21, 2023
556158 2.9 Low Apache HTTP Server multiple vulnerabilities Jul 13, 2023
556218 0 Info Apache HTTP Server Prior to 2.4.16/2.2.31 Multiple Vulnerabilit... Jul 17, 2023
481982 4.4 Medium Apache Hypertext Transfer Protocol Server (HTTP Server) Mul... Jul 23, 2023
555436 3.6 Low Apache Hypertext Transfer Protocol Server (HTTP Server) Mul... Jun 25, 2023
556613 7.4 High Apache Hypertext Transfer Protocol Server (HTTP Server) Mul... May 28, 2023
555765 2.6 Low Apache HTTP Server Multiple Vulnerabilities Jul 03, 2023
555897 2.5 Low Apache HTTP Server Multiple Vulnerabilities Jul 23, 2023
Ticket Vulnerable org.apache.httpcomponents:httpclient on Repository
ID / 482357
First Seen: Mar 27 2023, 5:00 PM (about 1 year ago)
7.8 HIGH
5.5 MEDIUM
Discovered
Details
Findings (5)
Assets (1)
Fixes
Comments
Activity
5 Findings (2 Remediated)
Split Into a New Ticket
Update
Severity score
Original Severity Score
State
More
Clear Filters
SEVERITY
ORIGINAL SEVERITY
STATUS
CVE
FIRST SEEN
6.6 Medium
5.5 Medium
Active
CVE-2020-13956
7/26/2023, 5:00:16 PM
DESCRIPTION
Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the librar
4.5.13 y 5.0.3, pueden interpretar inapropiadamente el componente authority malformado en las peticiones URI pasadas ??a la bibliioteca como ot
FIX
4.5.13
AVALOR SCORE WAS DEFINED CONSIDERING:
Base Score
Value
Score Share %
CVSS
5.3
30%
EPSS
0.0144
20%
Original Severity Score
0%
Score Adjustments
Value
Score Share %
Business Criticality
5
20%
Crown Jewel
True
20%
Production Environment
Prod
10%
Publicly Accessible, Behind Fir...
0%
Final Score
6.6 Medium
4.7 Medium
5.5 Medium
Active
CVE-2012-6153
6/29/2023, 5:00:16 PM
4.7 Medium
5.5 Medium
Active
CVE-2014-3577
5/16/2023, 5:00:16 PM
7.8 High
5.5 Medium
Undetected
CWE-23
4/28/2023, 5:00:16 PM
Showing 1-5 of 5
1
Create Jira use-case Ticket
Apply Changes


Avalor
Vulnerabilities
REMEDIATE
Tickets
Assets
Findings
Settings
ANALYZE
Overview
Remediation History
Risk
Pivot
Asset Coverage
ROI
My Dashboards
Remediation Hu
Active
16 tickets found
Ticket Vulnerable org.apache.httpcomponents:httpclient on Repository
First Seen: Mar 27 2023, 5:00 PM (about 1 year ago)
ID / 482357
7.8 HIGH
5.5 MEDIUM Source
Discovered
Details
Findings (5)
Assets (1)
Fixes
Comments
Activity
5 Findings (2 Remediated)
Split Into a New Ticket
Update
Severity score
Original Severity Score
State
More
Clear Filters
SEVERITY
ORIGINAL SEVERITY
STATUS
CVE
FIRST SEEN
6.6 Medium
5.5 Medium
Active
CVE-2020-13956
7/26/2023, 5:00:16 PM
DESCRIPTION
Apache HttpClient versions prior to version 4.5.13 and 5.0.3 can misinterpret malformed authority component in request URIs passed to the librar
4.5.13 y 5.0.3, pueden interpretar inapropiadamente el componente authority malformado en las peticiones URI pasadas ??a la biblioteca como ot
FIX
4.5.13
AVALOR SCORE WAS DEFINED CONSIDERING:
Base Score
Value
Score Share %
CVSS
5.3
30%
EPSS
0.0144
20%
Original Severity Score
0%
Score Adjustments
Value
Score Share %
Business Criticality
5
20%
Crown Jewel
True
20%
Production Environment
Prod
10%
Publicly Accessible, Behind Fir...
0%
Final Score
6.6 Medium
4.7 Medium
5.5 Medium
Active
CVE-2012-6153
6/29/2023, 5:00:16 PM
4.7 Medium
5.5 Medium
Active
CVE-2014-3577
5/16/2023, 5:00:16 PM
7.8 High
5.5 Medium
Undetected
CWE-23
4/28/2023, 5:00:16 PM


Avalor
Vulnerabilities
Detections
REMEDIATE
Tickets
Assets
Findings
Settings
ANALYZE
Overview
Remediation History
Risk
Pivot
Asset Coverage
ROI
My Dashboards
Remediation Hub
Active
apache
Is Fixable
Status: Discovered +6
Severity
Sources
State: ACTIVE
More
16 tickets found
Update
Merge
Comment
Create Issue
ID
Severity score
Title
First Seen
482146 7.3 High Vulnerable org.apache.commons:commons-compress on Rep... May 25, 2023
482357 7.8 High Vulnerable org.apache.httpcomponents:httpclient on Repository Mar 27, 2023
555827 0 Info Apache HTTP Server Prior to 2.4.16/2.2.31 Multiple Vulnerabilit... Jul 15, 2023
556594 4.7 Medium Apache Hypertext Transfer Protocol (HTTP) Server Out-of-bo... Jun 16, 2023
555797 2.5 Low Apache HTTP Server multiple vulnerabilities May 27, 2023
556323 4.7 Medium Apache httpd Server ap_get_basic_auth_pw() Authentication B... Jun 01, 2023
556168 6.9 Medium Apache httpd Server Information Disclosure Vulnerability (Opti... Jul 21, 2023
556158 2.9 Low Apache HTTP Server multiple vulnerabilities Jul 13, 2023
556218 0 Info Apache HTTP Server Prior to 2.4.16/2.2.31 Multiple Vulnerabilit... Jul 17, 2023
481982 4.4 Medium Apache Hypertext Transfer Protocol Server (HTTP Server) Mul... Jul 23, 2023
555436 3.6 Low Apache Hypertext Transfer Protocol Server (HTTP Server) Mul... Jun 25, 2023
556613 7.4 High Apache Hypertext Transfer Protocol Server (HTTP Server) Mul... May 28, 2023
555765 2.6 Low Apache HTTP Server Multiple Vulnerabilities Jul 03, 2023
555897 2.5 Low Apache HTTP Server Multiple Vulnerabilities Jul 23, 2023
Ticket Vulnerable org.apache.httpcomponents:httpclient on Repository
ID / 482357
First Seen: Mar 27 2023, 5:00 PM (about 1 year ago)
7.8 HIGH
5.5 MEDIUM
Discovered
Details
Findings (5)
Assets (1)
Fixes
Comments
Activity
Fixes Summary
FIX VERSION
VULNERABILITIES SOLVED
4.5.13 Fixes All C 0 H 1 M 4 L 0 N 0
4.5.3 C 0 H 1 M 3 L 0 N 0
4.3.4 C 0 H 0 M 3 L 0 N 0
4.2.3 C 0 H 0 M 2 L 0 N 0
4.1 C 0 H 0 M 1 L 0 N 0
Showing 1-5 of 5
1
Create Jira use-case Ticket
Apply Changes


Avalor
Vulnerabilities
Detections
REMEDIATE
Tickets
Assets
Findings
Settings
ANALYZE
Overview
Remediation History
Risk
Pivot
Asset Coverage
ROI
My Dashboards
Remediation Hub
Active
apache
Is Fixable
16 tickets found
ID
482146
482357
555827
556594
555797
556323
556168
556158
556218
481982
555436
556613
555765 2.6 Low Apache HTTP Server Multiple Vulnerabilities Jul 03, 2023
555897 2.5 Low Apache HTTP Server Multiple Vulnerabilities Jul 23, 2023
Ticket Vulnerable org.apache.httpcomponents:httpclient on Repository
First Seen: Mar 27 2023, 5:00 PM (about 1 year ago)
ID / 482357
7.8 HIGH
5.5 MEDIUM
Discovered
Showing 1-5 of 5
1
Create Jira use-case Ticket
Apply Changes
Finding Duplication
Active Findings
15.7M
Open Tickets
64k (246:1)
Active Open Tickets
64k


Avalor
Vulnerabilities
Detections
RR
REMEDIATE
Tickets
Assets
Findings
Settings
ANALYZE
Overview
Remediation History
Risk
Pivot
Asset Coverage
ROI
My Dashboards
Remediation History
Select Saved View...
Is Fixable
Status
Severity
Sources
Assignee
More
Clear Filters
Day
Week
Month
Apr 01, 2024 - Jun 06, 2024
Active Tickets Progress Over Time
Historical Data
Critical
High
Medium
Others
600
450
300
150
0
April 2024
May 2024
June 2024
Open Tickets by Current Status
Discovered
Opened
Acknowledged
In Progress
Remediated
Risk Accepted
False Positive
1.2k
900
600
300
0
Discovered
Opened
Acknowledged
In Progress
Remediated
Exception
Analyze Remediation Work
Historical Data
% Total Tickets Over SLA
Total Tickets Over SLA
Total Open Tickets
By
Assignee
APRIL 2024
MAY 2024
JUNE 2024
Assignee
% Total Tickets Over SLA
Total Tickets Over SLA
Total Open Tickets
Ent-Server R&D 72.22% 13 13 72.22% 13 13 72.22% 13 13
Unknown 0% 0 0 0% 0 0 0% 0 0
Infra-Utilities DevOps 40.82% 20 29 40.82% 20 29 40.82% 20 29
Infra-Utilities R&D 64.39% 85 91 64.39% 85 91 64.39% 85 91
Ava-Server DevOps 42.86% 24 30 42.86% 24 30 42.86% 24 30
Api R&D 82.19% 60 60 82.19% 60 60 82.19% 60 60
Ava-Server R&D 48.17% 79 91 48.17% 79 91 48.17% 79 91
Data-Pipeline R&D 69.47% 91 91 69.47% 91 91 69.47% 91 91
Ent-Server DevOps 52.17% 12 13 52.17% 12 13 52.17% 12 13
Api DevOps 58.36% 653 654 58.36% 653 654 58.36% 653 654
Summary 58.44% 1,066 1,101 58.44% 1,066 1,101 58.44% 1,066 1,101
Showing 1-10 of 12
1
2


Avalor
Vulnerabilities
Detections
REMEDIATE
Tickets
Assets
Findings
Remediation History
Select Saved View...
Is Fixable
Status
Severity
Sources
Assignee
More
Clear Filters
Day
Week
Month
Apr 01, 2024 - Jun 06, 2024
Analyze Remediation Work
Historical Data
% Total Tickets Over SLA
Total Tickets Over SLA
Total Open Tickets
By
Assignee
APRIL 2024
MAY 2024
JUNE 2024
Assignee
% Total Tickets Over SLA
Total Tickets Over SLA
Total Open Tickets
Ent-Server R&D 72.22% 13 13 72.22% 13 13 72.22% 13 13
Unknown 0% 0 0 0% 0 0 0% 0 0
Infra-Utilities DevOps 40.82% 20 29 40.82% 20 29 40.82% 20 29
Infra-Utilities R&D 64.39% 85 91 64.39% 85 91 64.39% 85 91
Ava-Server DevOps 42.86% 24 30 42.86% 24 30 42.86% 24 30
Api R&D 82.19% 60 60 82.19% 60 60 82.19% 60 60
Ava-Server R&D 48.17% 79 91 48.17% 79 91 48.17% 79 91
Data-Pipeline R&D 69.47% 91 91 69.47% 91 91 69.47% 91 91
Ent-Server DevOps 52.17% 12 13 52.17% 12 13 52.17% 12 13
Api DevOps 58.36% 653 654 58.36% 653 654 58.36% 653 654
Summary 58.44% 1,066 1,101 58.44% 1,066 1,101 58.44% 1,066 1,101
Showing 1-10 of 12
1
2

Demo: Risk360

Deepen Desai
Chief Security Officer

Dashboard

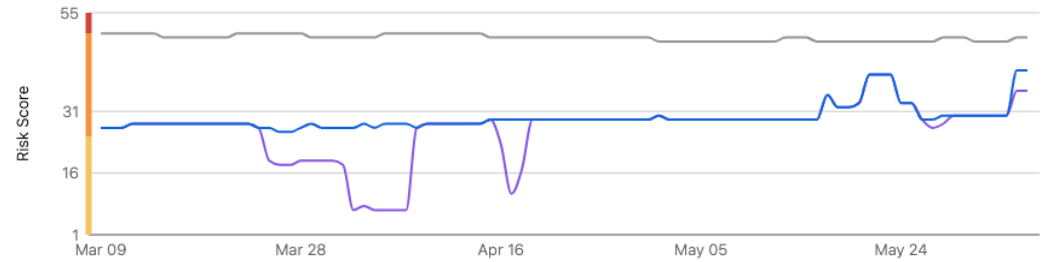
Organization Risk Score

External Attack Surface 70.00
Compromise 20.21
Lateral Propagation 21.74
Data Loss 31.46

