Zscaler – Sicher, flexibel, intelligent

Wie Zscaler Unternehmen in der digitalen Welt mit Hilfe der KI schützt

Mike Schumak
Partner Consulting Sales Engineer

16.09.2025, Congress Park Hanau

Zscaler - Sicher, flexibel, intelligent:

Wie wir Unternehmen in der digitalen Welt mit Hilfe der KI schützen

Mike Schumak, Partner Consulting Sales Engineer

Agenda

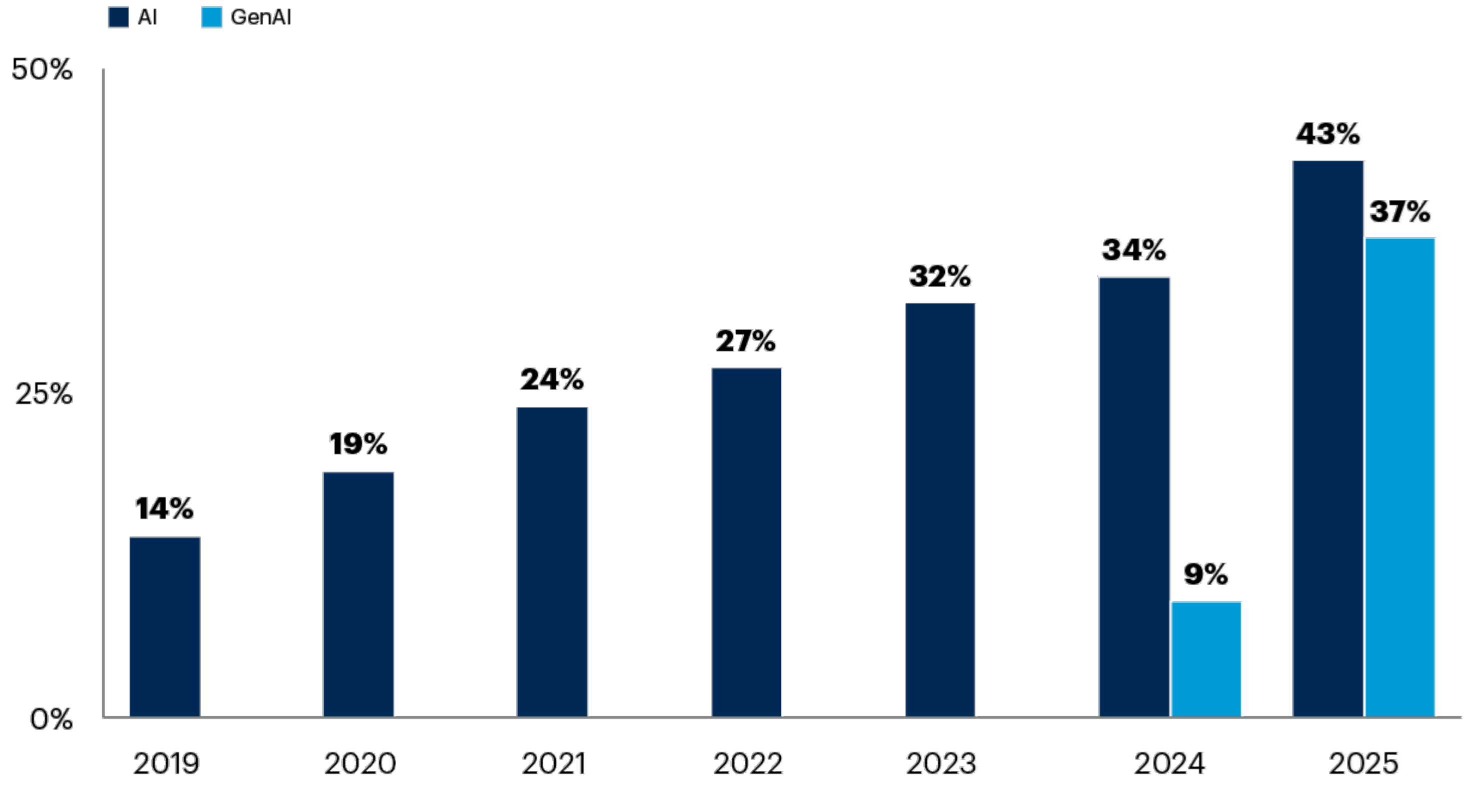
1. AI in the Zero Trust Industry
2. AI in Foundational Zscaler Platforms
3. AI in Advanced Zscaler Platforms
4. TikTok Perspective on Zero Trust AI
5. AI in Extensions from Core Zscaler Platforms

AI in the Zero Trust Industry

How pervasive is AI in your organization?

Rise of AI in the Industry

Deployment of Artificial Intelligence
Percentage of respondents



n = 2,882 (2019), 1,063 (2020), 1,825 (2021), 2,363 (2022), 2,186 (2023), 2,443 (2024), 3,143 (2025)

Q: What are your enterprise's plans in terms of the following digital technologies and trends?

Source: Gartner CIO and Technology Executive Agenda Surveys, 2019 through 2025

822902_C

Active AI projects by organizations around the globe, training their own models, and procuring their own data.

Gartner: “Geopolitics Is Shaping Generative AI (and Vice Versa). 13 December 2024

Is AI GOOD or BAD ?

it depends …

Real World Data on AI

What impact does AI have on the retail industry ?

PuroMarketing

Market analyst firm PuroMarketing conducted a study on the impact of AI in retail, finding:

15% to 20% reduced operating cost

by automating tasks, improving staff efficiency, optimizing product distribution

30% increased inventory accuracy

avoiding overstocking and stockouts

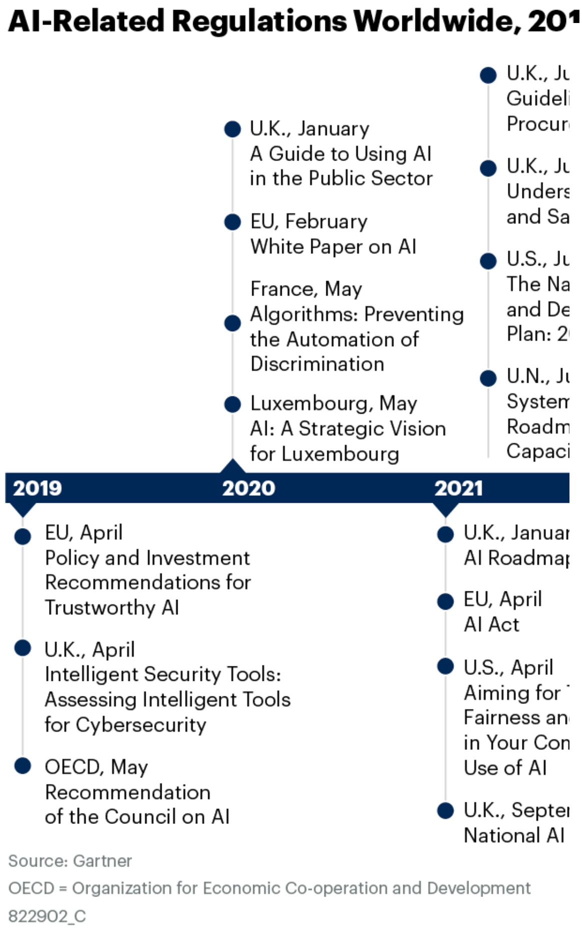
10% to 15% sales growth

personalization to push offers

PuroMarketing: https://www.puromarketing.com/145/214545/datos-revelan-impacto-inteligencia-artificial-eficiencia-sector-retail. October 2024

99.3% of Zscaler revenue comes from AI-powered products.

AI Regulations Around the World



AI-Related Regulations Worldwide, 2019 to 2022

- U.K., January
  A Guide to Using AI in the Public Sector
- EU, February
  White Paper on AI
- France, May
  Algorithms: Preventing the Automation of Discrimination
- Luxembourg, May
  AI: A Strategic Vision for Luxembourg
- U.K., Ju
  Guidel
  Procur
- U.K., Ju
  Unders
  and Sa
- U.S., Ju
  The Na
  and De
  Plan: 2
- U.N., Ju
  System
  Roadm
  Capaci

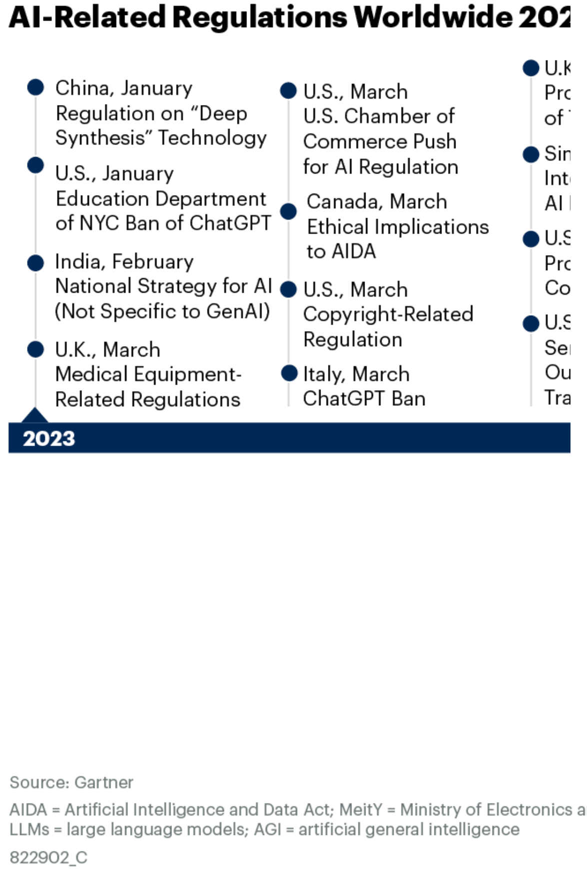
2019 2020 2021

- EU, April
  Policy and Investment Recommendations for Trustworthy AI
- U.K., April
  Intelligent Security Tools: Assessing Intelligent Tools for Cybersecurity
- OECD, May
  Recommendation of the Council on AI
- U.K., Januar
  AI Roadmap
- EU, April
  AI Act
- U.S., April
  Aiming for
  Fairness an
  in Your Con
  Use of AI
- U.K., Septer
  National AI

Source: Gartner

OECD = Organization for Economic Co-operation and Development

822902_C



AI-Related Regulations Worldwide 202

- China, January
  Regulation on "Deep Synthesis" Technology
- U.S., January
  Education Department of NYC Ban of ChatGPT
- India, February
  National Strategy for AI (Not Specific to GenAI)
- U.K., March
  Medical Equipment-Related Regulations
- U.S., March
  U.S. Chamber of Commerce Push for AI Regulation
- Canada, March
  Ethical Implications to AIDA
- U.S., March
  Copyright-Related Regulation
- Italy, March
  ChatGPT Ban
- U.K
  Pro
  of
- Sin
  Int
  AI I
- U.S
  Pro
  Co
- U.S
  Se
  Ou
  Tra

2023

for using AI model/LLMs

- EU, March
  AI Act, Adding AGI to "High Risk" Category

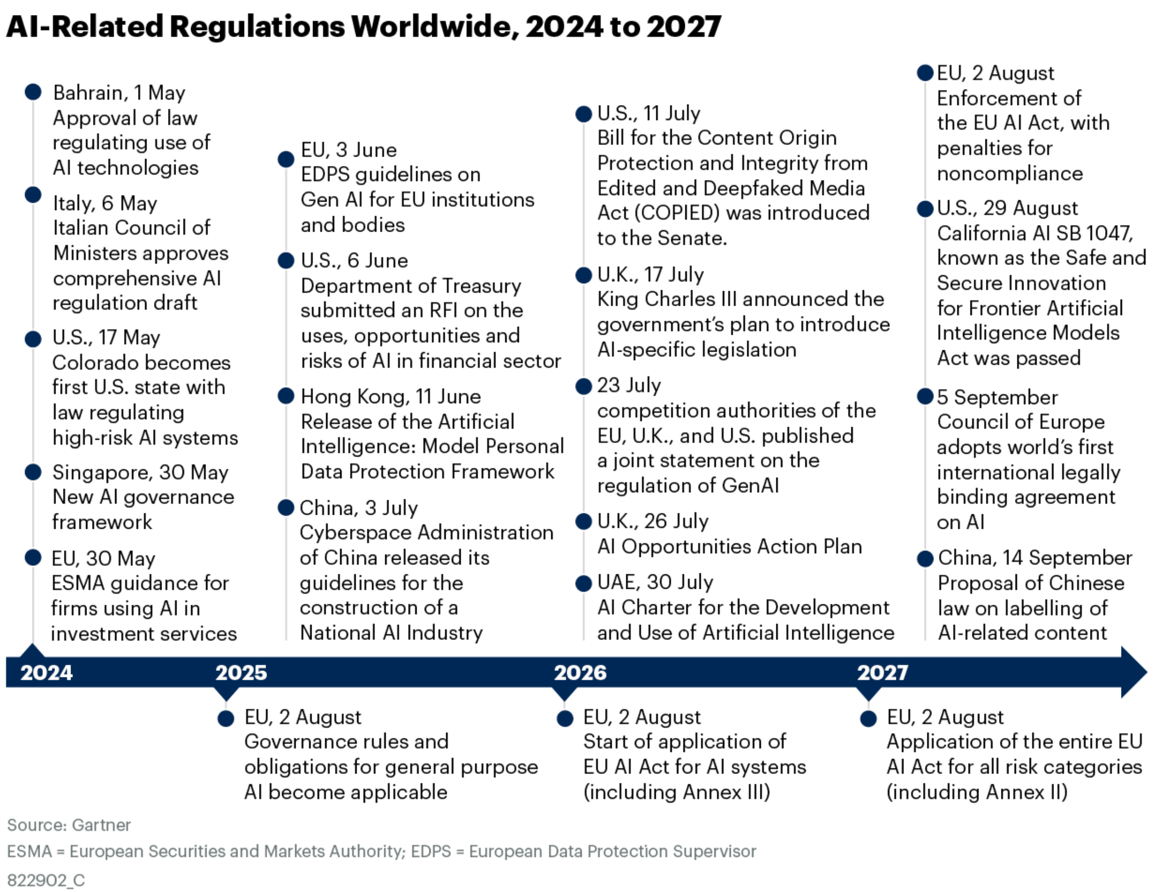
and Fairness

- Bangladesh, April
  New National AI Policy published

Source: Gartner

AIDA = Artificial Intelligence and Data Act; MeitY = Ministry of Electronics and Information Technology; LLMs = large language models; AGI = artificial general intelligence