Low Medium High Critical

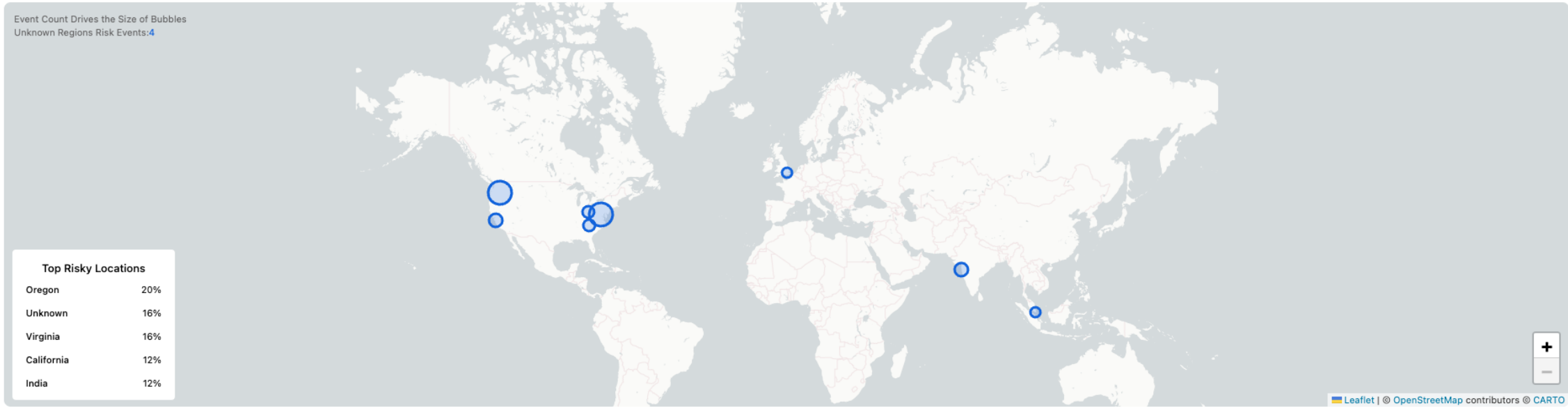
Risk Score Trend

Key Events



Customized Risk Score Risk Score Industry Peer Average Score

Risk Events by Location



Contributing Factors by Entity

View All

Workforce
3rd Parties
Applications
Assets

Help

Dashboard

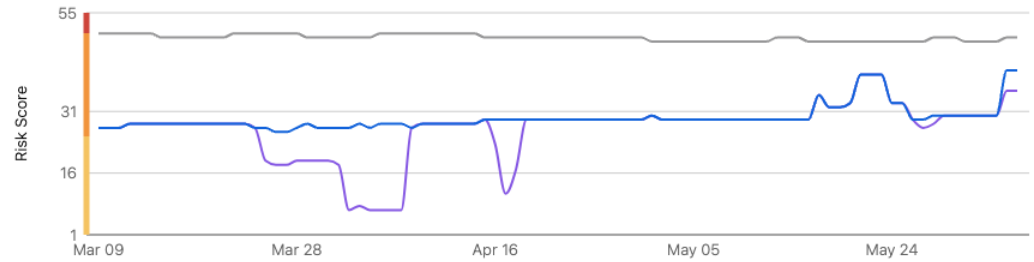
Organization Risk Score

External Attack Surface 70.00
Compromise 20.21
Lateral Propagation 21.74
Data Loss 31.46

Low Medium High Critical

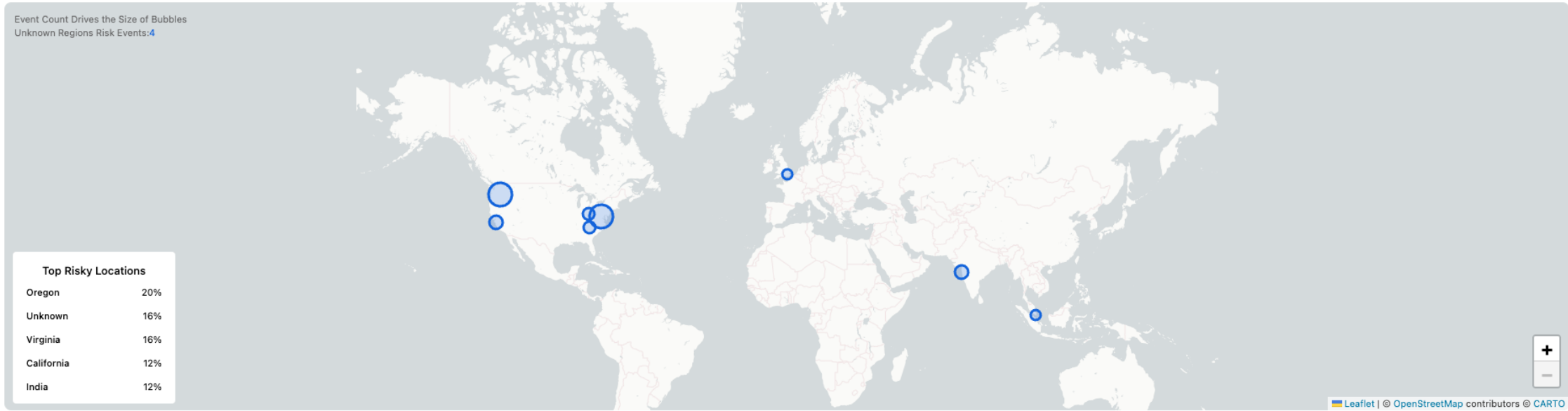
Risk Score Trend

Key Events



Customized Risk Score Risk Score Industry Peer Average Score

Risk Events by Location

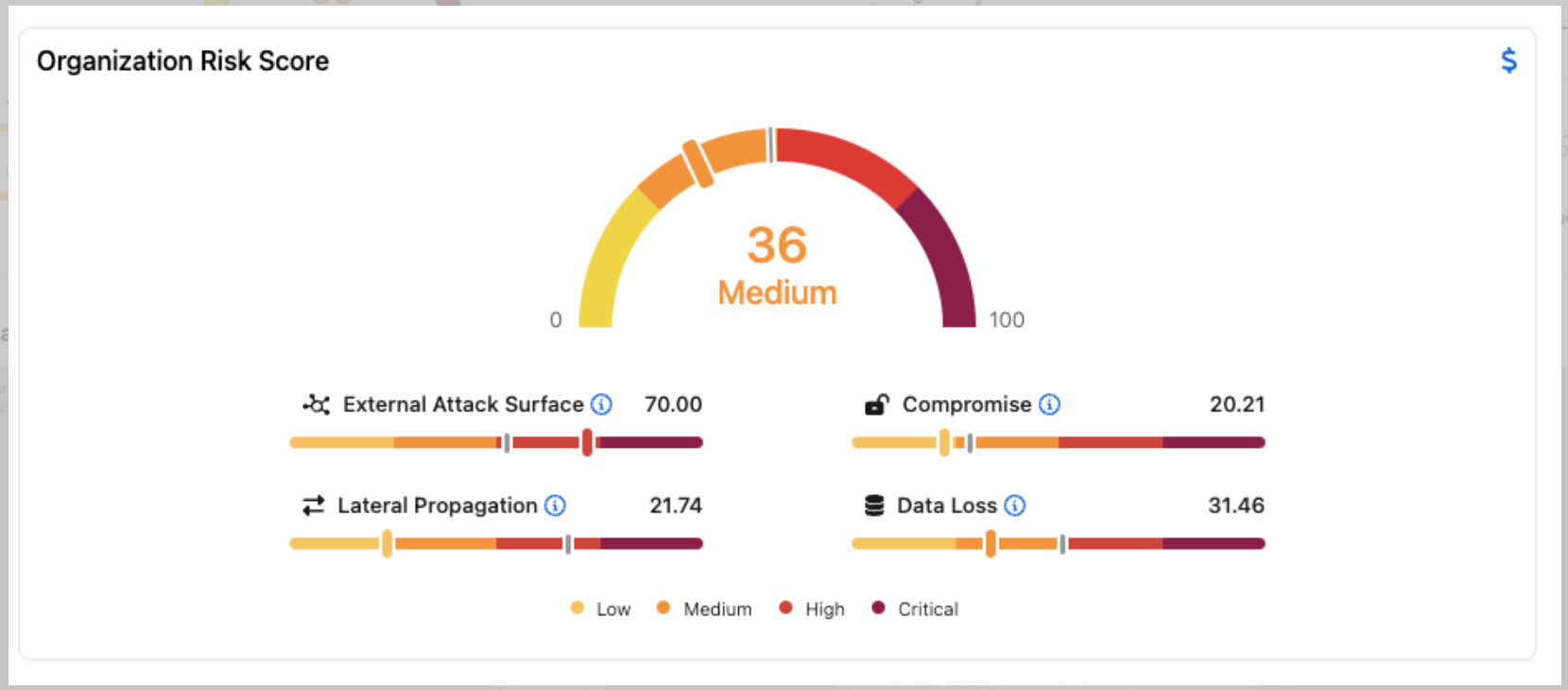


Contributing Factors by Entity

View All

Workforce
3rd Parties
Applications
Assets

Help


Organization Risk Score
36
Medium
0
100
External Attack Surface
70.00
Compromise
20.21
Lateral Propagation
21.74
Data Loss
31.46
Low
Medium
High
Critical

Dashboard

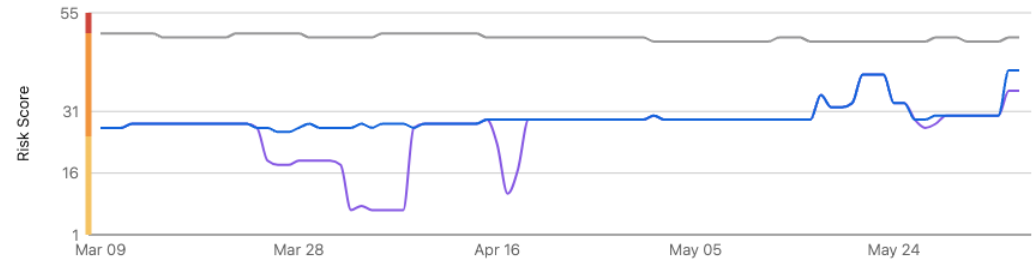
Organization Risk Score

External Attack Surface 70.00
Compromise 20.21
Lateral Propagation 21.74
Data Loss 31.46

Low Medium High Critical

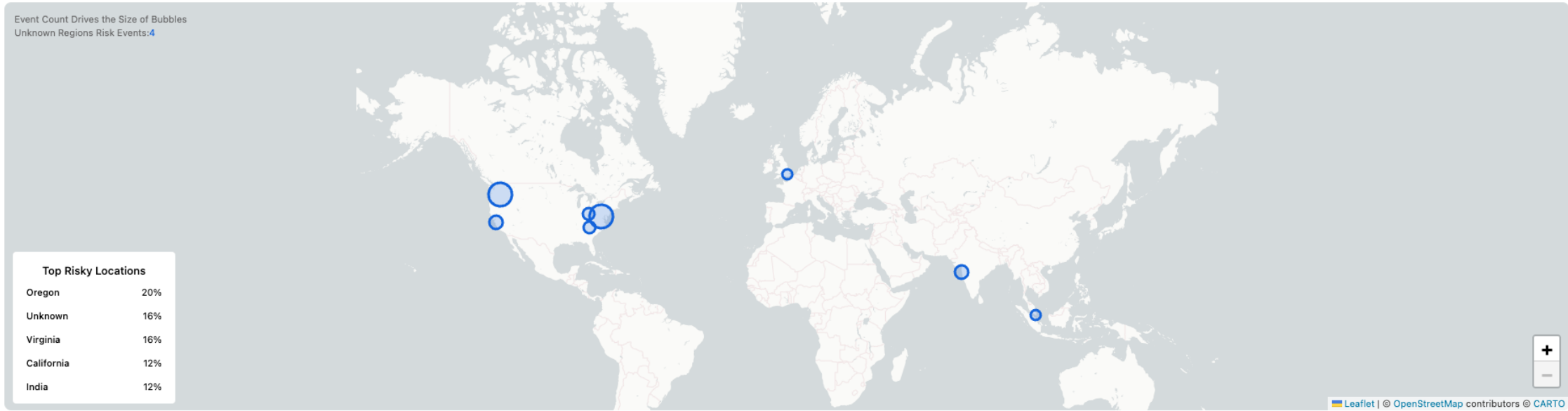
Risk Score Trend

Key Events



Customized Risk Score Risk Score Industry Peer Average Score

Risk Events by Location



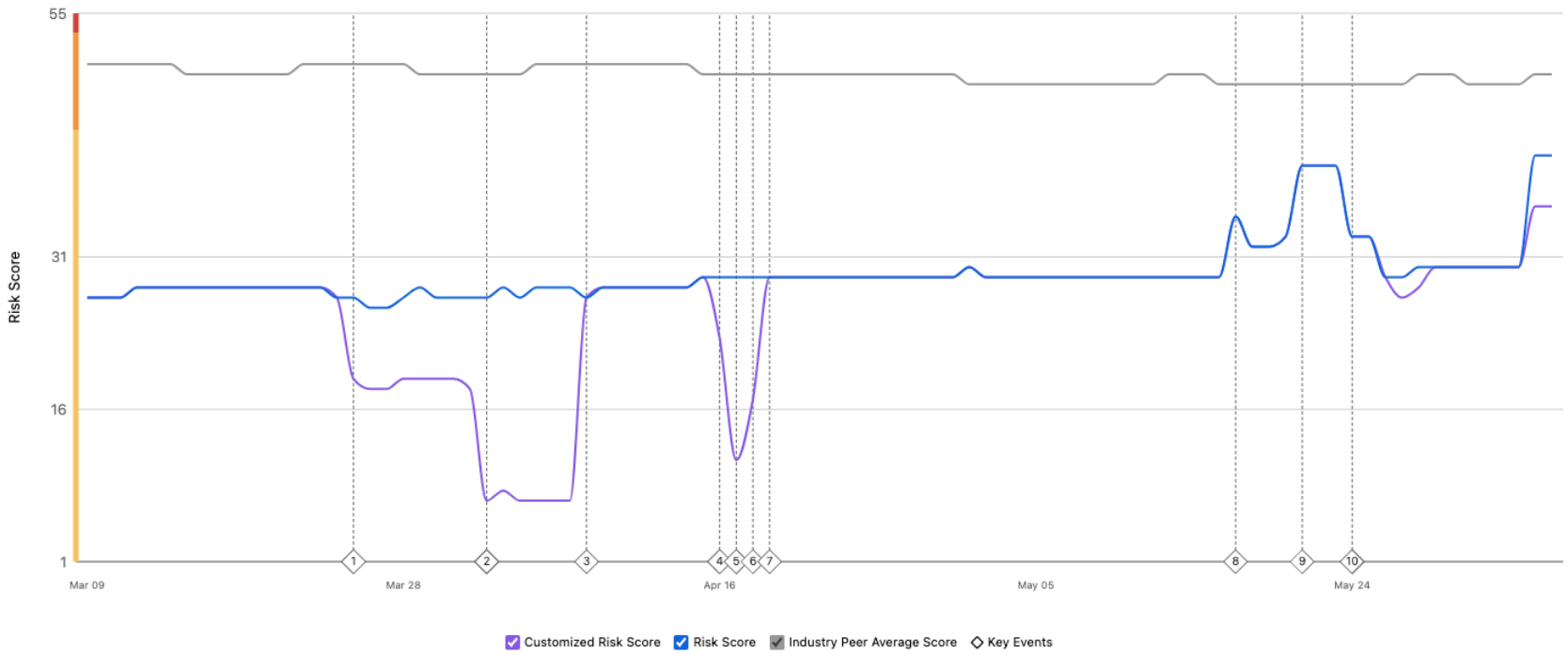
Contributing Factors by Entity

View All

Workforce 3rd Parties Applications Assets

Help

Risk Score Trend



Top 10 Events

1. Effective Date: Mar 25, 2024
   8.47 point drop (27.34 ↘ 18.87)
   Posture Profiles Not Used in Access Policies (-3.48)
   VPN Usage Observed (-5.00)
2. Effective Date: Apr 02, 2024
   11.54 point drop (18.38 ↘ 6.84)
   Application Segments with Open Ports (-2.17)
   Deception Not Enabled (-2.17)
   DLP Policy Violations (-3.05)
   Unscanned SSL Traffic (-0.11)
   Severe Botnet Infections Observed (-0.98)
   Risky Application Usage (-3.05)
3. Effective Date: Apr 08, 2024
   19.99 point increase (7.03 ↗ 27.02)
   Application Segments with Open Ports (2.17)
   Posture Profiles Not Used in Access Policies (3.48)
   Deception Not Enabled (2.17)
   VPN Usage Observed (5.00)
   DLP Policy Violations (3.05)
   Data Uploaded to Unsanctioned Application (-0.92)
   Unscanned SSL Traffic (0.02)
   Severe Botnet Infections Observed (1.96)
   Risky Application Usage (3.05)
4. Effective Date: Apr 16, 2024
   6.26 point drop (29.18 ↘ 22.92)
   VPN Usage Observed (-5.00)
   Exposed Servers (Services Exposed) (-1.00)
   Namespace Exposure on Internet (-0.25)
5. Effective Date: Apr 17, 2024
   11.74 point drop (22.92 ↘ 11.19)
   Application Segments with Open Ports (-2.17)
   Posture Profiles Not Used in Access Policies (-3.48)
   DLP Policy Violations (-3.05)
   Unscanned SSL Traffic (0.01)
   Risky Application Usage (-3.05)
6. Effective Date: Apr 18, 2024
   6.24 point increase (11.19 ↗ 17.43)
   VPN Usage Observed (5.00)
   Exposed Servers (Services Exposed) (1.00)
   Namespace Exposure on Internet (0.25)
7. Effective Date: Apr 19, 2024
   11.74 point increase (17.43 ↗ 29.17)
   Application Segments with Open Ports (2.17)
   Posture Profiles Not Used in Access Policies (3.48)

View All Events

Dashboard

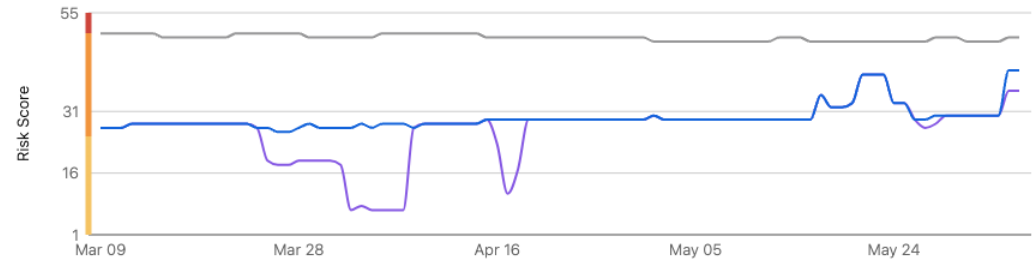
Organization Risk Score

External Attack Surface 70.00
Compromise 20.21
Lateral Propagation 21.74
Data Loss 31.46

Low Medium High Critical

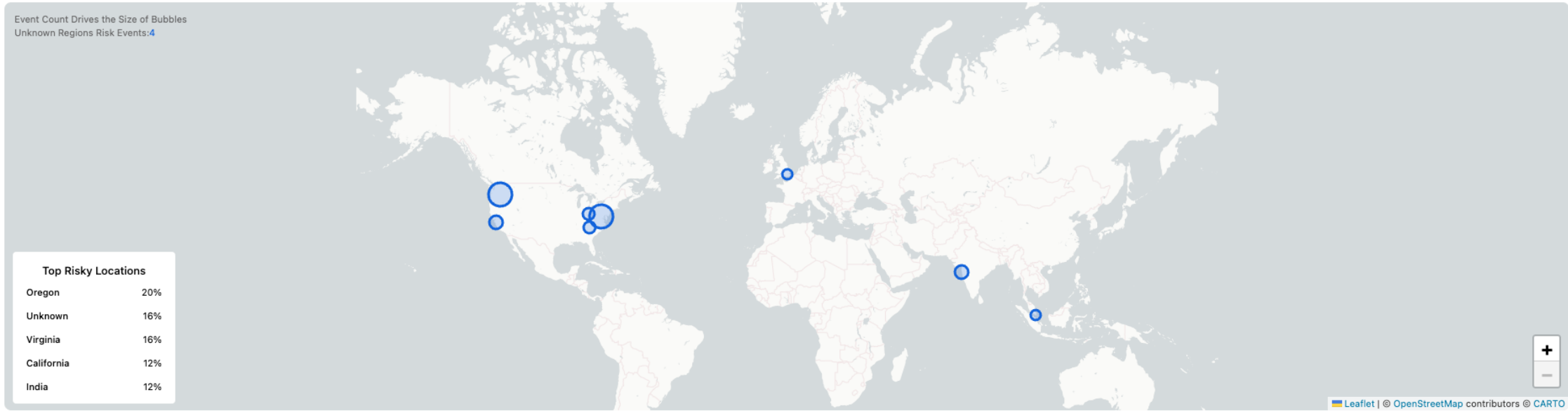
Risk Score Trend

Key Events



Customized Risk Score Risk Score Industry Peer Average Score

Risk Events by Location



Contributing Factors by Entity

View All

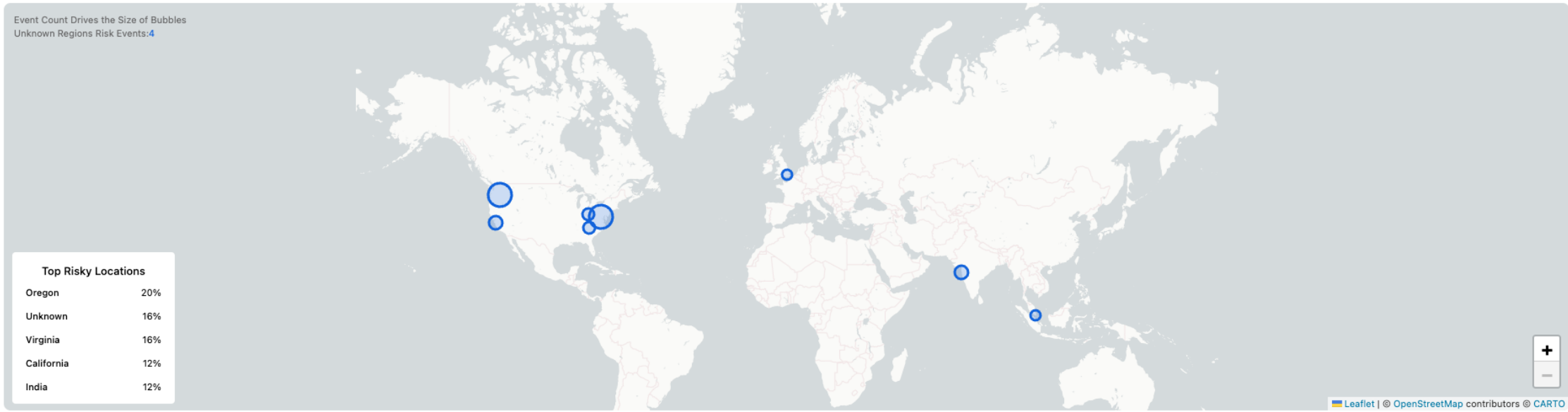
Workforce
3rd Parties
Applications
Assets

Help

Low Medium High Critical

Customized Risk Score Risk Score Industry Peer Average Score

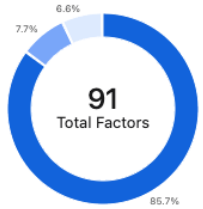
Risk Events by Location



Contributing Factors by Entity

View All

Workforce

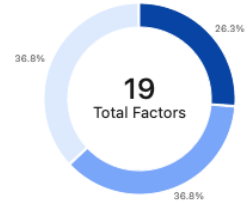


An organization's employee base creates risk concentrated primarily around compromise

3rd Parties

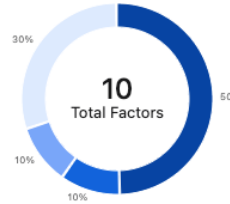
Third parties create risk related to lateral propagation and data loss

Applications



Applications are vulnerable to lateral propagation and expand an organization's external attack surface

Assets



Assets create risk distributed across the four stages of breach

External Attack Surface Compromise Lateral Propagation Data Loss

Top 10 Factors

Help

Top 10 Factors

View All

Category	Factor	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions
External Attack Surface	Known Vulnerabilities (CVEs)	6.25 / 6.25			N	Investigate these vulnerabilities* (CVEs): Critical: 3, High: 106, Medium: 236
External Attack Surface	Outdated SSL / TLS servers	5.00 / 5.00			N	Upgrade 4 servers* out of 58 exposed servers that are running outdated SSL/TLS versions.
External Attack Surface	Exposed Servers (Services Exposed)	4.00 / 5.00			N	Investigate 58 exposed servers*.
Data Loss	DLP Policy Violations	3.05 / 3.05			N	Investigate user activity resulting in active DLP policy triggers.
Data Loss	Risky Application Usage	3.05 / 3.05			N	Investigate the business use case for access to risky SaaS applications.
Lateral Propagation	Application Segments with Open Ports	2.17 / 2.17			N	Restrict ports for private application segments where possible.
Lateral Propagation	Deception Not Enabled	2.17 / 2.17			N	Configure application decoys to create high fidelity alerts.
Compromise	Sandbox - Behavioral Analysis	1.96 / 1.96			N	Configure Sandbox policies based on the recommended actions found on help site.
External Attack Surface	Namespace Exposure on Internet	1.25 / 1.25			N	Rename namespace for 198 keyword based domains with ambiguous names to eliminate leakage.
Lateral Propagation	Application Segmentation	1.09 / 5.43			N	Create application segments for 23 unsegmented FQDNs.

High Impact Recommendations

View All

External Attack Surface

Exposed Servers

Problem

These are list of servers running within your organization's network currently exposed to the Internet. The higher the number, larger will be the potential attack surface. While some of these might be intentional and available for internet use, many are often private applications that need to be made invisible to the public internet.

Recommendation

Implement a Zero Trust solution like ZPA to hide servers

External Attack Surface

External Facing Applications with Vulnerabilities

Problem

Attackers can use a public attack surface to enumerate public-facing applications and identify vulnerabilities to exploit

Recommendation

- Patch and remediate public vulnerabilities
- Consider adopting Zscaler Private Access to remove the public attack surface altogether.

Lateral Propagation

Segmentation

Problem

Attackers move laterally from a compromised endpoint. Increasing adoption of user-to-application segmentation will shrink the Lateral Movement Risk and limit the opportunity to spread laterally.

Recommendation

- Utilize Device Posture as part of segmentation policies.
- Shrink your Lateral Movement Risk by reviewing

Compromise

Malicious Content Blocks

Problem

A very high number of malicious content blocks are seen. An active infection could be one of the reasons for these high number of blocks.

Recommendation

Please review the source of these malicious content blocks. If an active infection is found, clean-up the infected systems.

Help

Contributing Factors to Organizational Risk Score

External Attack Surface 70.00 | Compromise 20.21 | Lateral Propagation 21.74 | Data Loss 31.46

List View | Tree View

Search

Factor	Category	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions	Include
Known Vulnerabilities (CVEs)	External Attack Surface	6.25 /6.25			N	Investigate these vulnerabilities* (CVEs): Critical: 3, High: 106, Medium: 236	
Outdated SSL / TLS servers	External Attack Surface	5.00 /5.00			N	Upgrade 4 servers* out of 58 exposed servers that are running outdated SSL/TLS versions.	
Exposed Servers (Services Exposed)	External Attack Surface	4.00 /5.00			N	Investigate 58 exposed servers*.	
DLP Policy Violations	Data Loss	3.05 /3.05			N	Investigate user activity resulting in active DLP policy triggers.	
Risky Application Usage	Data Loss	3.05 /3.05			N	Investigate the business use case for access to risky SaaS applications.	
Application Segments with Open Ports	Lateral Propagation	2.17 /2.17			N	Restrict ports for private application segments where possible.	
Deception Not Enabled	Lateral Propagation	2.17 /2.17			N	Configure application decoys to create high fidelity alerts.	
Sandbox - Behavioral Analysis	Compromise	1.96 /1.96			N	Configure Sandbox policies based on the recommended actions found on help site.	
Namespace Exposure on Internet	External Attack Surface	1.25 /1.25			N	Rename namespace for 198 keyword based domains with ambiguous names to eliminate ...	
Application Segmentation	Lateral Propagation	1.09 /5.43			N	Create application segments for 23 unsegmented FQDNs.	
Public Cloud - Exposed instances	External Attack Surface	1.00 /2.50			N	Investigate 40 exposed servers.	
Malware (Malicious Content Blocked)	Compromise	0.98 /0.98			N	Investigate if user training or quarantine measures are required due to malicious content blocks ...	
Data Uploaded to Unsanctioned Application	Data Loss	0.92 /4.57			N	Investigate users uploading data to unsanctioned apps. Consider labeling application if ...	
> UEBA	Data Loss	0.85 /2.13			N	Investigate users flagged with these alerts and take necessary actions.	
Unscanned Traffic Observed From Firewall Disabled Location	Compromise	0.64 /0.66			N	Enable non-web firewall traffic inspection on 97.43% unscanned firewall traffic bytes, to reduc...	
> Advanced Settings	Compromise	0.34 /1.18			N	Configure the optimal advanced settings mix to minimize risk.	
> Mobile Advanced Threat Settings	Compromise	0.34 /0.61			N	Configure the optimal mix of mobile malware protection policies.	