822902_C



AI-Related Regulations Worldwide, 2024 to 2027

- Bahrain, 1 May
  Approval of law regulating use of AI technologies
- Italy, 6 May
  Italian Council of Ministers approves comprehensive AI regulation draft
- U.S., 17 May
  Colorado becomes first U.S. state with law regulating high-risk AI systems
- Singapore, 30 May
  New AI governance framework
- EU, 30 May
  ESMA guidance for firms using AI in investment services
- EU, 3 June
  EDPS guidelines on Gen AI for EU institutions and bodies
- U.S., 6 June
  Department of Treasury submitted an RFI on the uses, opportunities and risks of AI in financial sector
- Hong Kong, 11 June
  Release of the Artificial Intelligence: Model Personal Data Protection Framework
- China, 3 July
  Cyberspace Administration of China released its guidelines for the construction of a National AI Industry
- U.S., 11 July
  Bill for the Content Origin Protection and Integrity from Edited and Deepfaked Media Act (COPIED) was introduced to the Senate.
- U.K., 17 July
  King Charles III announced the government's plan to introduce AI-specific legislation
- 23 July
  competition authorities of the EU, U.K., and U.S. published a joint statement on the regulation of GenAI
- U.K., 26 July
  AI Opportunities Action Plan
- UAE, 30 July
  AI Charter for the Development and Use of Artificial Intelligence
- EU, 2 August
  Enforcement of the EU AI Act, with penalties for noncompliance
- U.S., 29 August
  California AI SB 1047, known as the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act was passed
- 5 September
  Council of Europe adopts world's first international legally binding agreement on AI
- China, 14 September
  Proposal of Chinese law on labelling of AI-related content

2024 2025 2026 2027

- EU, 2 August
  Governance rules and obligations for general purpose AI become applicable
- EU, 2 August
  Start of application of EU AI Act for AI systems (including Annex III)
- EU, 2 August
  Application of the entire EU AI Act for all risk categories (including Annex II)

Source: Gartner

ESMA = European Securities and Markets Authority; EDPS = European Data Protection Supervisor

822902_C

Gartner: "Geopolitics Is Shaping Generative AI (and Vice Versa). 13 December 2024

Zscaler **does NOT use customer data** to train global AI models.

2025 Zscaler, Inc. All rights reserved

Best Practices for Evaluating AI - powered Product Risk

Keep things in context:

How much PII is collected and exploited by Google with every search by your workers?

How much more confidential data is exposed with every ChatGPT?

When it comes to AI- powered security services:

1. **Protect your data** . Any time your data is used for AI model training, there is a risk that other customers will see part of your confidential data. Transforming your data to de- identify or otherwise anonymize your data is usually the control you look for to mitigate this risk.
2. **Don't get hung up on AI governance frameworks made for consumer AI** . Most enterprise security powered by AI does not collect PII or personal data. And most of them take anonymized data and aggregate or share the insights. Nowhere near the risk of doing this with consumer AI which works with PII.
3. **Generative AI models using LLMs are more risky** . In general, any data processed by an LLM is incorporated and "learned" by the LLM, making it potentially available in responses to other requests. Chatbots are an easy example of this.

FORRESTER®

According to Forrester research, Zero Trust AI, on average, delivers the following benefits:

Does a Zero Trust AI approach really make a difference ?

65% reduced risk
of exposure to breach costs

75% efficiency increase
in IT and security operational efficiency

6.5 hours saved
per end-user per year

Forrester: The Total Economic Impact of Zscaler Internet Access. May 2025

Take Aways

1

AI can be good, but taking some precautions is prudent.

2

When analyzing AI risk to your company, **start by focusing on how to protect your data**. What data is being used and how personal or confidential is that data?

3

To date, **much of the AI risk comes in how data models are trained**. If confidential and personal data is used in modeling, spend time focusing on how your data is protected.

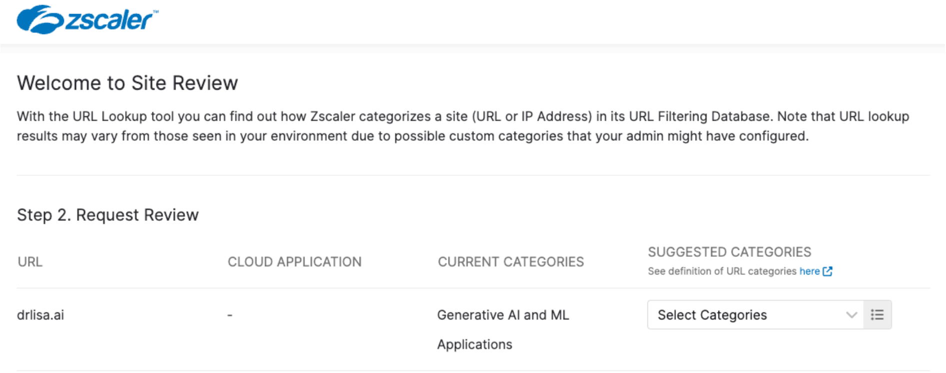
AI in Foundational Zscaler Platforms

Automated Domain Categorization and Assessment

ZIA – automated categorization and classification

AI automates the process of keeping up the changing Internet landscape. Policies are by category and risk score, so they do not need change as new domains come and old domains go.

No configuration necessary.



Welcome to Site Review

With the URL Lookup tool you can find out how Zscaler categorizes a site (URL or IP Address) in its URL Filtering Database. Note that URL lookup results may vary from those seen in your environment due to possible custom categories that your admin might have configured.

Step 2. Request Review

URL	CLOUD APPLICATION	CURRENT CATEGORIES	SUGGESTED CATEGORIES See definition of URL categories here
drlisa.ai	-	Generative AI and ML Applications	Select Categories

Site Review

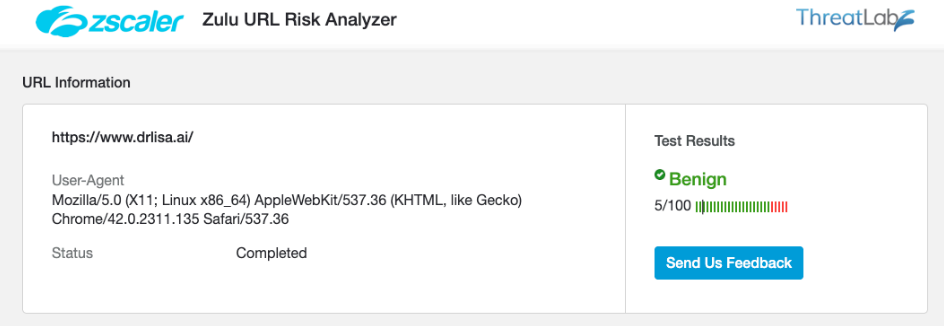
sitereview.zscaler.com

Categorization

Zulu Risk Analyzer

zulu.zscaler.com

Risk assessment



URL Information

https://www.drlisa.ai/

User-Agent
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36

Status Completed

Test Results

Benign

5/100

1.1 Billion

total websites

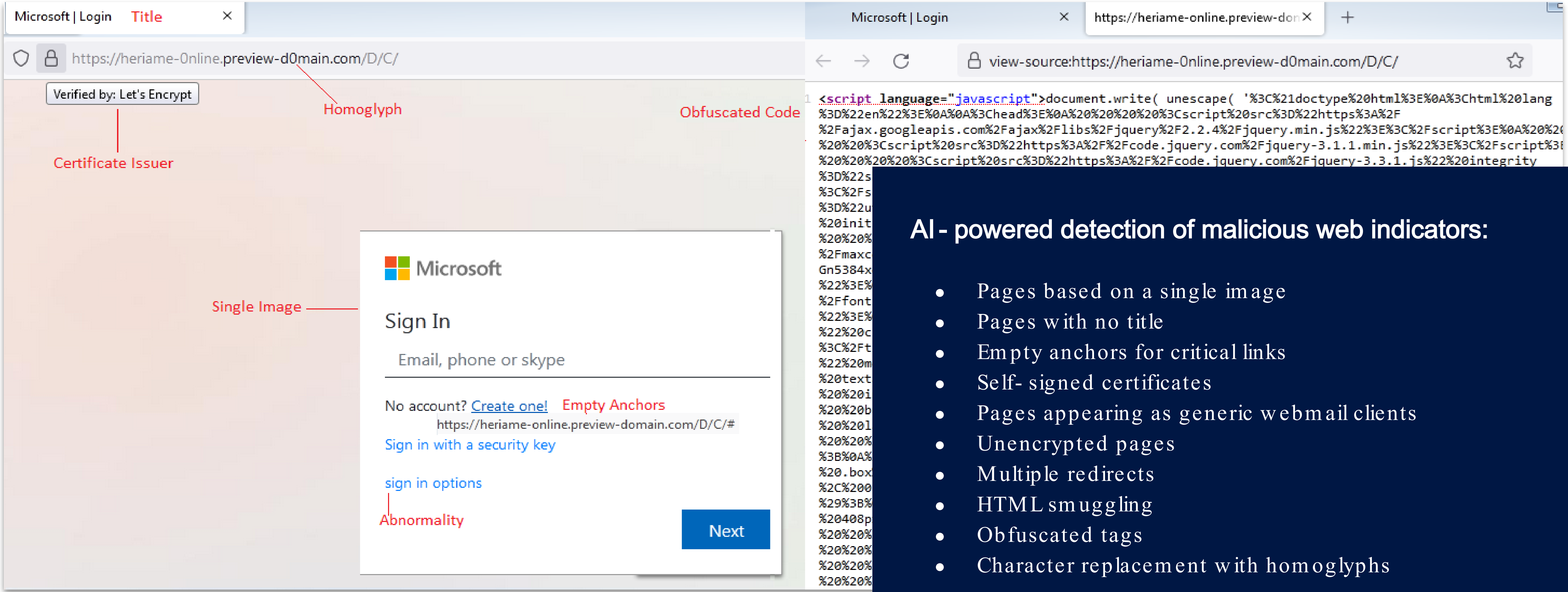
175,000

new websites everyday

145,000

websites retired everyday

AI - powered Page Inspection for Phishing



Microsoft | Login
Title
https://heriame-0nline.preview-d0main.com/D/C/
Verified by: Let's Encrypt
Homoglyph
Certificate Issuer
Obfuscated Code
Single Image
Microsoft
Sign In
Email, phone or skype
No account? Create one!
Empty Anchors
https://heriame-online.preview-domain.com/D/C/#
Sign in with a security key
sign in options
Abnormality
Next
Microsoft | Login
https://heriame-online.preview-dor
view-source:https://heriame-0nline.preview-d0main.com/D/C/

```
<script language="javascript">document.write( unescape( '%3C%21doctype%20html%3E%0A%3Chtml%20lang
%3D%22en%22%3E%0A%0A%3Chead%3E%0A%20%20%20%20%3Cscript%20src%3D%22https%3A%2F
%2Fajax.googleapis.com%2Fajax%2Flibs%2Fjquery%2F2.2.4%2Fjquery.min.js%22%3E%3C%2Fscript%3E%0A%20%2
%20%20%3Cscript%20src%3D%22https%3A%2F%2Fcode.jquery.com%2Fjquery-3.1.1.min.js%22%3E%3C%2Fscript%3
%20%20%20%20%3Cscript%20src%3D%22https%3A%2F%2Fcode.jquery.com%2Fjquery-3.3.1.js%22%20integrity
%3D%22s
%3C%2Fs
%3D%22u
%20init
%20%20%
%2Fmaxc
Gn5384x
%22%3E%
%2Ffont
%22%3E%
%22%20c
%3C%2Ft
%22%20m
%20text
%20%20i
%20%20b
%20%20l
%20%20%
%3B%0A%
%20.box
%2C%200
%29%3B%
%20408p
%20%20%
%20%20%
%20%20%
%20%20%
```

AI - powered detection of malicious web indicators:

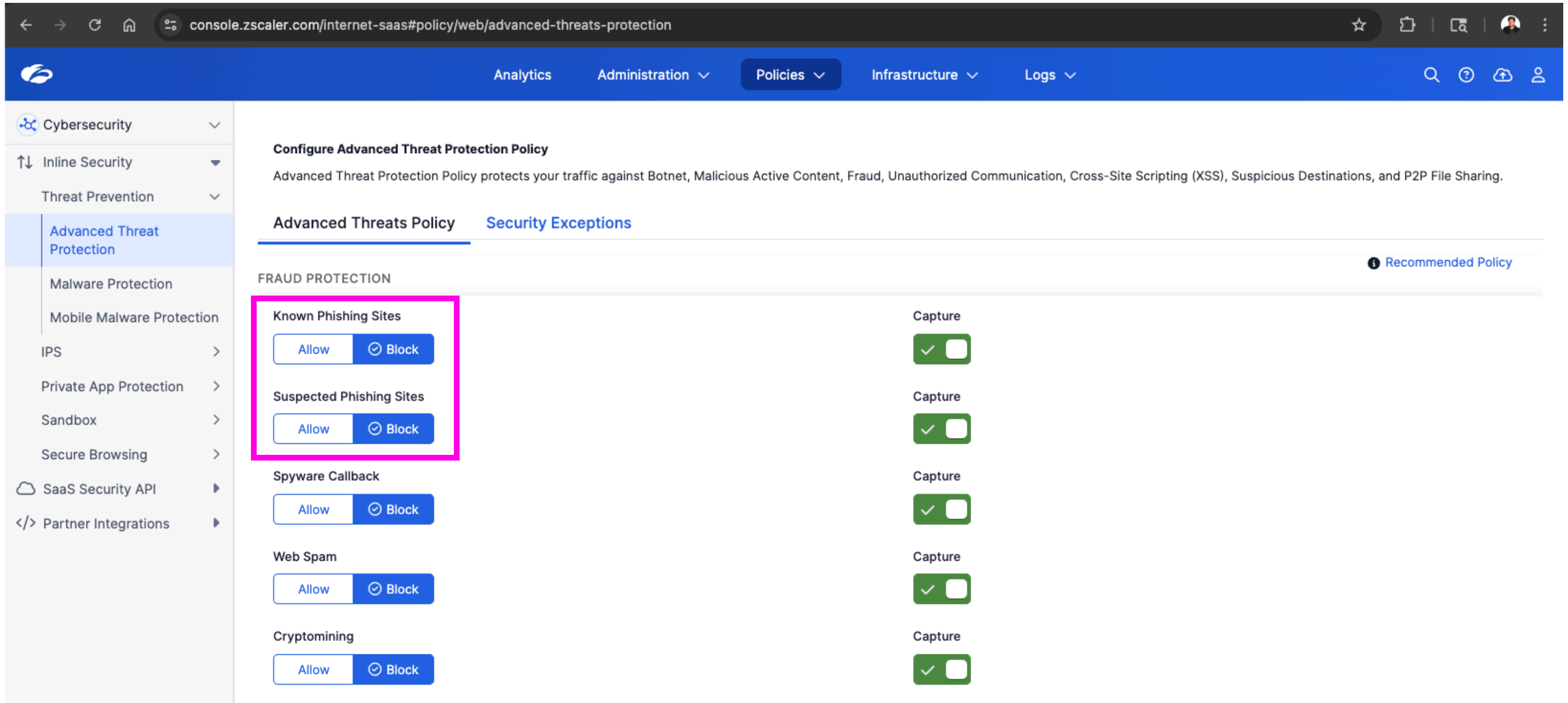
- Pages based on a single image
- Pages with no title
- Empty anchors for critical links
- Self- signed certificates
- Pages appearing as generic webmail clients
- Unencrypted pages
- Multiple redirects
- HTML smuggling
- Obfuscated tags
- Character replacement with homoglyphs

Advanced Protection from Phishing

ZIA – PhishCatch

Not only signatures or a TI feed, but an AI-powered process inspects each page, looking for malicious web indicators, just like a human. It compares images and sign-in pages for top-phished domains to authentic objects. It checks for homoglyphs and obfuscated code.

Make sure you have enabled both phishing controls in Advanced Threat Policy.



Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.

FRAUD PROTECTION

Known Phishing Sites: Allow [✓ Block]	Capture ✓
Suspected Phishing Sites: Allow [✓ Block]	Capture ✓
Spyware Callback: Allow [✓ Block]	Capture ✓
Web Spam: Allow [✓ Block]	Capture ✓
Cryptomining: Allow [✓ Block]	Capture ✓

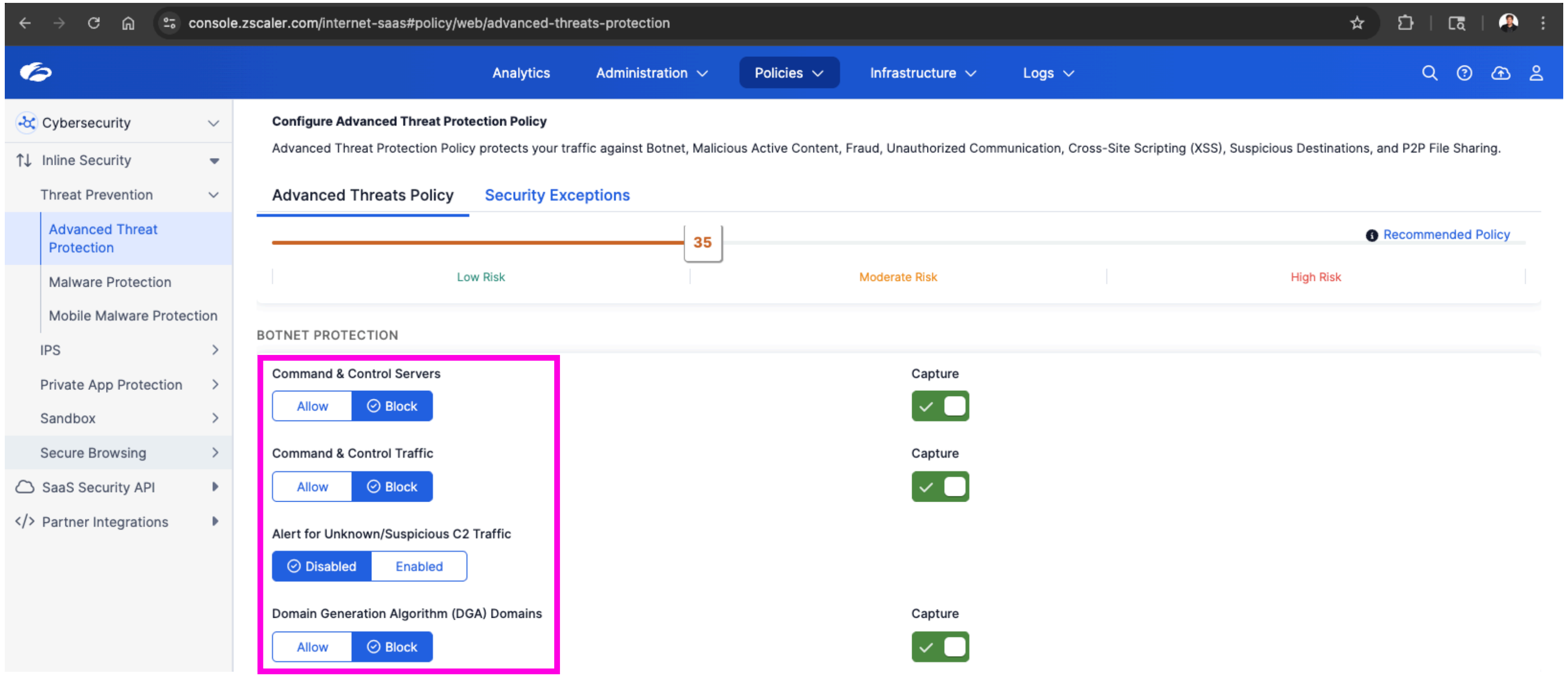
Policies / Cybersecurity / Inline Security / Threat Prevention / Advanced Threat Prevention

Advanced Protection Against Command & Control Comms

ZIA – Advanced Botnet Security

Callback traffic is intended to elude security controls. A simple list of known C2 sites is no longer sufficient. Zscaler uses AI to monitor traffic behavior, looking for anomalous flows with malicious indicators. AI is needed to correlate anomalies with weak indicators. Domain Generation Algorithms can be used for evasion. The algorithms let malware know how to reach their constantly moving Command server at any given time. AI helps decipher to algorithm and pinpoint those malicious communications amongst the noise of other traffic.

Make sure you have enabled all the Botnet controls in Advanced Threat Policy.



Configure Advanced Threat Protection Policy

Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing.

BOTNET PROTECTION

Command & Control Servers: Allow [✓ Block] — Capture ✓

Command & Control Traffic: Allow [✓ Block] — Capture ✓

Alert for Unknown/Suspicious C2 Traffic: [✓ Disabled] Enabled

Domain Generation Algorithm (DGA) Domains: Allow [✓ Block] — Capture ✓

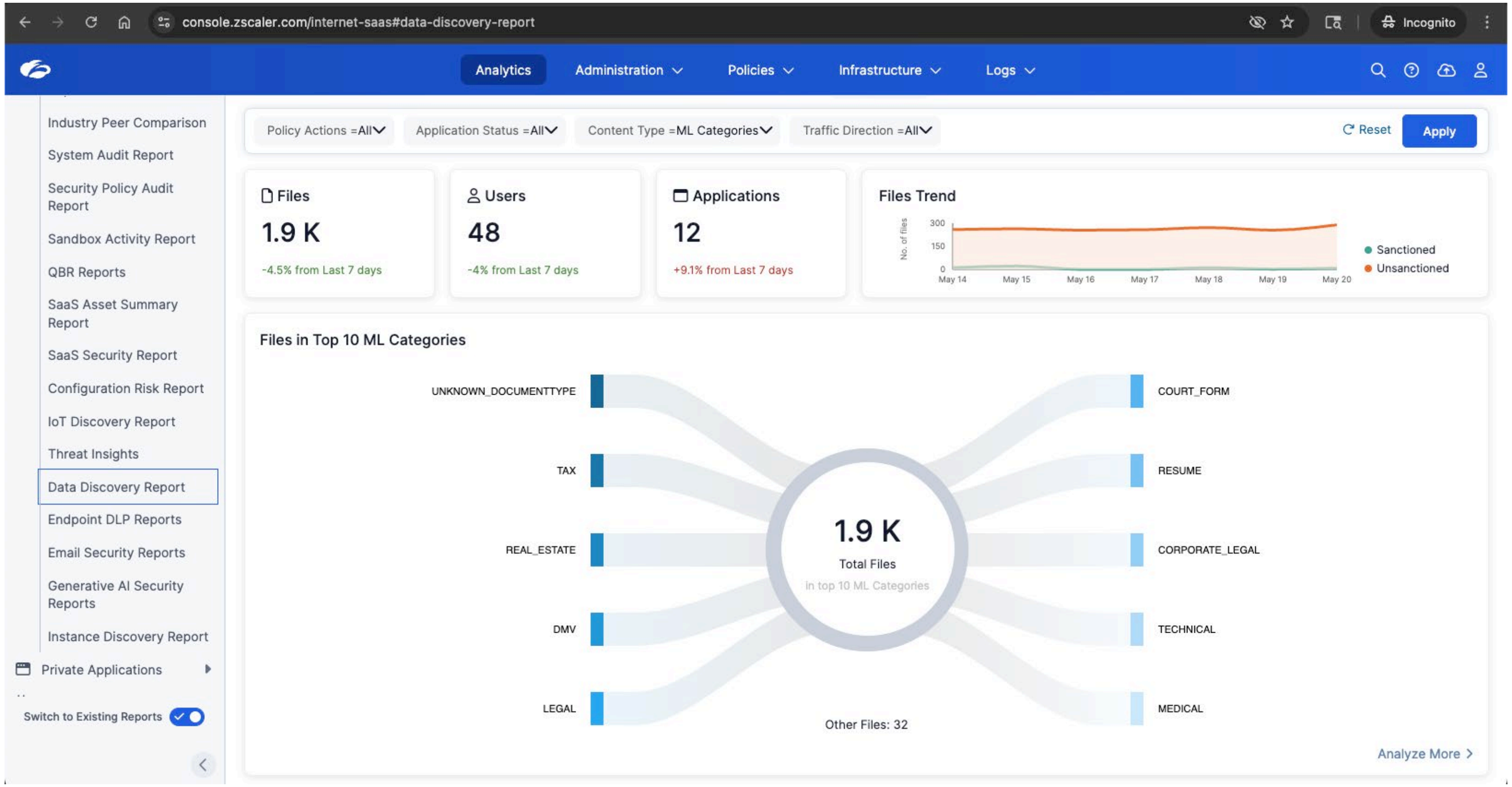
Policies / Cybersecurity / Inline Security / Threat Prevention / Advanced Threat Prevention

AI - Powered Data Discovery and Classification

ZIA – Automatic Discovery & Classification

ML Categories grew from 15 to 200 this past year, but here are showing Top 10. Out-of-the-box, as Data Protection processes scan files, an AI-powered process maps files to these ML categories. No dictionaries or engines need to be configured for this automatic discovery and classification. Click Analyze More to see which applications are transporting these files to which users.

No configuration necessary.



console.zscaler.com/internet-saas#data-discovery-report

Policy Actions =All · Application Status =All · Content Type =ML Categories · Traffic Direction =All

Analytics / Switch to Existing Reports / Analytics / Data Discovery Report

Take Aways

1 Advanced **AI - powered capabilities are available to all Zscaler customers** , helping to reduce operational effort and improve security.

2 Many of these features require no configuration or are enabled by default but **check your configuration to make sure you are taking advantage** of these capabilities.

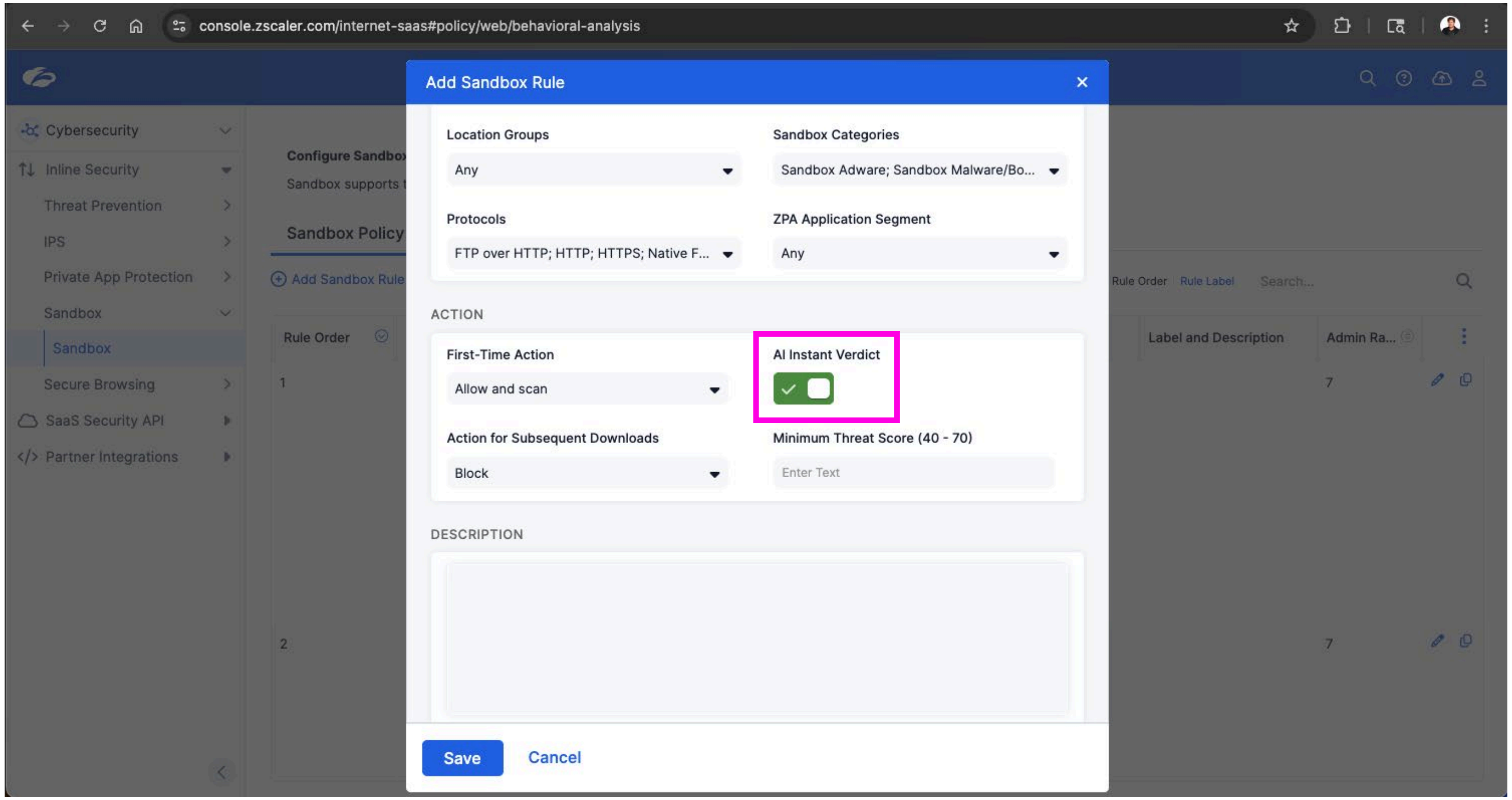
AI in Advanced Zscaler Platforms

Instant Sandbox Results – Great User Experience

ZIA – AI Instant Verdict

Sandbox analysis is great, but it may take a couple of minutes and that wait is not welcome to most users. AI Instant Verdict can predict some malicious files before going through full dynamic analysis. Machine Learning looks for patterns in static file characteristics common with previously convicted malicious files. When files match the malicious pattern with high confidence, they are blocked immediately – no waiting.

AI Instant Verdict controls are found when you add sandbox rules. Flip the switch and modify the risk threshold if desired. Sandbox Advanced license is needed.



console.zscaler.com/internet-saas#policy/web/behavioral-analysis

Add Sandbox Rule

Location Groups: Any

Sandbox Categories: Sandbox Adware; Sandbox Malware/Bo...

Protocols: FTP over HTTP; HTTP; HTTPS; Native F...

ZPA Application Segment: Any

ACTION

First-Time Action: Allow and scan

AI Instant Verdict: ✓

Action for Subsequent Downloads: Block

Minimum Threat Score (40 - 70): Enter Text

DESCRIPTION

Save Cancel

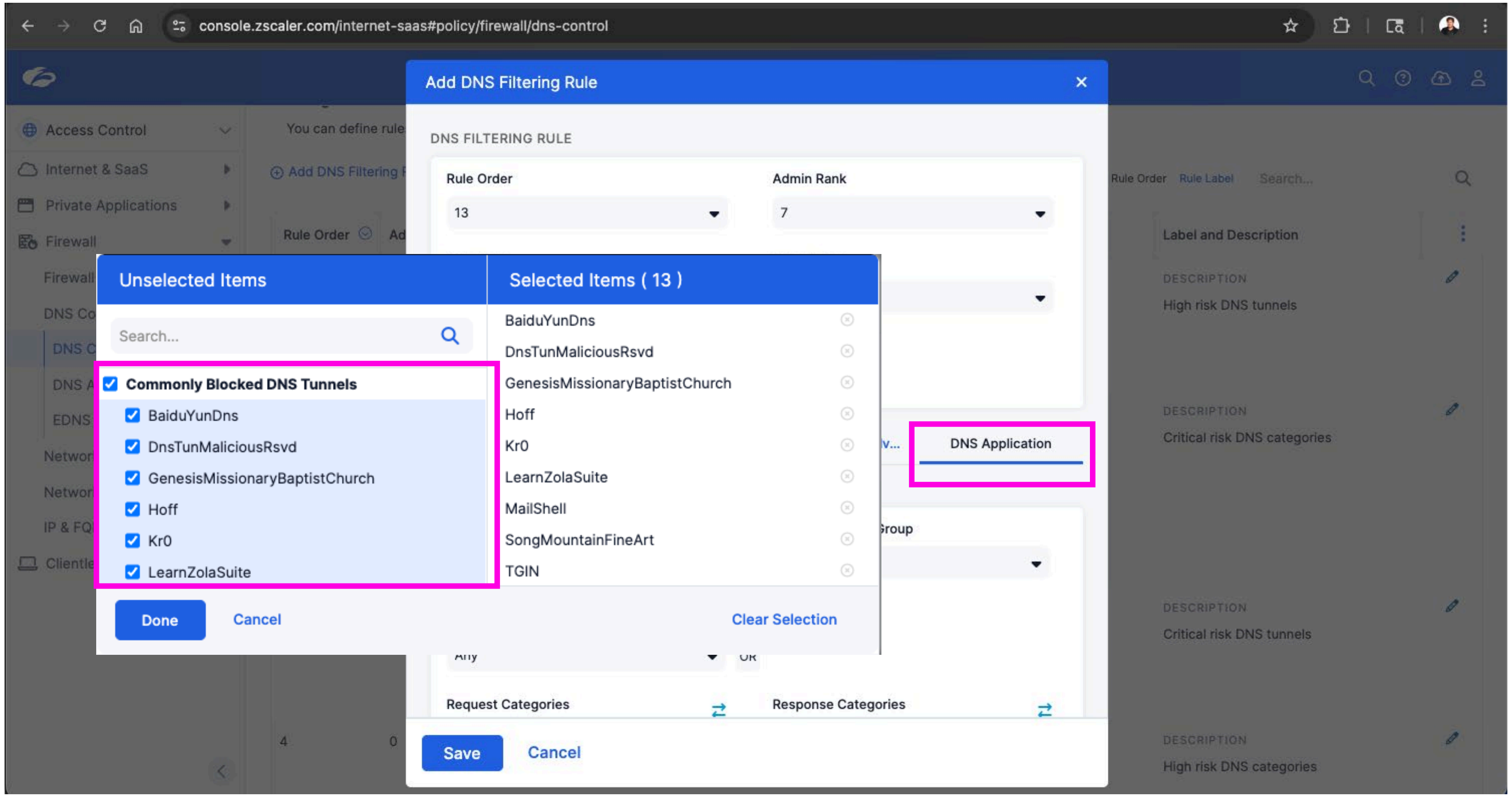
Policies / Cybersecurity / Inline Security / Sandbox / Advanced Policy Settings / Add Sandbox Rule

Prevent Malicious DNS Tunneling

ZIA – DNS Tunneling

DNS traffic is assumed to be good in most networks and typically bypassed at the firewall. Tunnels can be set up in DNS to transfer data, such as is often used for security software updates. But it is not uncommon for bad actors to use DNS tunnel for C2 communications. Zscaler can monitor DNS for tunneling and use AI to determine whether the tunnel is malicious.

DNS tunneling settings are found where you add DNS filtering rules. Select criteria in DNS Tunnels & Network Apps. DNS Advanced capabilities come with the Firewall Advanced license.



console.zscaler.com/internet-saas#policy/firewall/dns-control

Add DNS Filtering Rule

DNS FILTERING RULE

Rule Order: 13

Admin Rank: 7

Unselected Items

Search...

☑ Commonly Blocked DNS Tunnels
- ☑ BaiduYunDns
- ☑ DnsTunMaliciousRsvd
- ☑ GenesisMissionaryBaptistChurch
- ☑ Hoff
- ☑ Kr0
- ☑ LearnZolaSuite

Selected Items (13)
- BaiduYunDns
- DnsTunMaliciousRsvd
- GenesisMissionaryBaptistChurch
- Hoff
- Kr0
- LearnZolaSuite
- MailShell
- SongMountainFineArt
- TGIN

Done Cancel Clear Selection

Request Categories

Response Categories

Save Cancel

Label and Description
DESCRIPTION High risk DNS tunnels
DESCRIPTION Critical risk DNS categories
DESCRIPTION Critical risk DNS tunnels
DESCRIPTION High risk DNS categories

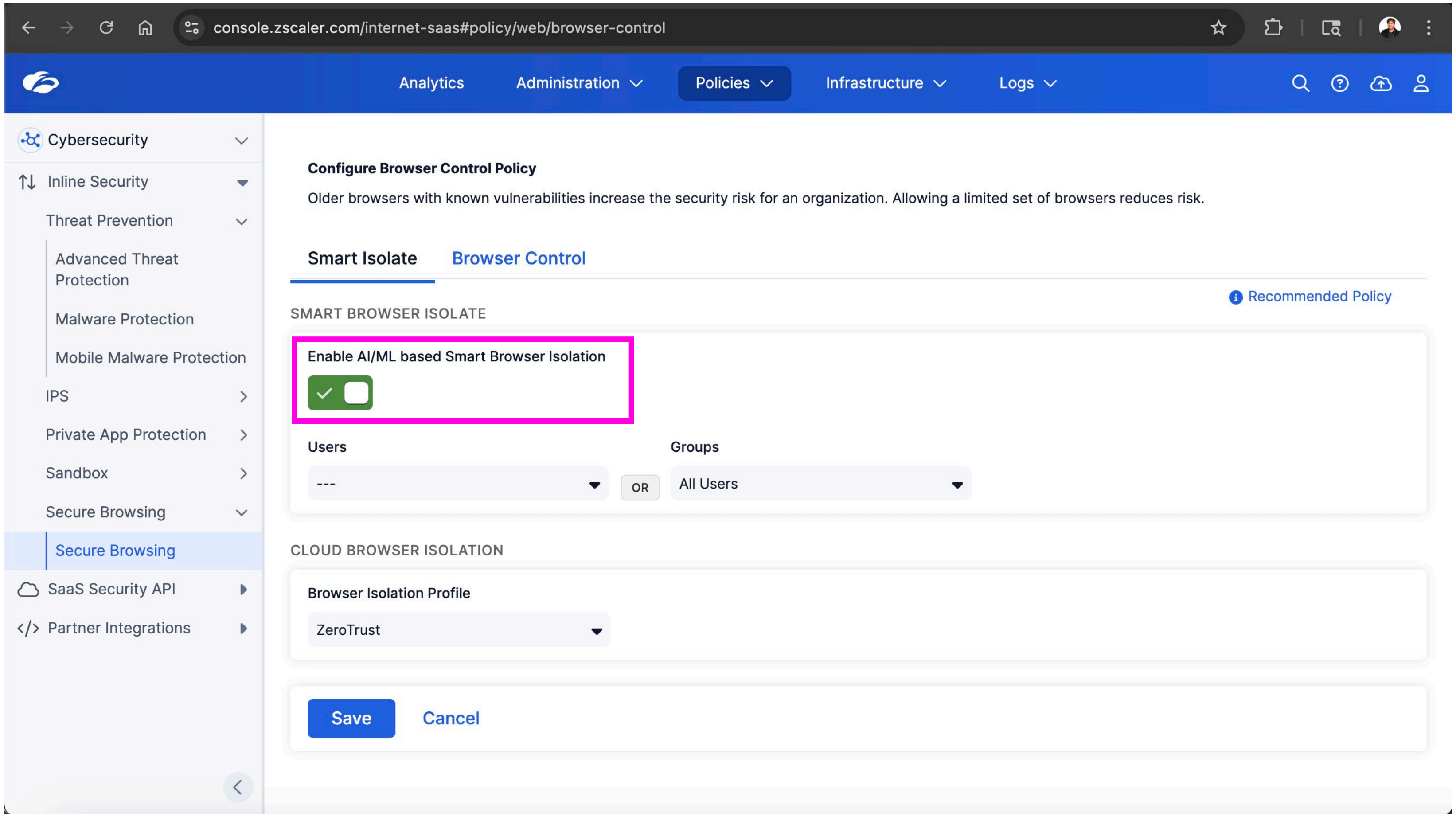
Policies / Access Control / Firewall / DNS Control / Add DNS Filtering Rule / DNS Application

Browser Isolation Only When Risk is High

ZIA – Smart Browser Isolation

Browser isolation is great, but it may seem that you have to deliberately configure which categories or domains will be rendered in isolation. Not so. Zscaler can be configured so only high risk domains are rendered in isolation. This is important as domain risk may chance over time, as well as the constantly changing catalog of domains that come and go.