Contributing Factors to Organizational Risk Score

List View | Tree View

External Attack Surface 70.00 | Compromise 20.21 | Lateral Propagation 21.74 | Data Loss 31.46

Search

Factor	Category	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions	Include
Sandbox - Behavioral Analysis	Compromise	1.96 /1.96			N	Configure Sandbox policies based on the recommended actions found on help site.	
Malware (Malicious Content Blocked)	Compromise	0.98 /0.98			N	Investigate if user training or quarantine measures are required due to malicious content blocks ...	
Unscanned Traffic Observed From Firewall Disabled Location	Compromise	0.64 /0.66			N	Enable non-web firewall traffic inspection on 97.43% unscanned firewall traffic bytes, to reduc...	
Advanced Settings	Compromise	0.34 /1.18			N	Configure the optimal advanced settings mix to minimize risk.	
Mobile Advanced Threat Settings	Compromise	0.34 /0.61			N	Configure the optimal mix of mobile malware protection policies.	
Browser Control Settings	Compromise	0.32 /0.51			N	Block outdated and known vulnerable browser versions.	
File Type Control	Compromise	0.29 /0.29			N	Consider blocking upload/download of file types such as FLASH, IPA, JAVA_APPLET, APK.	
Advanced URL Filter and Cloud App Settings	Compromise	0.10 /0.59			N	Configure Zscaler recommended URL Filtering rules and Cloud App Control policy based on you...	
Advanced Threat Settings	Compromise	0.04 /1.62			N	Enable the optimal mix of advanced threat settings to protect your users.	
Unscanned SSL Traffic	Compromise	0.03 /3.04			N	Enable inspection for 0.87% qualified SSL traffic.	
Unauthenticated Traffic	Compromise	0.01 /1.47			N	Consider reducing unauthenticated traffic.	
Active Infections	Compromise	0.00 /2.94			N	Investigate 0 active infections (botnets) and reimage the machine to eliminate future ...	
Severe Botnet Infections Observed	Compromise	0.00 /2.45			N	Quarantine machines that have botnets making callbacks to C&C hosts.	
Suspicious Domains (NRD/NOD/NADs)	Compromise	0.00 /1.47			N	Investigate users communicating with 0 NRD/NOD/NAD sites and provide user training as...	
Malware Protection Settings	Compromise	0.00 /1.13			N	Enable the recommended mix of virus and spyware settings.	
Zero Day Prevention - Sandbox Quarantine	Compromise	0.00 /0.98			N	Enable quarantine for recommended file types to prevent zero-day threats.	
URL Filtering Policy	Compromise	0.00 /0.86			N	Configure a rule to block all categories in the Legal Liability class such as Adult Material, Drug...	

Contributing Factors to Organizational Risk Score

List View | Tree View

External Attack Surface 46.55 | Compromise 21.76 | Lateral Propagation 12.20 | Data Loss 21.71

tenable

Factor	Category	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions	Include
Tenable - Attack Surface	External Attack Surface	1.94 /2.37			N	Patch / upgrade the vulnerable software ...	✓
↳ Tenable - Critical and High VPR vulnerabilities with available exploit code	External Attack Surface	1.08 /1.08			N	Investigate Critical and High severity vulnerabilities ...	✓
↳ Tenable - Critical and High severity vulnerabilities based on CVSS score	External Attack Surface	0.86 /0.86			N	Investigate these Critical or High severity vulnerabilitie...	✓
↳ Tenable - Critical and High VPR vulnerabilities with available exploit code and high threat recency	External Attack Surface	0.00 /0.43			N	Investigate Critical and High severity vulnerabilities ...	✓

Help

Contributing Factors to Organizational Risk Score

List View | Tree View

External Attack Surface 46.55 | Compromise 21.76 | Lateral Propagation 12.20 | Data Loss 21.71

crowd

Factor	Category	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions	Include
CrowdStrike - Compromise	Compromise	0.44 /1.82			N	Detailed recommendations are provided per factor.	
↳ CrowdStrike - End-of-Life Operating System	Compromise	0.18 /0.18			N	Please consider upgrading the operating system to a ...	
↳ CrowdStrike - Unmanaged Devices	Compromise	0.09 /0.09			N	If the asset is supported but unmanaged, consider ...	
↳ CrowdStrike - Unsupported Devices	Compromise	0.09 /0.09			N	Maintain an asset inventory for devices where a ...	
↳ CrowdStrike - Endpoint Security CrowdScore	Compromise	0.04 /0.45			N	Investigate key incidents in the CrowdStrike Falcon ...	
↳ CrowdStrike - Zero Trust Score	Compromise	0.04 /0.45			N	Investigate incidents related to accounts with a high ris...	
↳ CrowdStrike - Critical and High Incidents	Compromise	0.00 /0.36			N	It is recommended to address critical and high ...	
↳ CrowdStrike - High Severity XDR Detections	Compromise	0.00 /0.18			N	It is recommended to review the high severity XDR ...	
CrowdStrike - Lateral Propagation	Lateral Propagation	0.00 /1.63			N	Detailed recommendations are provided per factor.	
CrowdStrike - CVEs with Critical and High severity	External Attack Surface	0.00 /1.08			N	Patch / upgrade the vulnerable software ...	

Help

Contributing Factors to Organizational Risk

External Attack Surface 46.55 | Compromise 21.76

Factor	Category
CrowdStrike - Compromise	Compromis
↳ CrowdStrike - End-of-Life Operating System	Compromis
↳ CrowdStrike - Unmanaged Devices	Compromis
↳ CrowdStrike - Unsupported Devices	Compromis
↳ CrowdStrike - Endpoint Security CrowdScore	Compromis
↳ CrowdStrike - Zero Trust Score	Compromis
↳ CrowdStrike - Critical and High Incidents	Compromis
↳ CrowdStrike - High Severity XDR Detections	Compromis
CrowdStrike - Lateral Propagation	Lateral Prop
CrowdStrike - CVEs with Critical and High severity	External At

CrowdStrike - Zero Trust Score

Parent Factor Name: CrowdStrike - Compromise

Details | Compliance

Severity: Low

Recommended Action

Investigate incidents related to accounts with a high risk score in CrowdStrike Falcon.

Description

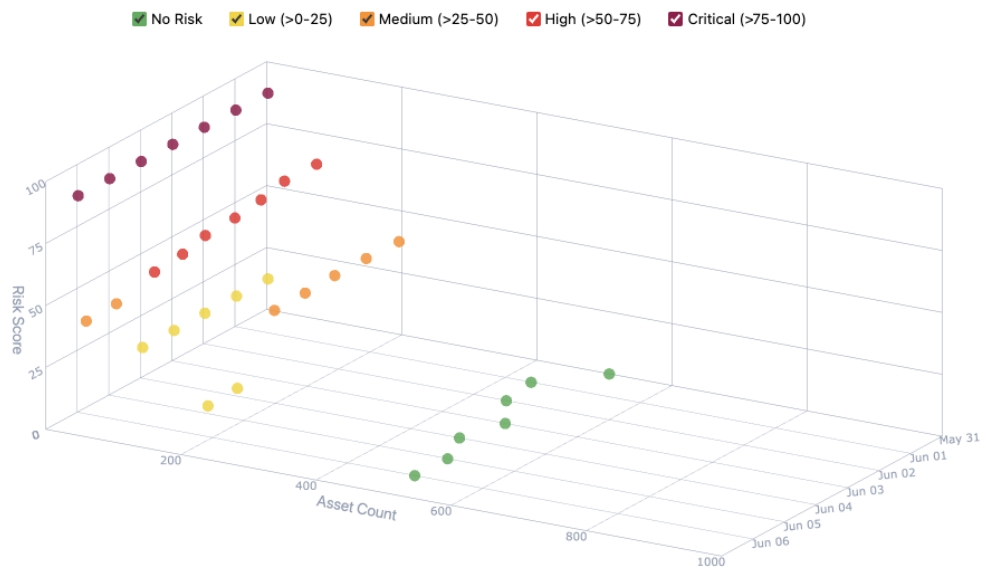
The Falcon Zero Trust Risk Score is a dynamic score resulting from the activities and the behavior of a user or computer account. It is based on the entire account information available, and, to a large extent, it represents the likelihood of the account being successfully breached by a malicious attacker or of an insider going rogue. The average overall score in your environment is 92.239075. Full list of endpoints and their score can be found in the CrowdStrike Falcon web interface.

Help

Assets

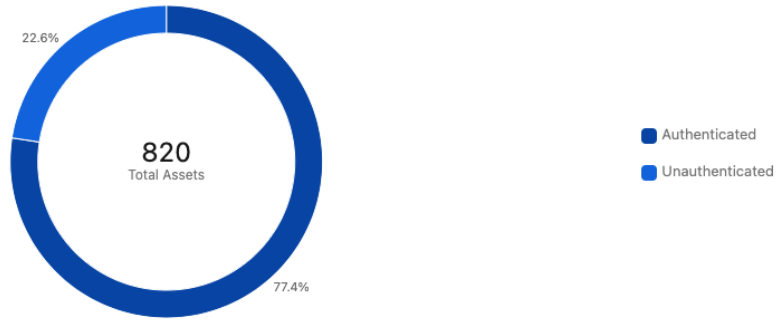
Overview

Total Assets Count: 820

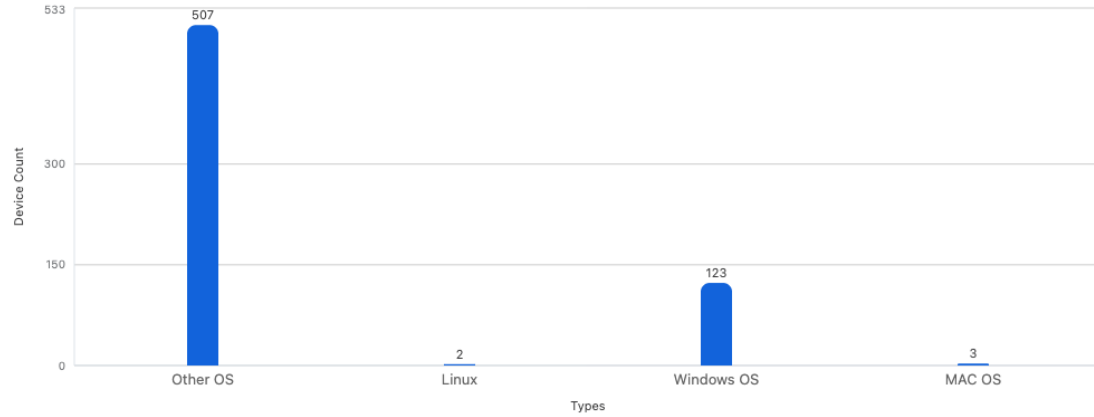


Reset chart position

Distribution of Assets by Authentication Status



Authenticated Assets



Risky Asset Inventory

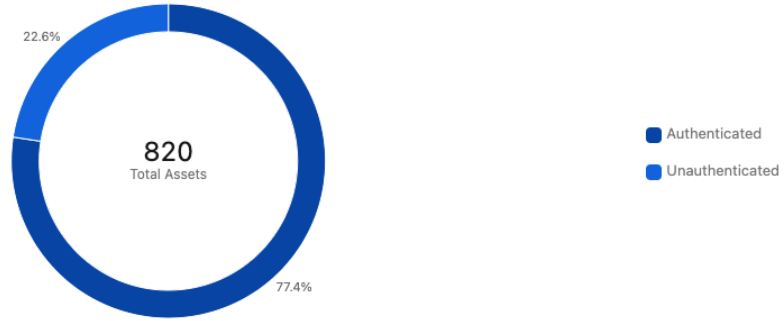
Asset ID | Asset Type | Location

Search

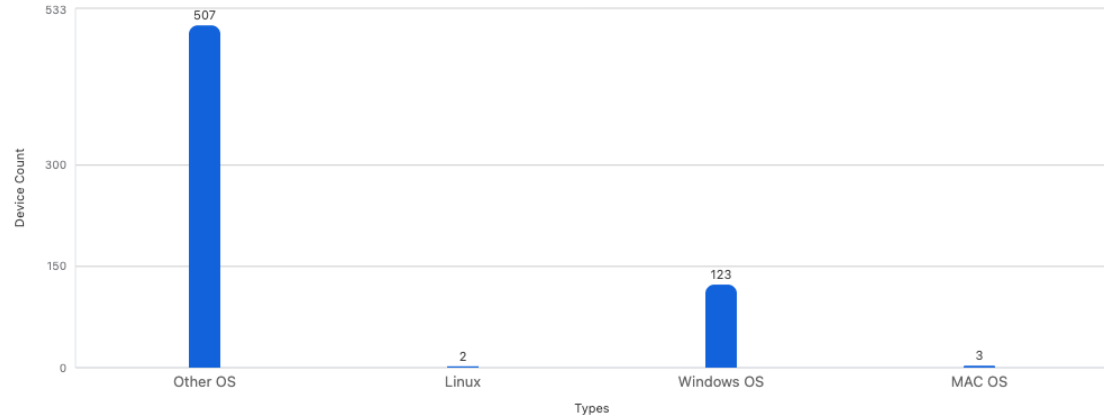
Asset ID	Private IP Address	Egress IP Address	Username	Asset Type	Authentication Status	Risk Score	Last Seen