Make sure that you have Browser Isolation profiles configured, then simply enable Smart Isolate by user or group. Cyber Browser Isolation Advanced license is needed.



Configure Browser Control Policy

Older browsers with known vulnerabilities increase the security risk for an organization. Allowing a limited set of browsers reduces risk.

Smart Isolate | Browser Control

Recommended Policy

SMART BROWSER ISOLATE

Enable AI/ML based Smart Browser Isolation: ✓

Users: ---

OR

Groups: All Users

CLOUD BROWSER ISOLATION

Browser Isolation Profile: ZeroTrust

Save | Cancel

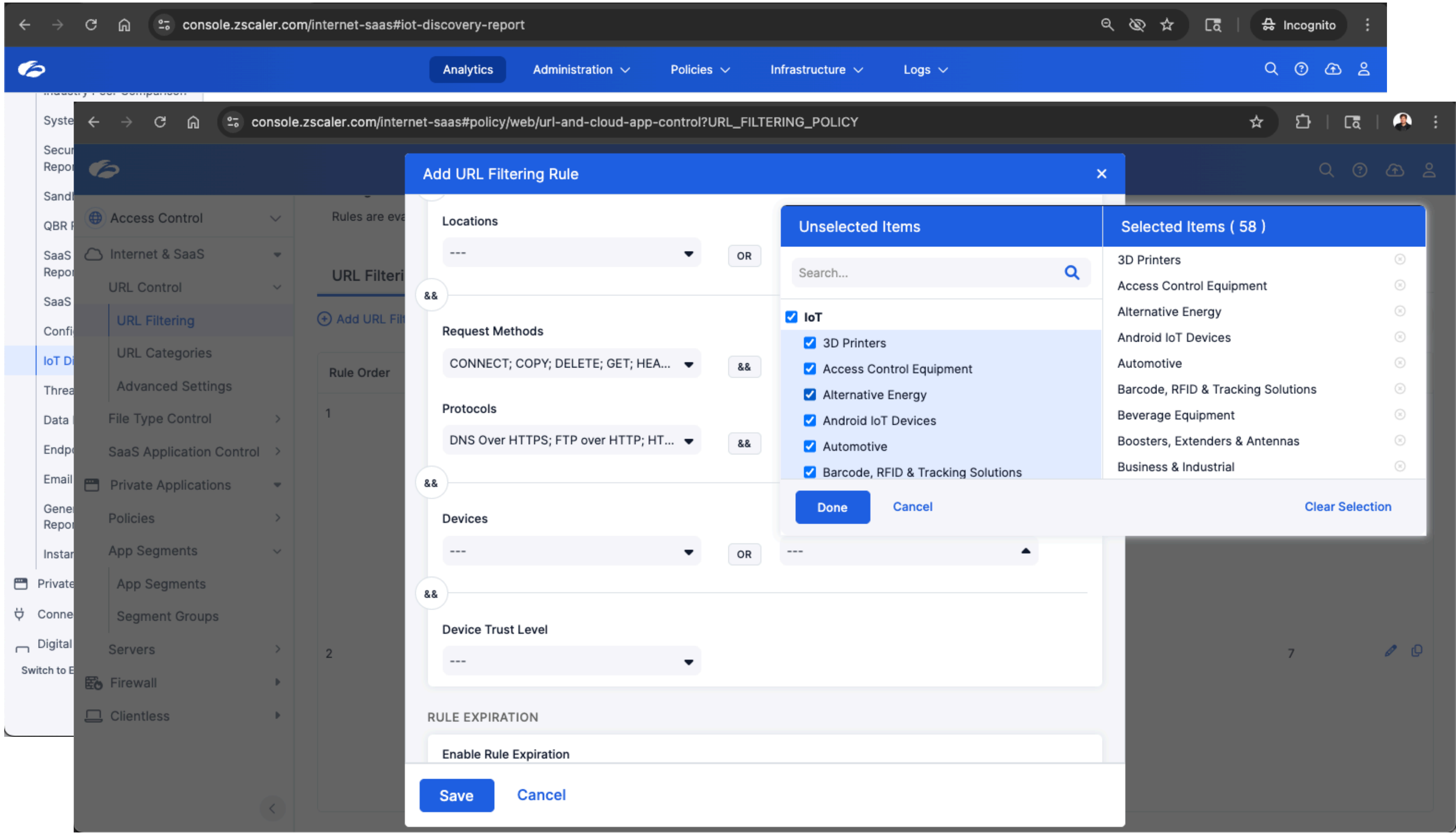
Policies / Cybersecurity / Inline Security / Secure Browsing

IoT Device Fingerprinting

ZIA – IoT Device Groups & Report

ZIA uses AI to discover IoT devices and organize them into their functional groups. You can now set URL Filtering policies with IoT devices as a Device Group setting, giving you granular control over groups of IoT in your network.

Enable IoT Discovery and Policy Control (2 buttons) in Location definitions (Infrastructure / Locations / Legacy Locations). As discovery automatically occurs, the IoT Discovery Report and IoT items under Device Groups will appear.



console.zscaler.com/internet-saas#iot-discovery-report

console.zscaler.com/internet-saas#policy/web/url-and-cloud-app-control?URL_FILTERING_POLICY

Add URL Filtering Rule

Locations: ---

Request Methods: CONNECT; COPY; DELETE; GET; HEA...

Protocols: DNS Over HTTPS; FTP over HTTP; HT...

Devices: ---

Device Trust Level: ---

RULE EXPIRATION

Enable Rule Expiration

Unselected Items

☑ IoT
- ☑ 3D Printers
- ☑ Access Control Equipment
- ☑ Alternative Energy
- ☑ Android IoT Devices
- ☑ Automotive
- ☑ Barcode, RFID & Tracking Solutions

Selected Items (58)
- 3D Printers
- Access Control Equipment
- Alternative Energy
- Android IoT Devices
- Automotive
- Barcode, RFID & Tracking Solutions
- Beverage Equipment
- Boosters, Extenders & Antennas
- Business & Industrial

Analytics / Switch to Existing Reports / Internet & SaaS / Analytics / IoT Discovery Report

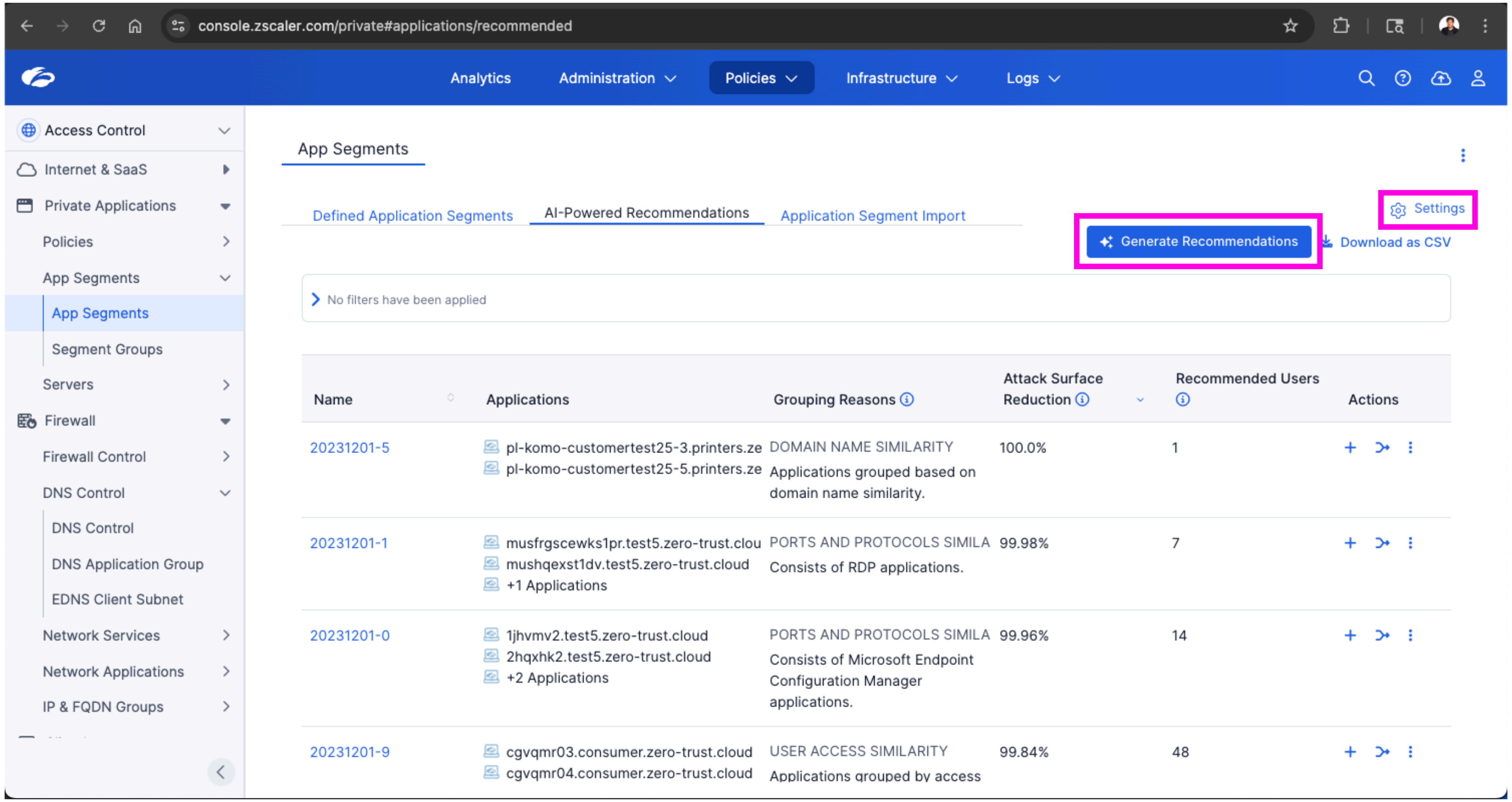
Policies / Access Control / Internet & SaaS / URL Filtering / Add Filtering Rule / Device Group

Recommended App Segment Definitions and Policies

ZPA – Recommendations for App Segments

Defining an App Segment is easy, but many organizations have 1000s or 10000s private services or resources. AI-Powered Recommendations learns from your traffic and recommends App Segment definitions as well as user access policies. This service also calculates the attack surface reduction with the recommended policy.

AI - Powered Recommendations are found in the tab next to where your defined App Segments are. Click Generate Recommendations to get started. Private Access Segmentation license is needed.



Name	Applications	Grouping Reasons	Attack Surface Reduction	Recommended Users	Actions
20231201-5	pl-komo-customertest25-3.printers.ze pl-komo-customertest25-5.printers.ze	DOMAIN NAME SIMILARITY Applications grouped based on domain name similarity.	100.0%	1	+ ⋮
20231201-1	musfrgscewks1pr.test5.zero-trust.clou mushqexst1dv.test5.zero-trust.cloud +1 Applications	PORTS AND PROTOCOLS SIMILA Consists of RDP applications.	99.98%	7	+ ⋮
20231201-0	1jhvmv2.test5.zero-trust.cloud 2hqxhk2.test5.zero-trust.cloud +2 Applications	PORTS AND PROTOCOLS SIMILA Consists of Microsoft Endpoint Configuration Manager applications.	99.96%	14	+ ⋮
20231201-9	cgvqmr03.consumer.zero-trust.cloud cgvqmr04.consumer.zero-trust.cloud	USER ACCESS SIMILARITY Applications grouped by access	99.84%	48	+ ⋮

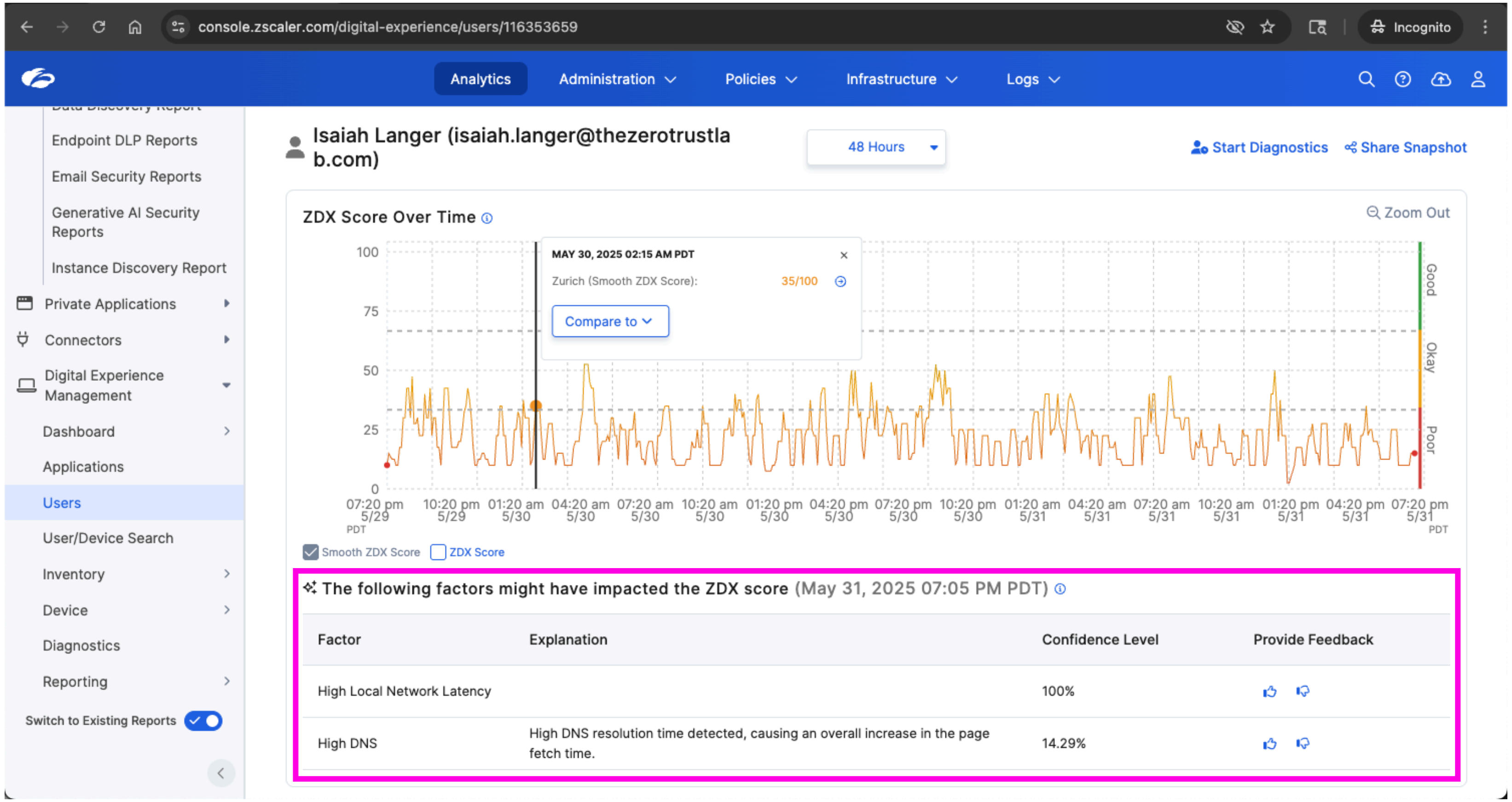
Policies / Access Control / Private Applications / App Segments / AI-Powered Recommendations

AI- Assisted Performance Troubleshooting

ZDX – Root Cause Analysis

Once your probes are configured, ZDX provides volumes of performance data across networks, app services, and the endpoint itself. AI- powered Root Cause Analysis looks across all the data and proposes the most likely causes for poor performance. Plug this into your Helpdesk and quickly identify and triage most end- user performance complaints.

Root cause analysis is automatically calculated for low ZDX scores. Simply navigate through users and apps to your desired ZDX score and the analysis automatically launches. ZDX Advanced Plus license is needed.



Isaiah Langer (isaiah.langer@thezerotrustlab.com)

The following factors might have impacted the ZDX score (May 31, 2025 07:05 PM PDT)

Factor	Explanation	Confidence Level	Provide Feedback
High Local Network Latency		100%	👍 👎
High DNS	High DNS resolution time detected, causing an overall increase in the page fetch time.	14.29%	👍 👎

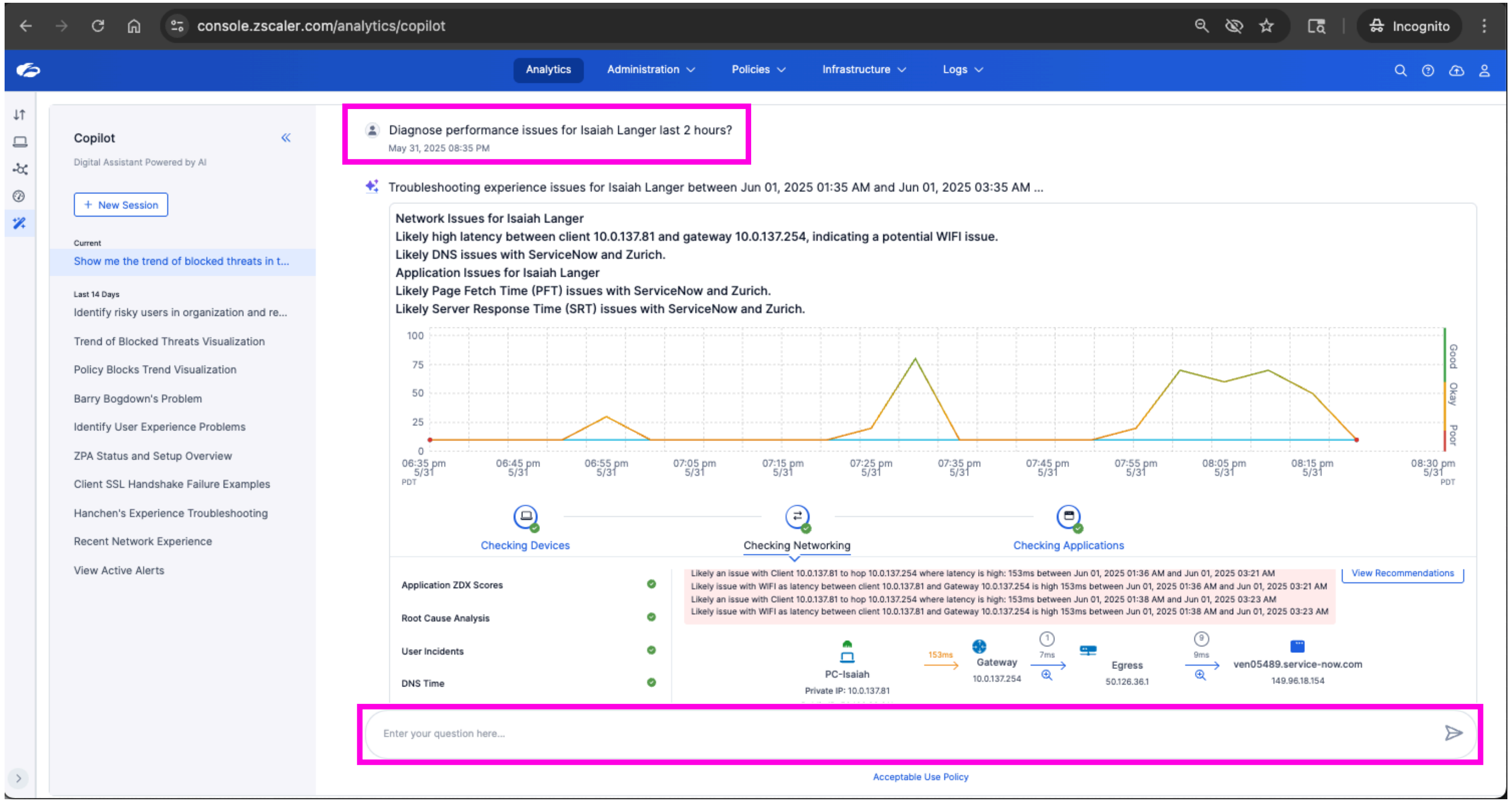
Analytics / Switch to Existing Reports / Digital Experience Management / Users

Copilot for ZDX

ZDX – Copilot

Zscaler Copilot works like you would expect – ask questions in natural language and Zscaler Copilot will interpret and pull information to answer your question. Ask simple questions such as what is a user's ZDX score for the past two hours, or ask complex questions, such as troubleshoot this user's performance and Copilot will interrogate Zscaler, using all Zscaler ZDX capabilities available, to compose a complete response.

Copilot is one of the tabs on Analytics. Just start asking questions, or choose one of the suggested questions to get started. ZDX Advanced Plus license is needed.


console.zscaler.com/analytics/copilot
Incognito
Analytics
Administration
Policies
Infrastructure
Logs
Copilot
Digital Assistant Powered by AI
+ New Session
Current
Show me the trend of blocked threats in t...
Last 14 Days
Identify risky users in organization and re...
Trend of Blocked Threats Visualization
Policy Blocks Trend Visualization
Barry Bogdown's Problem
Identify User Experience Problems
ZPA Status and Setup Overview
Client SSL Handshake Failure Examples
Hanchen's Experience Troubleshooting
Recent Network Experience
View Active Alerts

Diagnose performance issues for Isaiah Langer last 2 hours?
May 31, 2025 08:35 PM

Troubleshooting experience issues for Isaiah Langer between Jun 01, 2025 01:35 AM and Jun 01, 2025 03:35 AM ...

Network Issues for Isaiah Langer
Likely high latency between client 10.0.137.81 and gateway 10.0.137.254, indicating a potential WIFI issue.
Likely DNS issues with ServiceNow and Zurich.
Application Issues for Isaiah Langer
Likely Page Fetch Time (PFT) issues with ServiceNow and Zurich.
Likely Server Response Time (SRT) issues with ServiceNow and Zurich.

Likely an issue with Client 10.0.137.81 to hop 10.0.137.254 where latency is high: 153ms between Jun 01, 2025 01:36 AM and Jun 01, 2025 03:21 AM
Likely issue with WIFI as latency between client 10.0.137.81 and Gateway 10.0.137.254 is high 153ms between Jun 01, 2025 01:36 AM and Jun 01, 2025 03:21 AM
Likely an issue with Client 10.0.137.81 to hop 10.0.137.254 where latency is high: 153ms between Jun 01, 2025 01:38 AM and Jun 01, 2025 03:23 AM
Likely issue with WIFI as latency between client 10.0.137.81 and Gateway 10.0.137.254 is high 153ms between Jun 01, 2025 01:38 AM and Jun 01, 2025 03:23 AM

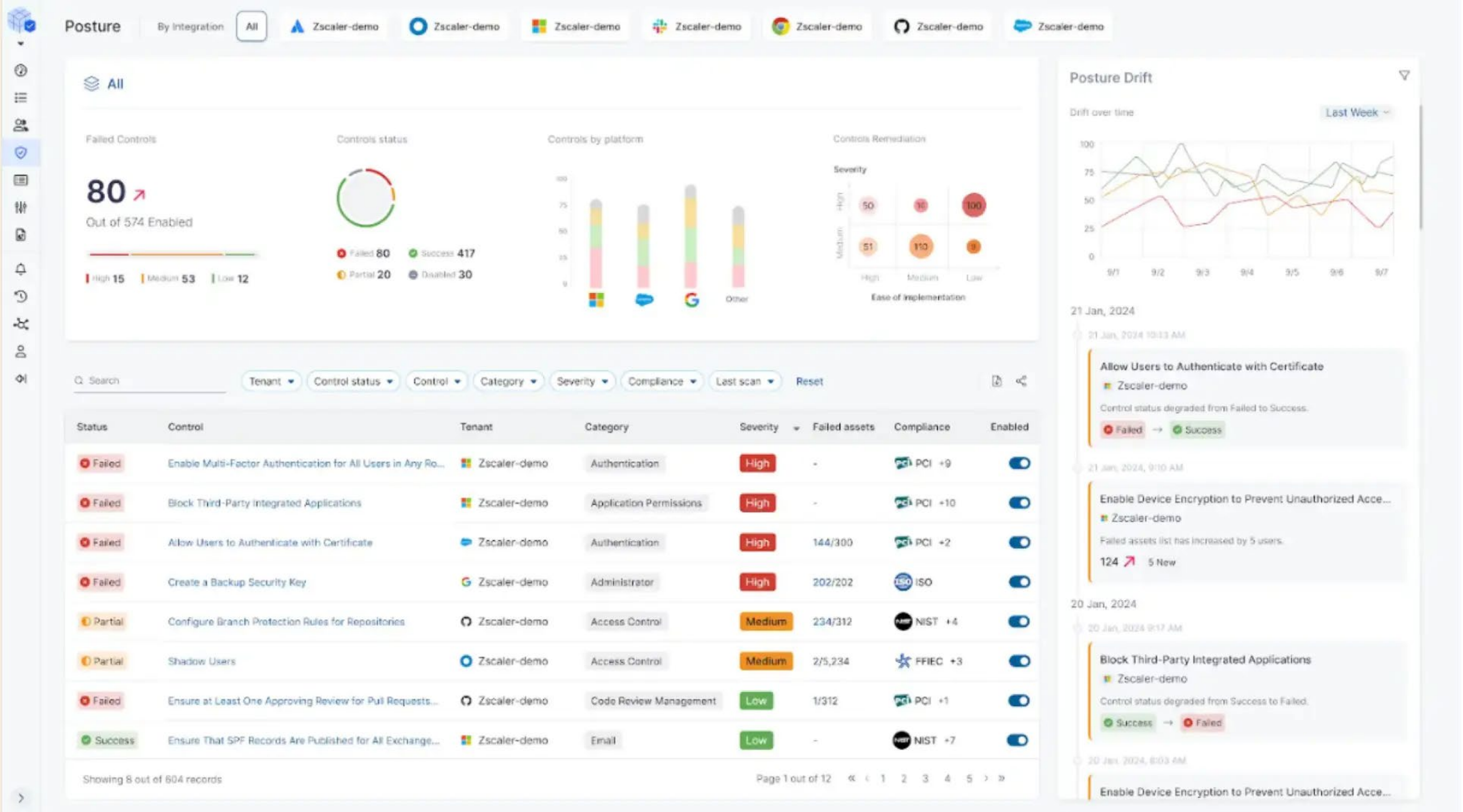
Analytics / Copilot

Keep SaaS Configurations Safe

ZIA – SaaS Posture Management

SaaS Security Posture Management (SSPM) ensures that your SaaS application configurations do not drift. This includes AI analysis of controls to maintain compliance, to keep remediation steps current, and to regularly evaluate CVE risk 3rd- party access. Some of this is visible in the SaaS Security Report, but there is also an Advanced Posture Management console with expert capabilities.