Reset chart position

Distribution of Assets by Authentication Status



Authenticated Assets



Risky Asset Inventory

Asset ID | Asset Type | Location

Search

Asset ID	Private IP Address	Egress IP Address	Username	Asset Type	Authentication Status	Risk Score	Last Seen
41bec0685a5ee81b99c872e35fdadd49	192.168.1.29	103.247.111.65	user_109360279	Other OS	Authenticated	100.00	May 31 2024 09:01:46 AM UTC
d4582c47c3ed009e8534c4f73754154c	172.20.10.4	119.234.32.41	user_107502105	Other OS	Authenticated	72.63	Jun 05 2024 06:23:41 AM UTC
01fe11bbfc0c2e89aee985799b68d9af	10.0.0.2	206.198.150.49	user_82640181	Windows OS	Authenticated	67.53	Jun 03 2024 01:36:41 AM UTC
07767fd199804d70dd1dc6755eb0952a	10.0.0.2	206.198.150.49	user_82636419	Windows OS	Authenticated	67.53	May 30 2024 07:47:37 PM UTC
0a0e0ada4e9a489c7b09e0761addf142	10.0.0.2	206.198.150.52	user_82735517	Other OS	Authenticated	67.53	Jun 06 2024 07:40:02 PM UTC
0b741d45be8ae1631e60a0f07010e283	10.0.0.2	206.198.150.51	user_82636418	Windows OS	Authenticated	67.53	Jun 02 2024 07:32:47 PM UTC
1147f886676b913d7077681695a2a64d	10.0.0.2	206.198.150.49	user_82476945	Other OS	Authenticated	67.53	Jun 05 2024 07:32:39 PM UTC
157f7ed04476135f5aa3d387c09db718	10.0.0.2	206.198.150.51	user_82634118	Windows OS	Authenticated	67.53	May 30 2024 06:07:57 PM UTC
16ac7c2b92f084936c601d949a7c633a	10.0.0.2	206.198.150.53	user_82641660	Other OS	Authenticated	67.53	Jun 06 2024 03:59:35 PM UTC

Contributing Factors to Organizational Risk

External Attack Surface 46.55 | Compromise 21.76

Factor	Category
Tenable - Attack Surface	External At
Tenable - Critical and High VPR vulnerabilities with available exploit code	External At
Tenable - Critical and High severity vulnerabilities based on CVSS score	External At
Tenable - Critical and High VPR vulnerabilities with available exploit code and high threat recency	External At

Tenable - Critical and High VPR vulnerabilities with available exploit code

Parent Factor Name: Tenable - Attack Surface

Details | Compliance

Severity: ● Critical

Recommended Action

Investigate Critical and High severity vulnerabilities based on VPR score and High, Functional and PoC exploit code maturity which are either in Open or Reopened State and are discoverable in your environment

Description

This is the breakdown of Critical and High severity vulnerabilities based on VPR score and exploit code maturity which are either in Open or Reopened State and are discoverable in your environment.

Count	VPR Category	Exploit Code Maturity
50	Critical	High
143	Critical	Functional
11	Critical	PoC
9	High	High
219	High	Functional
402	High	PoC

First, identify services that must be publicly exposed and immediately apply known patches to remove the vulnerability.

Second, identify any services that are meant to be internal and leverage Zscaler Private Access to eliminate the exposure.

Finally, identify any services that are no longer in use and remove them entirely.

You may also create perimeter decoys that 'mimic' exposed assets via strategically configured honeypots, by leveraging Zscaler Deception. If licensed, you can create perimeter decoys by visiting the Threat Intelligence section of Deception.

Useful Links:

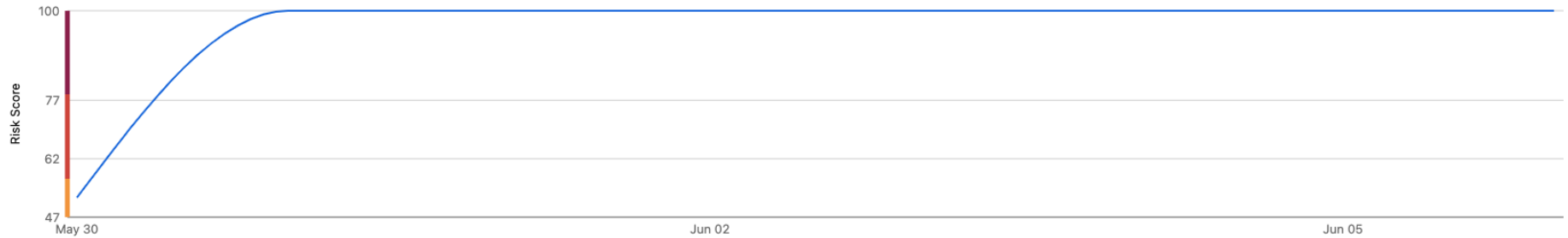
- Creating Exposed Server Decoys
- Step by step configuration guide for ZPA

Help

Assets > ID: 41bec0685a5ee81b99c872e35fdadd49

Asset Risk Score

Asset Risk Score Trend



Asset Details

Asset ID	41bec0685a5ee81b99c872e35fdadd49	Department	department_48863618	Device Hostname	N/A
Username	user_109360279	Asset Type	Other OS	OS Type	Other OS
Private IP	192.168.1.29	Last Seen	May 31 2024 09:01:46 AM UTC	OS Version	N/A
Egress IP	103.247.111.65	Authentication Status	Authenticated		
Location	Road Warrior	Enrolled Device Type Version	N/A		

Asset Location

Events Contributing to Risk Score for Last 7 Days

- Malware block: malicious file
  May 31 2024 09:01:46 AM UTC | Malware
- Sandbox block inbound response: malicious file
  May 31 2024 08:48:19 AM UTC | Malware
- Sandbox block inbound response: malicious file
  May 31 2024 08:48:16 AM UTC | Malware
- Sandbox block inbound response: malicious file
  May 31 2024 08:48:12 AM UTC | Malware
- Sandbox block inbound response: malicious file
  May 31 2024 08:48:07 AM UTC | Malware


Risk360
Search
Dashboard
Factors
Assets Beta
Insights
Financial Risk
Frameworks
MITRE ATT&CK®
NIST CSF
Reports
Alerts Beta
My Profile
Help
Logout
MITRE ATT&CK® (v13.1)
Legend
Active Subscription
Zscaler for Users Enterprise Licens...
47%
106 out of 226
Techniques Covered
Zscaler Coverage 106
Custom Coverage 0
Not Covered 120
Configurations 106
Configured 24
Misconfigured 82
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
T1595 Active Scanning 3
T1592 Gather Victim Host Information 4
T1589 Gather Victim Identity... 3
T1590 Gather Victim Network... 6
T1591 Gather Victim Org Information 4
T1598 Phishing for Information 3
T1597 Search Closed Sources 2
T1596 Search Open Technical... 5
T1593 Search Open Websites/Doma... 3
T1594 Search Victim-Owned Websites
T1650 Acquire Access
T1583 Acquire Infrastructure 8
T1586 Compromise Accounts 3
T1584 Compromise Infrastructure 7
T1587 Develop Capabilities 4
T1585 Establish Accounts 3
T1588 Obtain Capabilities 6
T1608 Stage Capabilities 6
T1189 Drive-by Compromise
T1190 Exploit Public-Facing... 9
T1133 External Remote Services
T1200 Hardware Additions
T1566 Phishing 3
T1091 Replication Through...
T1195 Supply Chain Compromise 3
T1199 Trusted Relationship
T1078 Valid Accounts 4
T1651 Cloud Administration...
T1059 Command and Scripting... 9
T1609 Container Administration...
T1610 Deploy Container
T1203 Exploitation for Client Execution
T1559 Inter-Process Communication 3
T1106 Native API
T1053 Scheduled Task/Job 5
T1648 Serverless Execution
T1129 Shared Modules
T1072 Software Deployment...
T1569 System Services 2
T1204 User Execution
T1098 Account Manipulation 5
T1197 BITS Jobs
T1547 Boot or Logon Autostart... 14
T1037 Boot or Logon Initialization... 5
T1176 Browser Extensions
T1554 Compromise Client Software...
T1136 Create Account 3
T1543 Create or Modify System Process 4
T1546 Event Triggered Execution 16
T1133 External Remote Services
T1574 Hijack Execution Flow 12
T1525 Implant Internal Image
T1556 Modify Authentication...
T1548 Abuse Elevation Control... 4
T1134 Access Token Manipulation 5
T1547 Boot or Logon Autostart... 14
T1037 Boot or Logon Initialization... 5
T1543 Create or Modify System Process 4
T1484 Domain Policy Modification 2
T1611 Escape to Host
T1546 Event Triggered Execution 16
T1068 Exploitation for Privilege...
T1574 Hijack Execution Flow 12
T1055 Process Injection 12
T1053 Scheduled Task/Job 5
T1078 Valid Accounts
T1548 Abuse Elevation Control... 4
T1134 Access Token Manipulation 5
T1197 BITS Jobs
T1612 Build Image on Host
T1622 Debugger Evasion
T1140 Deobfuscate/Decode Files or...
T1610 Deploy Container
T1484 Domain Policy Modification 2
T1480 Execution Guardrails 1
T1211 Exploitation for Defense Evasion
T1222 File and Directory... 2
T1564 Hide Artifacts
T1557 Adversary-in-the-Middle 3
T1110 Brute Force 4
T1555 Credentials from Password Stores 5
T1212 Exploitation for Credential...
T1187 Forced Authentication
T1606 Forge Web Credentials 2
T1056 Input Capture 4
T1556 Modify Authentication... 8
T1111 Multi-Factor Authentication...
T1621 Multi-Factor Authentication...
T1040 Network Sniffing
T1003 OS Credential Dumping 8
T1528 Steal Application Access Token
T1087 Account Discovery 4
T1010 Application Window...
T1217 Browser Information...
T1580 Cloud Infrastructure...
T1538 Cloud Service Dashboard
T1526 Cloud Service Discovery
T1619 Cloud Storage Object Discovery
T1613 Container and Resource...
T1622 Debugger Evasion
T1652 Device Driver Discovery
T1482 Domain Trust Discovery
T1083 File and Directory...
T1615 Group Policy Discovery
T1210 Exploitation of Remote Services
T1534 Internal Spearphishing
T1570 Lateral Tool Transfer
T1563 Remote Service Session Hijacking 2
T1021 Remote Services 7
T1091 Replication Through...
T1072 Software Deployment...
T1080 Taint Shared Content
T1550 Use Alternate Authentication... 4

MITRE ATT&CK® (v13.1)

Legend

Active Subscription

Zscaler for Users Enterprise Licens...

47%

106 out of 226

Techniques Covered

Zscaler Coverage	106
Custom Coverage	0
Not Covered	120

Configurations	106
Configured	24
Misconfigured	82

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1098 Account Manipulation 5	T1548 Abuse Elevation Control... 4	T1548 Abuse Elevation Control... 4	T1557 Adversary-in-the-Middle 3	T1087 Account Discovery 4	T1210 Exploitation of Remote Services	T1557 Adversary-in-the-Middle 3	T1071 Application Layer Protocol 4	T1020 Automated Exfiltration 1	T1531 Account Access Removal
T1197 BITS Jobs	T1134 Access Token Manipulation 5	T1134 Access Token Manipulation 5	T1110 Brute Force 4	T1010 Application Window...	T1534 Internal Spearphishing	T1560 Archive Collected Data 3	T1092 Communication Through...	T1030 Data Transfer Size Limits	T1485 Data Destructio
T1547 Boot or Logon Autostart... 14	T1547 Boot or Logon Autostart... 14	T1197 BITS Jobs	T1555 Credentials from Password Stores 5	T1217 Browser Information...	T1570 Lateral Tool Transfer	T1123 Audio Capture	T1132 Data Encoding 2	T1048 Exfiltration Over Alternative... 3	T1486 Data Encrypted for Impact
T1037 Boot or Logon Initialization... 5	T1037 Boot or Logon Initialization... 5	T1612 Build Image on Host	T1212 Exploitation for Credential...	T1580 Cloud Infrastructure...	T1563 Remote Service Session Hijacking 2	T1119 Automated Collection	T1001 Data Obfuscation 3	T1041 Exfiltration Over C2 Channel	T1565 Data Manipulation
T1176 Browser Extensions	T1543 Create or Modify System Process 4	T1622 Debugger Evasion	T1187 Forced Authentication	T1538 Cloud Service Dashboard	T1021 Remote Services 7	T1185 Browser Session Hijacking	T1568 Dynamic Resolution 3	T1011 Exfiltration Over Other Network... 1	T1491 Defacement
T1554 Compromise Client Software...	T1484 Domain Policy Modification 2	T1140 Deobfuscate/Decode Files or...	T1606 Forge Web Credentials 2	T1526 Cloud Service Discovery	T1091 Replication Through...	T1115 Clipboard Data	T1573 Encrypted Channel 2	T1052 Exfiltration Over Physical Medium 1	T1561 Disk Wipe
T1136 Create Account 3	T1611 Escape to Host	T1610 Deploy Container	T1056 Input Capture 4	T1619 Cloud Storage Object Discovery	T1072 Software Deployment...	T1530 Data from Cloud Storage	T1008 Fallback Channels	T1567 Exfiltration Over Web Service 3	T1499 Endpoint Denial of Service
T1543 Create or Modify System Process 4	T1546 Event Triggered Execution 16	T1006 Direct Volume Access	T1556 Modify Authentication... 8	T1613 Container and Resource...	T1080 Taint Shared Content	T1602 Data from Configuration... 2	T1105 Ingress Tool Transfer	T1029 Scheduled Transfer	T1495 Firmware Corruption
T1546 Event Triggered Execution 16	T1068 Exploitation for Privilege...	T1484 Domain Policy Modification 2	T1111 Multi-Factor Authentication...	T1622 Debugger Evasion	T1550 Use Alternate Authentication... 4	T1213 Data from Information... 3	T1104 Multi-Stage Channels	T1537 Transfer Data to Cloud Account	T1490 Inhibit System Recovery
T1133 External Remote Services	T1574 Hijack Execution Flow 12	T1480 Execution Guardrails 1	T1621 Multi-Factor Authentication...	T1652 Device Driver Discovery		T1005 Data from Local System	T1095 Non-Application Layer Protocol		T1498 Network Denial Service
T1674 Hijack Execution Flow 12	T1055 Process Injection 12	T1211 Exploitation for Defense Evasion	T1040 Network Sniffing	T1482 Domain Trust Discovery		T1039 Data from Network Share...	T1571 Non-Standard Port		T1496 Resource Hijacking
T1525 Implant Internal Image	T1053 Scheduled Task/Job 5	T1222 File and Directory... 2	T1003 OS Credential Dumping 8	T1083 File and Directory...		T1025 Data from Removable Media	T1572 Protocol Tunneling		T1489 Service Stop
T1556 Modify Authentication...	T1078 Valid Accounts	T1564 Hide Artifacts	T1528 Steal Application Access Token	T1615 Group Policy Discovery		T1074 Data Staged	T1090 Proxy		T1629 System Shutdown/Rebo

Reports

CISO Board Slides

Downloadable reports for security leadership summarizing the risk associated with your environment for a non-technical audience, including your financial exposure.

- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week5**
  May 25, 2024 - May 31, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week4**
  May 18, 2024 - May 24, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week3**
  May 11, 2024 - May 17, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week2**
  May 4, 2024 - May 10, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week1**
  April 27, 2024 - May 3, 2024

View All

Attack Surface Report

Downloadable powerpoint and spreadsheet reports with full detail on exposed servers and known CVEs.

- **Attack Surface Report thezerotrustexchange.com - Jun 04**
  June 4, 2024
- **Attack Surface Report thezerotrustexchange.com - May 31**
  May 31, 2024
- **Attack Surface Report thezerotrustexchange.com - May 24**
  May 24, 2024
- **Attack Surface Report thezerotrustexchange.com - May 17**
  May 17, 2024
- **Attack Surface Report thezerotrustexchange.com - May 10**
  May 10, 2024

View All

Cybersecurity Maturity Assessment Beta

Powerful, holistic reports on your zero trust journey, generated by a custom large language model (LLM) developed by Zscaler.

- **Cybersecurity Maturity Assessment - Jan 19**
  January 19, 2024
- **Cybersecurity Maturity Assessment - Dec 10**
  December 10, 2023

View All

SEC Disclosures

Sample language that can be a helpful starting point for security and legal teams in addressing the SEC's new cyber risk reporting regulations.

- **Risk360 SEC 10k Cyber Disclosures**

View All

Miscellaneous

Various materials on risk management, including a new book published on how board members can manage cyber risk.

- **Zscaler Cybersecurity eBook**
  by Andy Brown & Helmuth Ludwig

New SEC Rules for Cybersecurity Disclosures

Reports

CISO Board Slides

Downloadable reports for security leadership summarizing the risk associated with your environment for a non-technical audience, including your financial exposure.

- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week5**
  May 25, 2024 - May 31, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week4**
  May 18, 2024 - May 24, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week3**
  May 11, 2024 - May 17, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week2**
  May 4, 2024 - May 10, 2024
- **Risk360 CISOReport zscalerthree.net 44847399 May2024 Week1**
  April 27, 2024 - May 3, 2024

View All

Attack Surface Report

Downloadable powerpoint and spreadsheet reports with full detail on exposed servers and known CVEs.

- **Attack Surface Report thezerotrustexchange.com - Jun 04**
  June 4, 2024
- **Attack Surface Report thezerotrustexchange.com - May 31**
  May 31, 2024
- **Attack Surface Report thezerotrustexchange.com - May 24**
  May 24, 2024
- **Attack Surface Report thezerotrustexchange.com - May 17**
  May 17, 2024
- **Attack Surface Report thezerotrustexchange.com - May 10**
  May 10, 2024

View All

Cybersecurity Maturity Assessment Beta

Powerful, holistic reports on your zero trust journey, generated by a custom large language model (LLM) developed by Zscaler.

- **Cybersecurity Maturity Assessment - Jan 19**
  January 19, 2024
- **Cybersecurity Maturity Assessment - Dec 10**
  December 10, 2023

View All

SEC Disclosures

Sample language that can be a helpful starting point for security and legal teams in addressing the SEC's new cyber risk reporting regulations.

- **Risk360 SEC 10k Cyber Disclosures**

View All

Miscellaneous

Various materials on risk management, including a new book published on how board members can manage cyber risk.

- **Zscaler Cybersecurity eBook**
  by Andy Brown & Helmuth Ludwig

New SEC Rules for Cybersecurity Disclosures


zscaler™
Dashboard
Organization Risk Score
81
CRITICAL
Risk Score Trend
Risk Events by Location
Zscaler Risk360 Cybersecurity Maturity Assessment™
A Generative AI powered report on The Zero Trust Exchange's zero trust journey
January 19, 2024

1. Executive Summary Risk - risk score of 24.1 (compared to peers at 50.0)

Organization Risk Score

The Zero Trust Exchange's overall cybersecurity risk score is 24.1, which is significantly lower than its peers. The risk score translates to the company being approximately 76% of the way in achieving its zero trust journey. This report lays out the key findings related to The Zero Trust Exchange's cybersecurity posture.

The Zero Trust Exchange has a Data Loss Risk Score of 13.2, which is lower than the Peer Data Loss Risk Score of 46.4, because the company engages less actively in using risky applications. Its Lateral Propagation Risk Score is 35.7, below the Peer Lateral Propagation Risk Score of 66.7, due to a higher degree of application segmentation implemented by the company. The Zero Trust Exchange's Financial Risk is $9,676,259 which is lower than peers at $38,975,215.

Key statistics on The Zero Trust Exchange's cybersecurity architecture rollout:

- The Zero Trust Exchange has rolled out ZIA to all users. The Zero Trust Exchange has created 1 Sandbox rules compared to 1 for peers, 7 firewall rules compared to peers with 7, and 7 DNS rules compared to peers with 5. The company has 40+ key advanced threat settings enabled, including capabilities like detecting and blocking viruses, C2 traffic, adware/spyware, ransomware, IRC tunneling, anonymizers.
- The Zero Trust Exchange has rolled out ZPA to its users, for robust zero trust access to private applications. The Zero Trust Exchange is fairly mature in their segmentation journey, having configured 44 unique application segments (compared to peers at 13), along with 17 policies (compared to peers at 10).

The Zero Trust Exchange has made good progress in securing its cyber environment, though there is still work to be done. Some high impact recommendations are as follows. Discontinue the use of VPN services to mitigate the risk of lateral movement within the network. Implement posture checks to strengthen defenses and review access to SaaS applications to ensure necessary security measures are in place.

The Zero Trust Exchange's overall cybersecurity risk score is 24.1, which is significantly lower than its peers. The risk score translates to the company being approximately 76% of the way in achieving its zero trust journey. This report lays out the key findings related to The Zero Trust Exchange's cybersecurity posture.

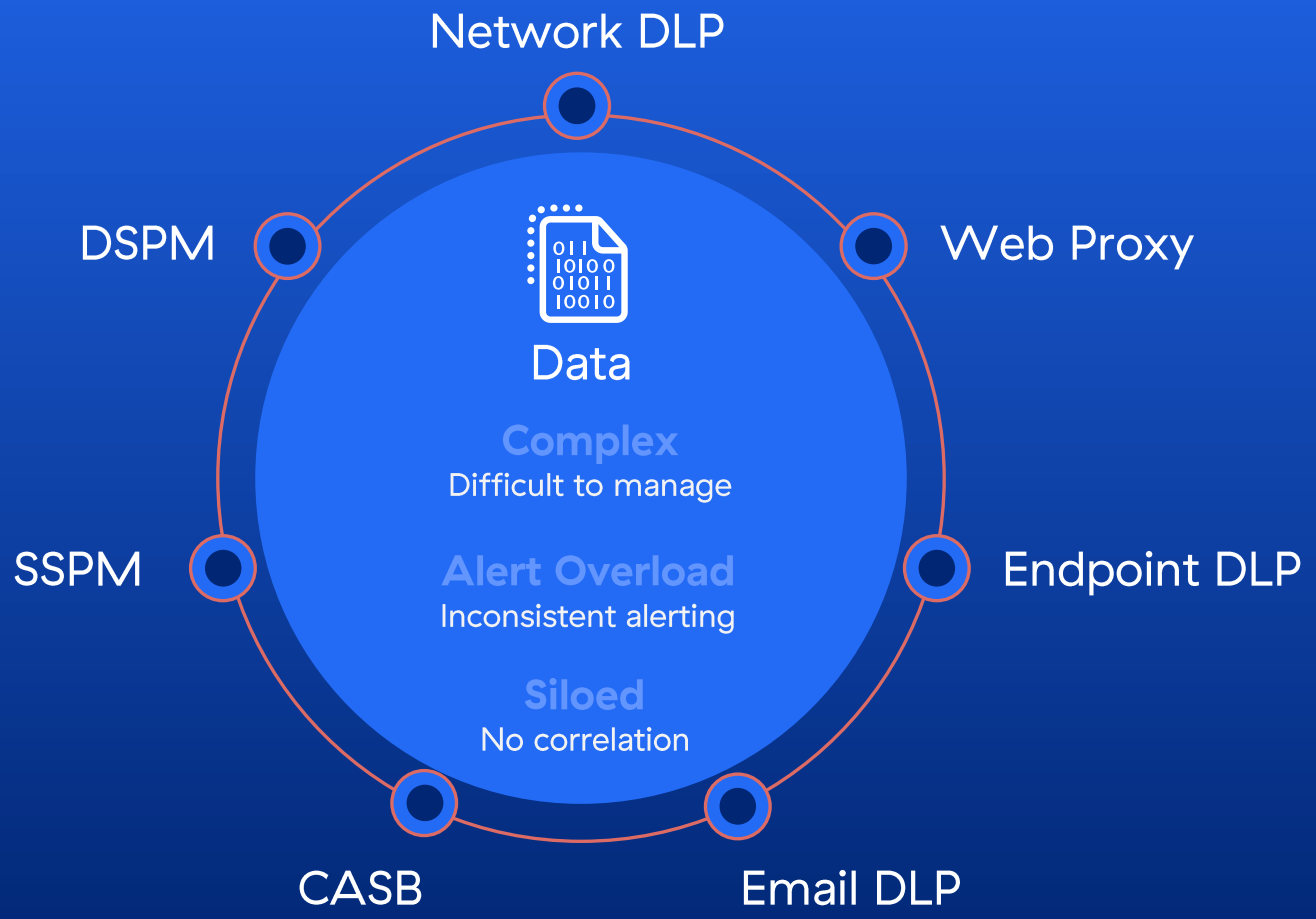
The Zero Trust Exchange has a Data Loss Risk Score of 13.2, which is lower than the Peer Data Loss Risk Score of 46.4, because the company engages less actively in using risky applications. Its Lateral Propagation Risk Score is 35.7, below the Peer Lateral Propagation Risk Score of 66.7, due to a higher degree of application segmentation implemented by the company. The Zero Trust Exchange's Financial Risk is $9,676,259 which is lower than peers at $38,975,215.

zscaler™

Data Protection

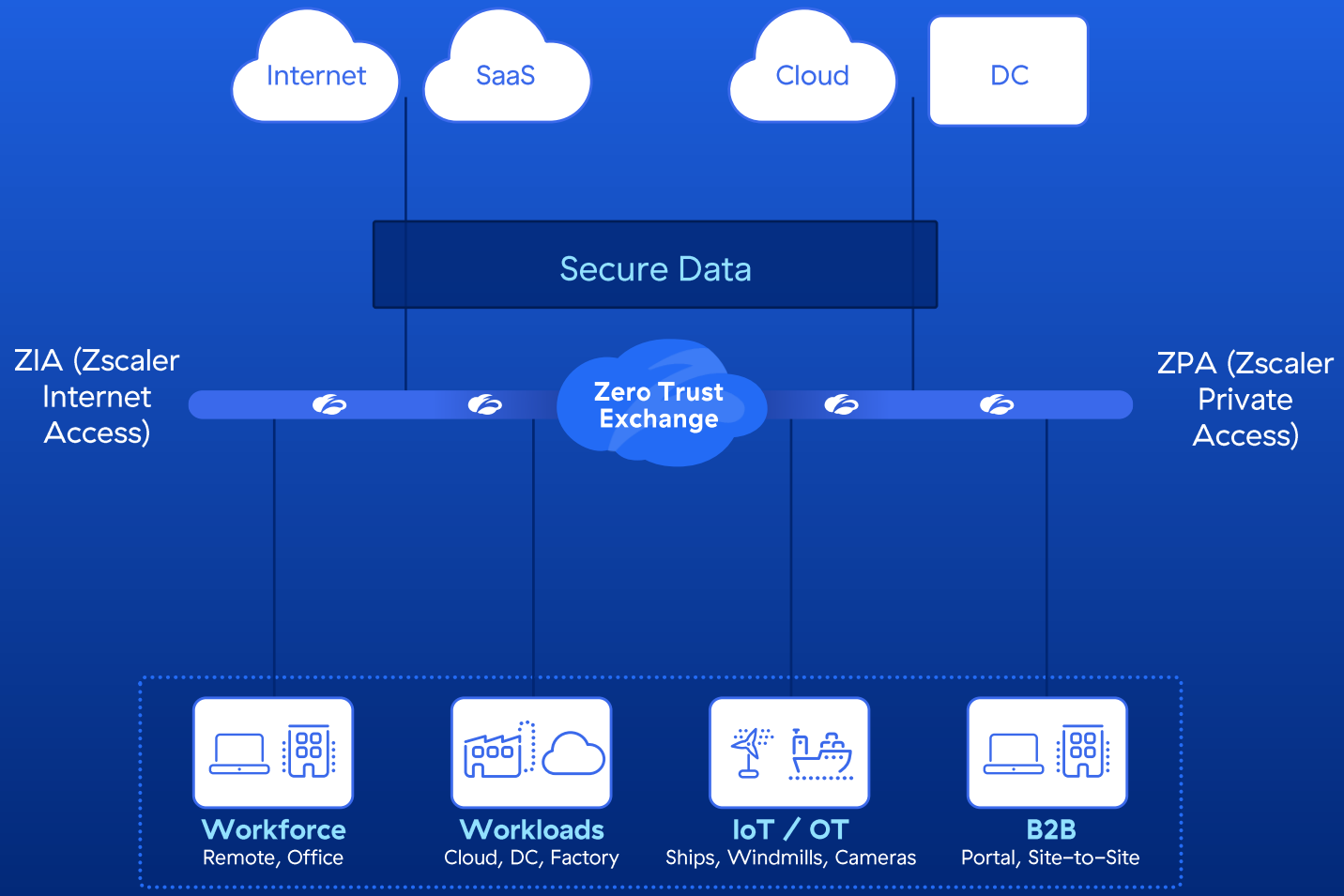
Moinul Khan
VP & GM, Data Protection

Point products for data protection leads to breaches



Zscaler has the best vantage point to deliver data security

- Inline, Inspecting all transactions at Realtime
- Secures data in all applications (Web, SaaS, On-prem & Cloud Apps)
- Natural fit for DP expansion, from Web to SaaS, to private apps, to IaaS, to Endpoint and to Email
- Integrated threat prevention to keep the bad guys out while protecting sensitive data from insider threats



Accelerating Data Protection pillar innovations

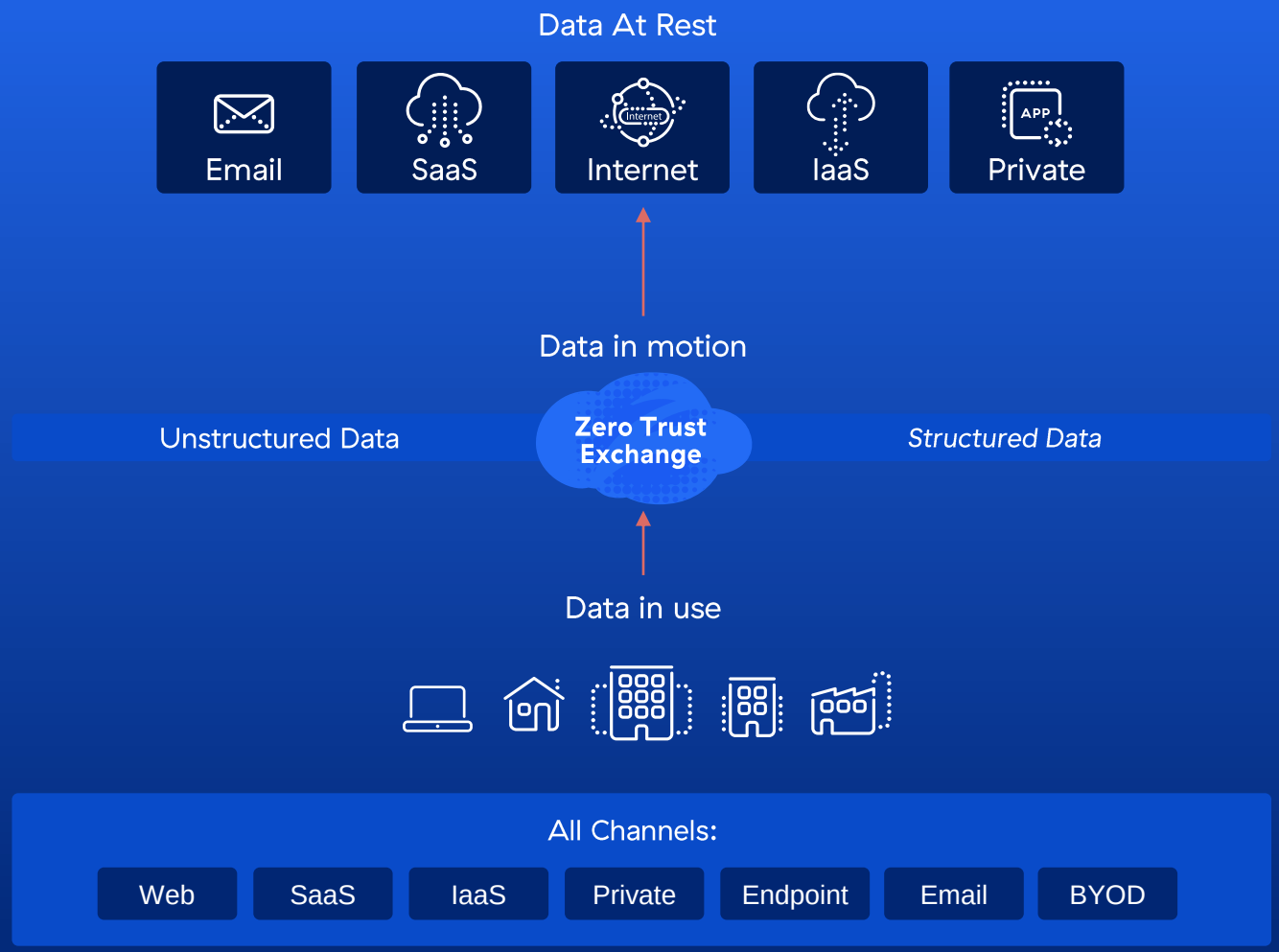
Data Protection Pillar

2019	2020	2021	2022	2023	2024
Inline Web DLP	**OCR IDM CASB**	**Private Apps Inline DLP**	**Workflow Automation**	**Endpoint DLP SaaS Supply Chain**	**Email DLP**
EDM	**MSFT AIP OOB API**	**CASB**	**AI/ML Data Discovery**	**Watermark Encryption**	**DSPM**
	Inline Web DLP	OCR IDM CASB	**SSPM**	**BYOD Browser Isolation**	**Gen-AI Security**
	EDM	MSFT AIP OOB API	Private Apps Inline DLP	Workflow Automation	Endpoint DLP SaaS Supply Chain
		Inline Web DLP	CASB	AI/ML Data Discovery	Watermark Encryption
		EDM	OCR IDM CASB	SSPM	BYOD Browser Isolation
			MSFT AIP OOB API	Private Apps Inline DLP	Workflow Automation
			Inline Web DLP	CASB	AI/ML Data Discovery
			EDM	OCR IDM CASB	SSPM
				MSFT AIP OOB API	Private Apps Inline DLP
				Inline Web DLP	CASB
				EDM	OCR IDM CASB
					MSFT AIP OOB API
					Inline Web DLP
					EDM

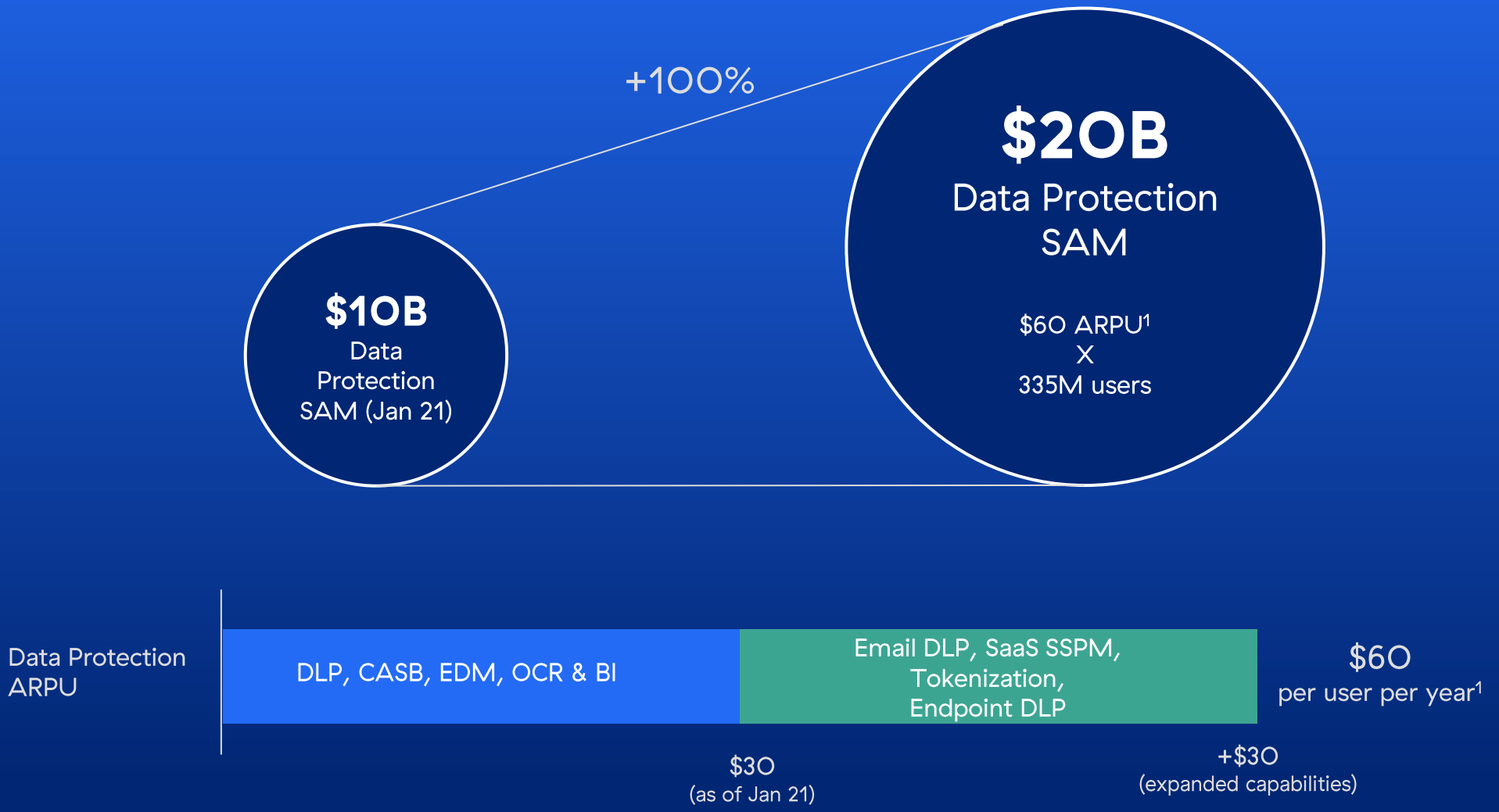
Acquisitions

	Cloudneeti	**Trustdome**	**Shift-Right**	**Canonic Security**
				SecurelyShare

Most comprehensive fully integrated Data Protection solutions



Data Protection SAM expansion driven by ARPU expansion



1. Per user pricing for individual products is effective annual prices to Zscaler for customers of 5,000 seats (also referred to as ARPU, or average revenue per user)

Data Protection customer wins

Global Bank
(New Zscaler logo)

~150k seats
SSE Play (SWG, ZTNA and DP)

Data Protection
- Inline Web DLP
- OOB CASB – Data at rest
- EDM/IDM/OCR
- Workflow automation
- 3rd party app governance (Canonic Security)
- Endpoint DLP

Fortune 500 Financial Services
(Endpoint DLP upsell)

>70k seats
Inline DLP & OO API based data at rest security

Symantec Replacement
- Leveraging the power of Zscaler platform
- Replaced Symantec Endpoint DLP with Zscaler's integrated endpoint DLP

Fortune 100 Technology
(Data Protection platform upsell)