Essentials configuration is available on the SaaS Security Posture Management page, including a link to the expert system console. SaaS Security license is needed.



Status	Control	Tenant	Category	Severity	Failed assets	Compliance	Enabled
Failed	Enable Multi-Factor Authentication for All Users in Any Ro...	Zscaler-demo	Authentication	High	-	PCI +9	●
Failed	Block Third-Party Integrated Applications	Zscaler-demo	Application Permissions	High	-	PCI +10	●
Failed	Allow Users to Authenticate with Certificate	Zscaler-demo	Authentication	High	144/300	PCI +2	●
Failed	Create a Backup Security Key	Zscaler-demo	Administrator	High	202/202	ISO	●
Partial	Configure Branch Protection Rules for Repositories	Zscaler-demo	Access Control	Medium	234/312	NIST +4	●
Partial	Shadow Users	Zscaler-demo	Access Control	Medium	2/5,234	FFIEC +3	●
Failed	Ensure at Least One Approving Review for Pull Requests...	Zscaler-demo	Code Review Management	Low	1/312	PCI +1	●
Success	Ensure That SPF Records Are Published for All Exchange...	Zscaler-demo	Email	Low	-	NIST +7	●

Showing 8 out of 604 records

Page 1 out of 12 « ‹ 1 2 3 4 5 › »

21 Jan, 2024

21 Jan, 2024 10:13 AM

Allow Users to Authenticate with Certificate
Zscaler-demo
Control status degraded from Failed to Success.
Failed → Success

21 Jan, 2024, 9:10 AM

Enable Device Encryption to Prevent Unauthorized Acce...
Zscaler-demo
Failed assets list has increased by 5 users.
124 ↗ 5 New

20 Jan, 2024

20 Jan, 2024 9:17 AM

Block Third-Party Integrated Applications
Zscaler-demo
Control status degraded from Success to Failed.
Success → Failed

20 Jan, 2024, 8:03 AM

Enable Device Encryption to Prevent Unauthorized Acce...

Policies / Data Protection / Policy / SaaS Security / SaaS Security Posture Management

Take Aways

1

Optional licenses often come as bundles and **many customers have access to advanced AI - powered capabilities and may not be aware** they have access. Check today to make sure you are not missing out.

2

If you are interested in an advanced AI- powered capability you are not currently licensed for, **ask you Zscaler sales executive** for a trial of that license.

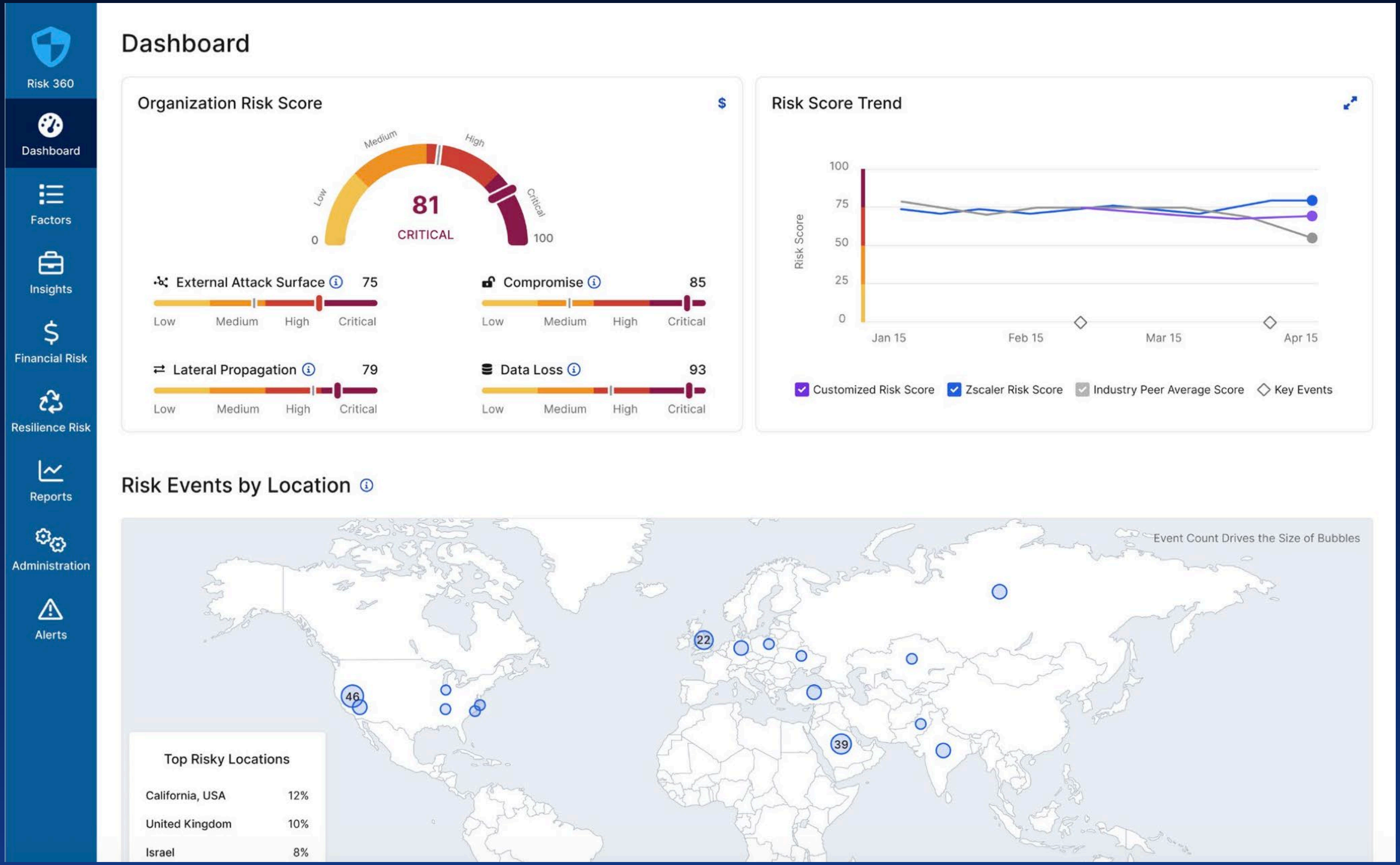
Real world benefits

- **Cloud- native security** replacing VPNs/ firewalls
- **Zero Trust** reduces attack surface
- **80% bandwidth savings** , faster performance
- **Blocks 99.9% threats** (AI/ ML- powered)
- **50% fewer breaches** , 60 % cost reduction (customer- reported)

AI in Extensions from Core Zscaler Platforms

Risk360

Is your organization safe or not? Configurations, external attack surface, compromises, data loss – measure risk over time and compare industry average.



Dashboard

Organization Risk Score

81 CRITICAL

External Attack Surface	75		Compromise	85
Lateral Propagation	79		Data Loss	93

Risk Score Trend

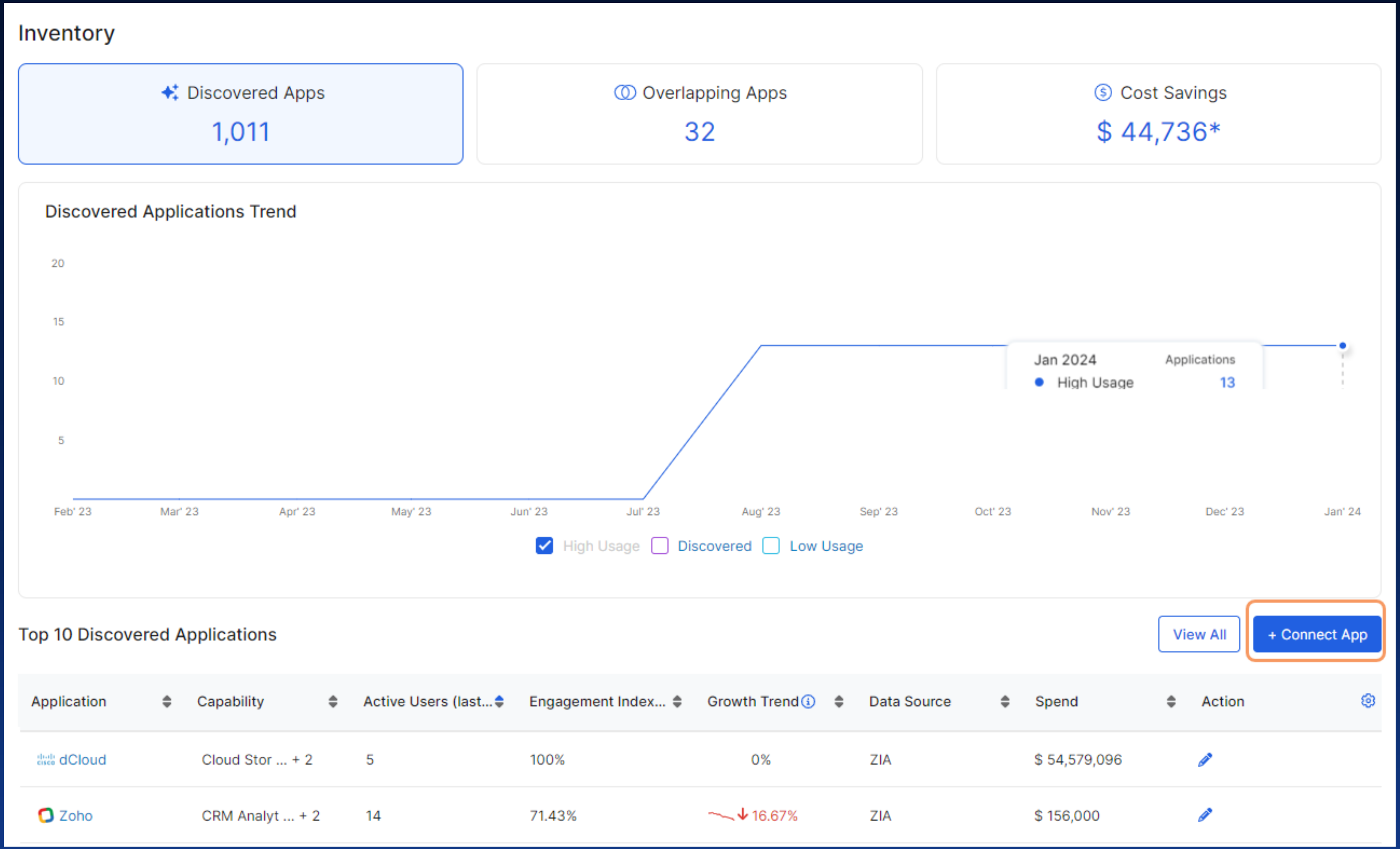
☑ Customized Risk Score ☑ Zscaler Risk Score ☑ Industry Peer Average Score ◇ Key Events

Risk Events by Location

Top Risky Locations

California, USA	12%
United Kingdom	10%
Israel	8%

https://www.zscaler.com/products-and-solutions/zscaler-risk-360



Inventory

Discovered Apps	Overlapping Apps	Cost Savings
1,011	32	$ 44,736*

Discovered Applications Trend

Top 10 Discovered Applications

Application	Capability	Active Users (last...	Engagement Index...	Growth Trend	Data Source	Spend	Action
dCloud	Cloud Stor ... + 2	5	100%	0%	ZIA	$ 54,579,096	✎
Zoho	CRM Analyt ... + 2	14	71.43%	↓16.67%	ZIA	$ 156,000	✎