Realized Value
After 6 months of ZIA use, realized they needed Data Protection

Replaced Digital Guardian
Data Protection Use
- Data in motion – Web DLP
- Data at rest - SaaS data
- Data in use - Endpoint DLP

zscaler™

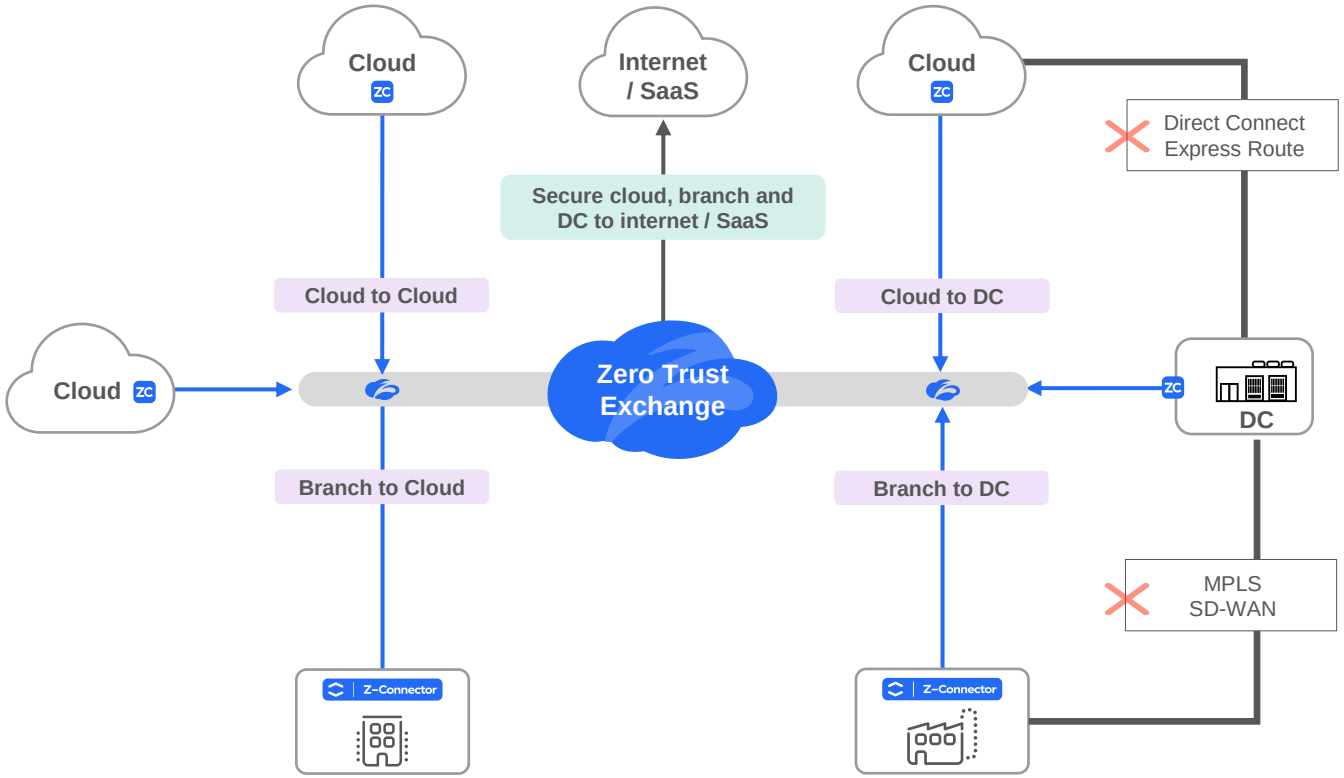
Zero Trust Networking

Naresh Kumar
VP, Product Management – Zero Trust Networking

Introducing Zero Trust Networking for Campuses and Clouds

1 Zero Trust SD-WAN

Secure Branch, Campus, Factory, Cloud, and DC Communication

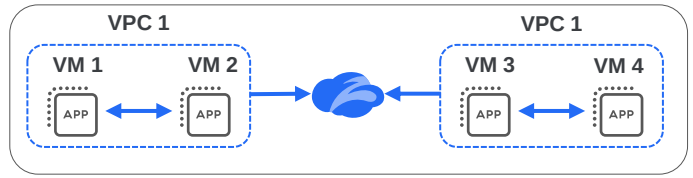


With Zero Trust SD-WAN Every branch is a Starbucks

SD-WAN, MPLS, Express Route, Direct Connect

2 Workload Communication

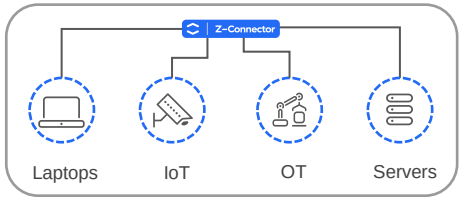
VPC to VPC, VM to VM using workload tags



Virtual Firewalls

3 Zero Trust Device Segmentation

Secure LAN Communications (IoT, OT)



NAC, East-West Firewalls

Zero Trust for Branch creating new market opportunities

Branches/Factories (including IoT/OT)

>7B Other devices[2]

(3rd party vendors and customers of customers)

~1.2B incremental devices[2]

(Commercial <2k employees)

~1.5B serviceable devices[2]

(Current target market of ~20k organizations[1] with 2k+ employees)

1. Based on Zscaler's analysis of worldwide organization and employee data from ZoomInfo
2. Based on Zscaler's analysis of worldwide commercial IoT/OT devices from Gartner
3. Average Revenue Per Device

Customer Wins

Global Legal Services
(Zero Trust SD-WAN Upsell)

70 sites
ZT400, ZT600, ZT800

Forcepoint Firewall Replacement
- Global deployment
- Replaced firewall and routers with integrated ZT device as gateway
- Site-to-site VPN replacement
- Zero Trust for IoT /OT devices in branch offices

European IT Services
(Zero Trust SD-WAN upsell)

45 sites
ZT800

Cisco Firewall & SD-WAN Replacement
- Network Modernization initiative
- Replaced Cisco SD-WAN with integrated ZT device as gateway
- Site-to-site VPN replacement
- Consistent security posture and policies

Healthcare
(Zero Trust SD-WAN upsell)

90 sites
ZT600, ZT800

Palo Firewall & Cisco SD-WAN Replacement
- Café-like branch initiative
- Network simplification & cost savings
- Site-to-site VPN challenges
- Remote printing, badge reader access, security camera streaming use cases

ZenithLive 24

Customer Journeys

Go-to-Market Strategy

Mike Rich
Chief Revenue Officer and President of Global Sales

The world's leading Zero Trust platform at the cusp of a massive opportunity

400B+	40%+	$96B	500+	50+
Daily transactions	F500 customers	Serviceable addressable market opportunity	$1M+ ARR customers	$5M+ ARR customers

Evolving the transition from transactional to account-centric selling

Focus on continuous customer value realization and account penetration

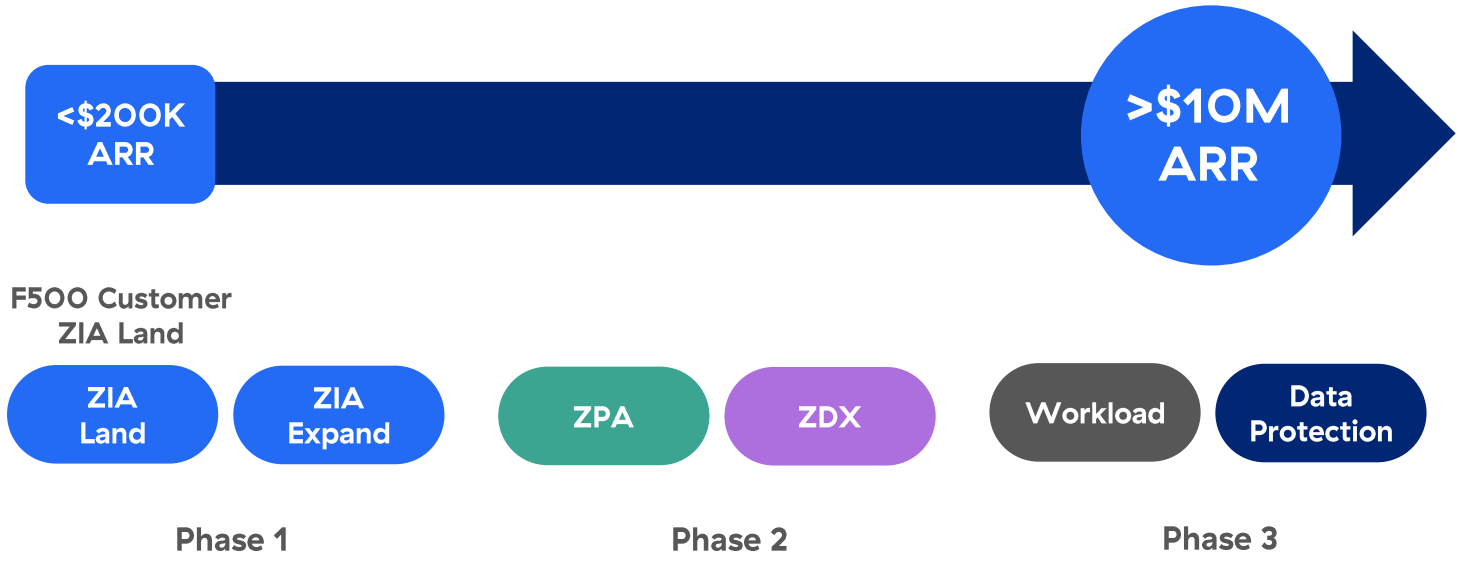
Increased footprint into the Global 2000 and Fortune 500

Collaborative pursuit of strategic focus accounts with GSIs

Scaling a proven playbook to add more $10M+ ARR customers

Results of Account-centric selling

Real Fortune 500 customer example



Global 2000 customers with <$1M ARR today

400+

Stronger GSI partnerships to drive greater value for customers

Zscaler already delivers customer outcomes that are important to GSIs

- Acceleration of large transformation projects
- Cost take out
- Network modernization
- Cloud migration
- M&A

Stepping up GSI partnerships with dedicated programs

- Get embedded into managed service practice
- CEO–to–CEO and executive connections with top GSIs
- Developing joint pursuit plans with strategic accounts
- Building dedicated GSI sales team

Verticalization will drive significant upsell and new logos

FY25 Focus	Future	Maximize TAM capture
Healthcare	Financial Services	Dedicated sales and marketing teams
Public Sector	Manufacturing	Specialized knowledge (e.g., regulations)
	Technology	Purpose-built, scalable solutions
		Specialized partners

Drive new logo, cross-sell, and upsell

Achieving scalability with simplicity

Simplification

Standardizing for Scalability

Decrease complexity for sellers

Global operating cadence and excellence

Driving a repeatable set of outcomes

Unify similar sales motions

Value Realization

Strengthening Customer Centricity

Value based sales methodology

Align pre- and post-sales activities to support the entire customer journey

Mutual success account plans

Acceleration

Activating Our Force Multipliers

People

Right sizing quota and territories to succeed.

Platform

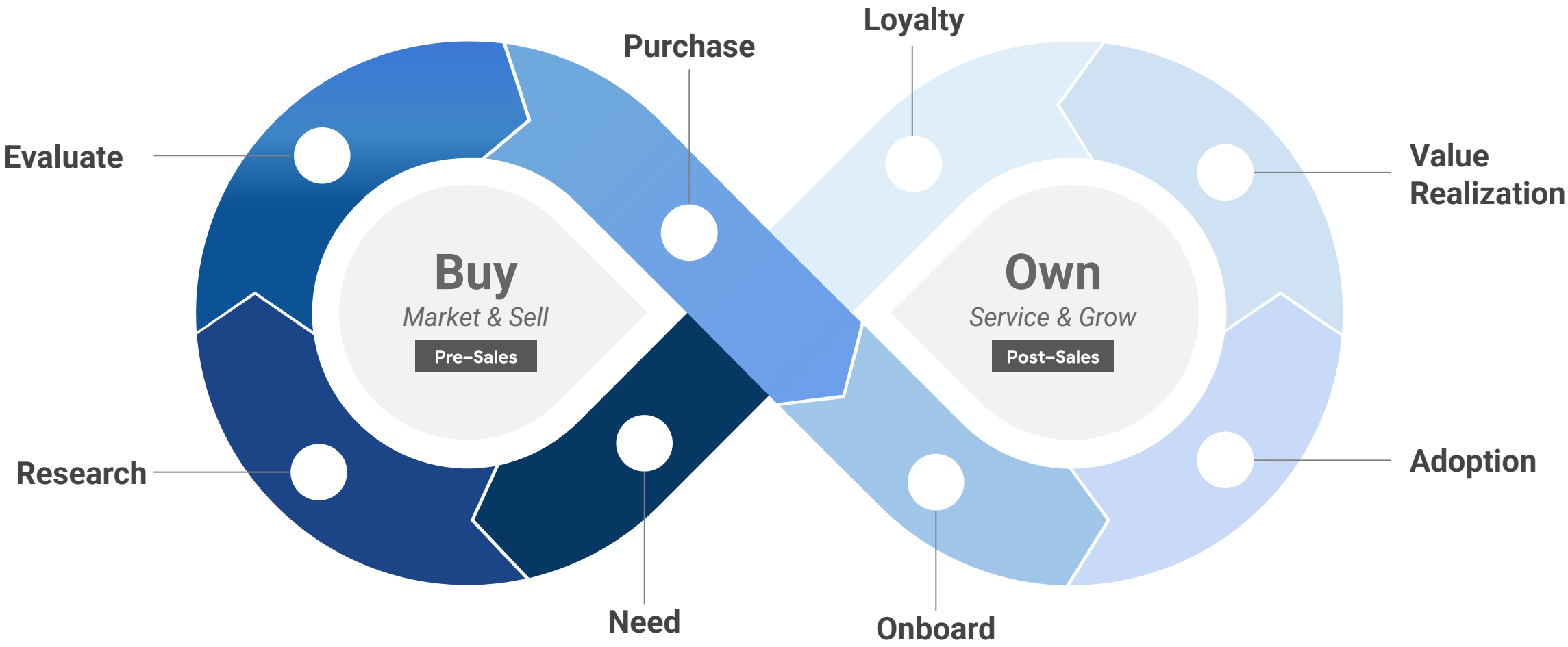
Enable sales to deliver value through our highly differentiated Zscaler Zero Trust platform.

Partners

GSIs targeted at majors and government. Scaling commercial motion through partner ecosystem.

Delight the customer at every stage

DRIVE PROGRESSION THROUGH CUSTOMER-CENTRIC "MOMENTS THAT MATTER"



Closing

Jay Chaudhry
Founder, Chairman, and CEO

Our platform is expanding to a class of its own

1. Our Zero Trust Exchange platform **expanded beyond traditional SASE** with innovations that are aligned with customer needs. These innovations are also **increasing our serviceable addressable market to $96B.**

2. With **Zscaler's Zero Trust Exchange data and Avalor's Data Fabric technology**, we will deliver unique AI-driven innovations to disrupt the traditional security risk management and operations market.

3. Zscaler has the **best vantage point to deliver Data Protection** as we are sitting inline with the traffic. We have accelerated the pace of innovations, and we have the most comprehensive data protection platform.

4. **Zero Trust SD-WAN** enables every branch and factory to be treated like a Starbucks, which means there is no lateral threat movement. **Zero Trust segmentation** eliminates the need for firewall-based segmentation.

5. **Building a strong Go-To-Market organization** to drive durable high growth and capture our large market opportunity.