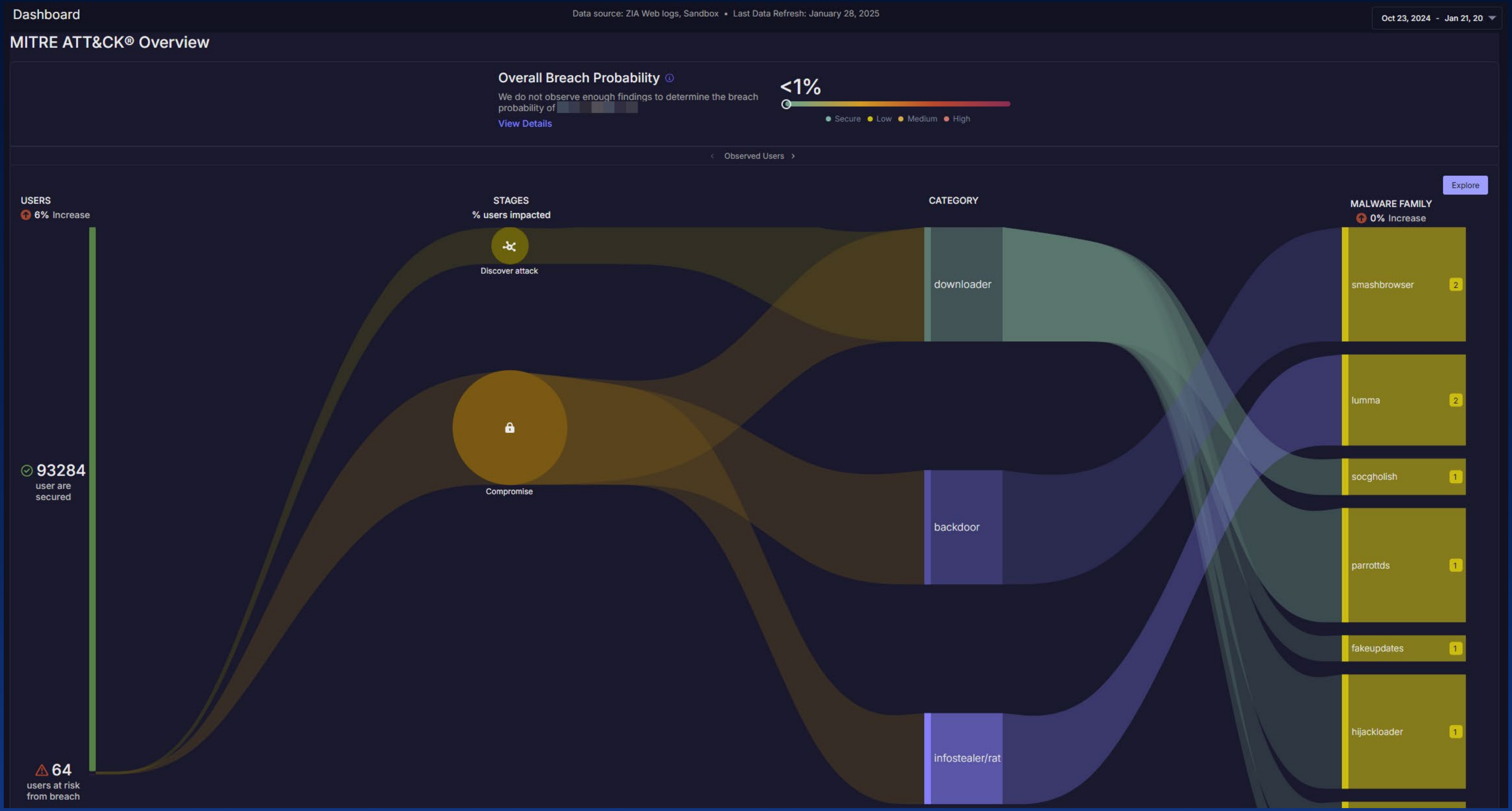
Business Insights

You pay a lot for apps and facilities, but how well are those investments being used? Zscaler can cross reference use of apps and locations by user, showing you how frequently resources are being used. This is especially insightful with shadow IT.

https://www.zscaler.com/products-and-solutions/business-insights

Breach Predictor

So many weak signals but which ones are worth your attention? Cut through the noise of information overflow. Breach Predictor examines weak signals, correlating, organizing, and prioritizing, pointing you to the most valuable use of your time.



Dashboard

Data source: ZIA Web logs, Sandbox • Last Data Refresh: January 28, 2025

Oct 23, 2024 - Jan 21, 20

MITRE ATT&CK® Overview

Overall Breach Probability

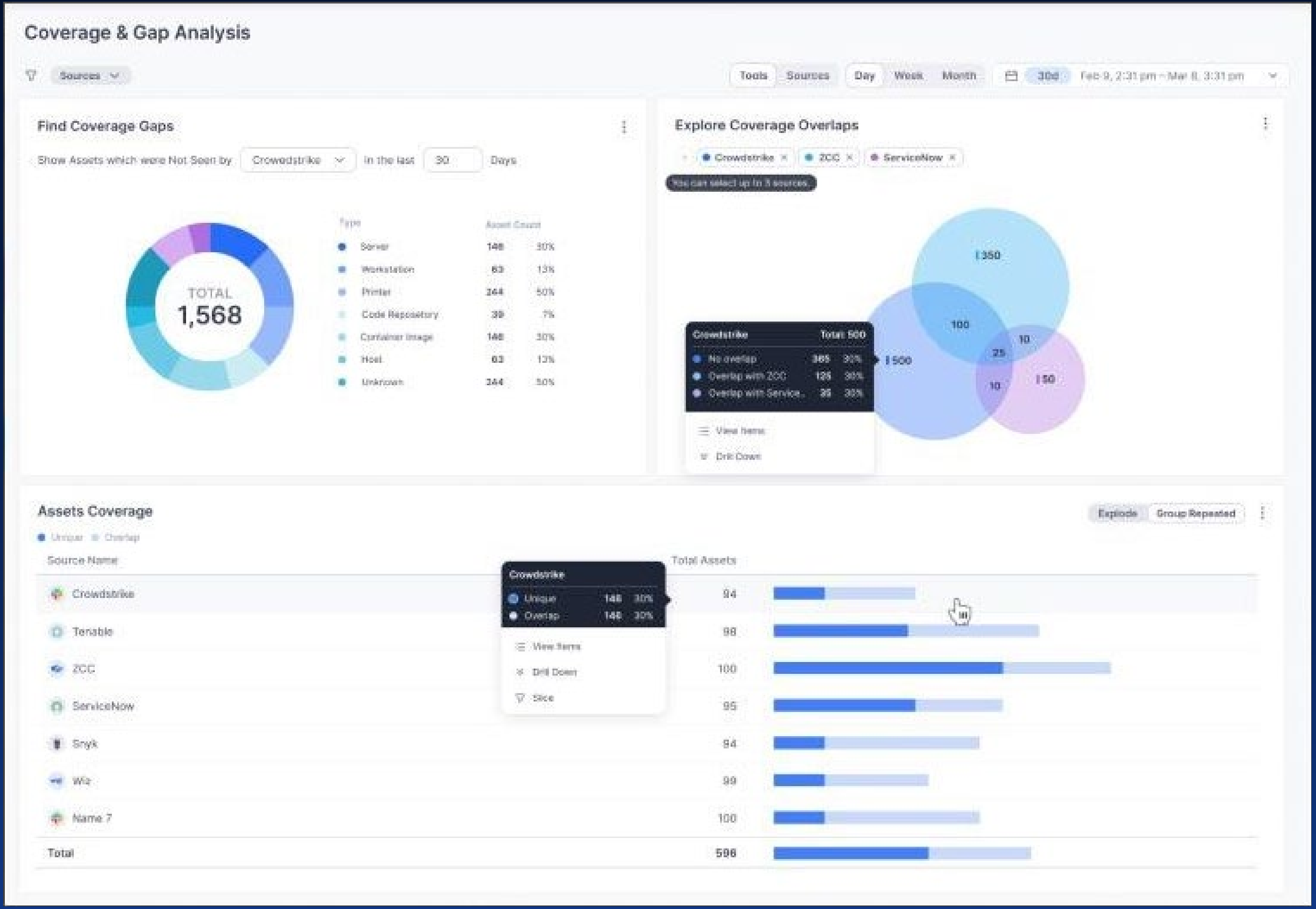
We do not observe enough findings to determine the breach probability of [redacted]

View Details

<1%

https://www.zscaler.com/products-and-solutions/breach-predictor

Asset Exposure Management



Coverage & Gap Analysis

Sources

Tools | Sources | Day | Week | Month | 30d | Feb 9, 2:31 pm – Mar 8, 3:31 pm

Find Coverage Gaps

Show Assets which were Not Seen by Crowdstrike in the last 30 Days

TOTAL 1,568

Type	Asset Count	
Server	146	30%
Workstation	63	13%
Printer	244	50%
Code Repository	39	7%
Container Image	146	30%
Host	63	13%
Unknown	244	50%

Explore Coverage Overlaps

Crowdstrike × | ZCC × | ServiceNow ×

You can select up to 3 sources.

Crowdstrike	Total: 500	
No overlap	365	30%
Overlap with ZCC	125	30%
Overlap with Service...	35	30%

Assets Coverage

Unique | Overlap

Explode | Group Repeated

Source Name	Total Assets
Crowdstrike	94
Tenable	98
ZCC	100
ServiceNow	95
Snyk	94
Wiz	99
Name 7	100
Total	596

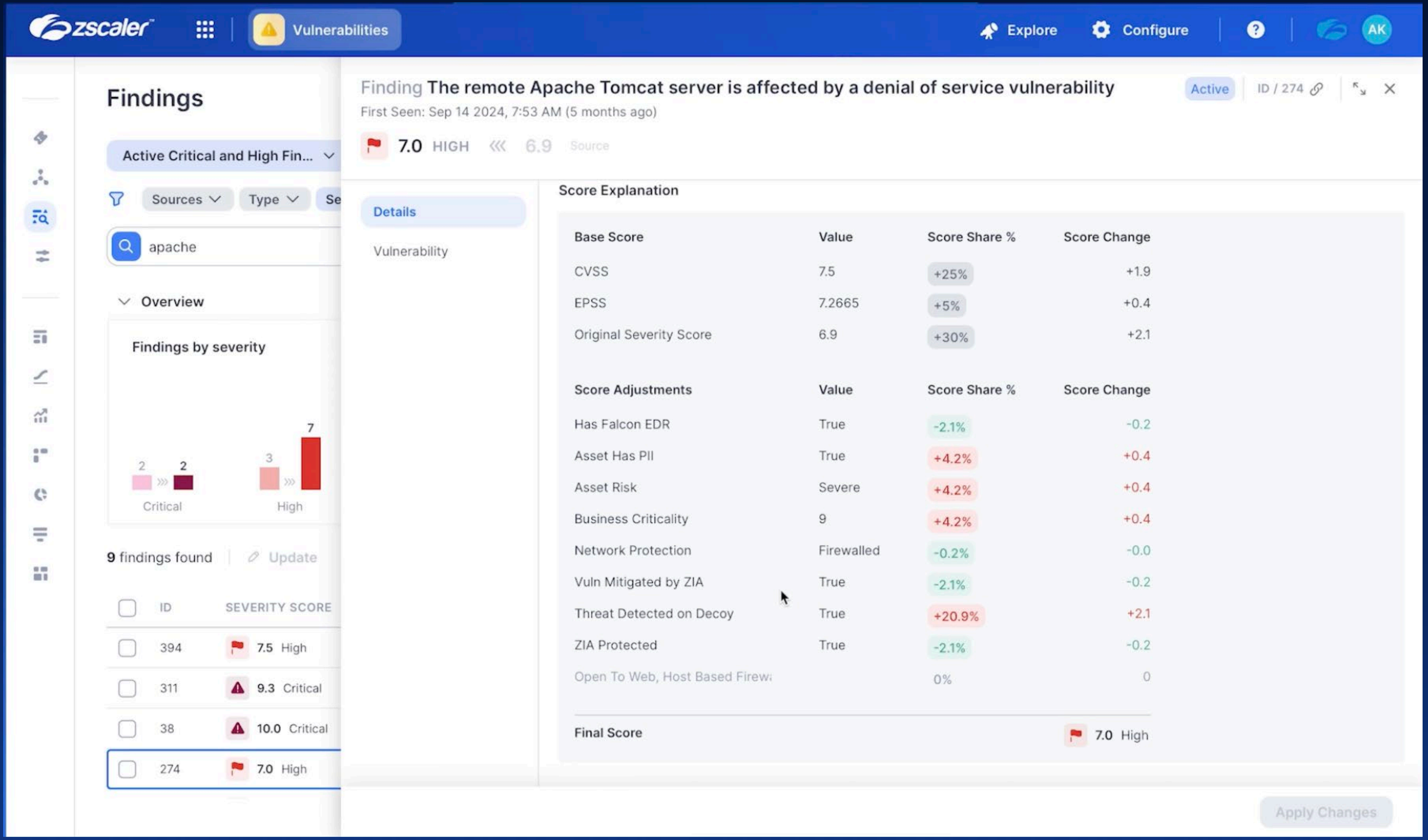
Crowdstrike		
Unique	146	30%
Overlap	146	30%

Are all your managed assets properly protected? Not only will Zscaler generate an accurate asset inventory of all active assets, but it will quickly enrich the CMDB with data from security tools so your view of exposure is always up-to-date.

https://www.zscaler.com/products-and-solutions/ctem

Unified Vulnerability Management

Vulnerability scanning alone only produces noise. Context beyond CVEs is needed to properly prioritize action and accurately measure risk. UVM enriches your vulnerability scans ranking them by real risk.



ID	SEVERITY SCORE
394	7.5 High
311	9.3 Critical
38	10.0 Critical
274	7.0 High

Finding The remote Apache Tomcat server is affected by a denial of service vulnerability

First Seen: Sep 14 2024, 7:53 AM (5 months ago)

7.0 HIGH «« 6.9 Source

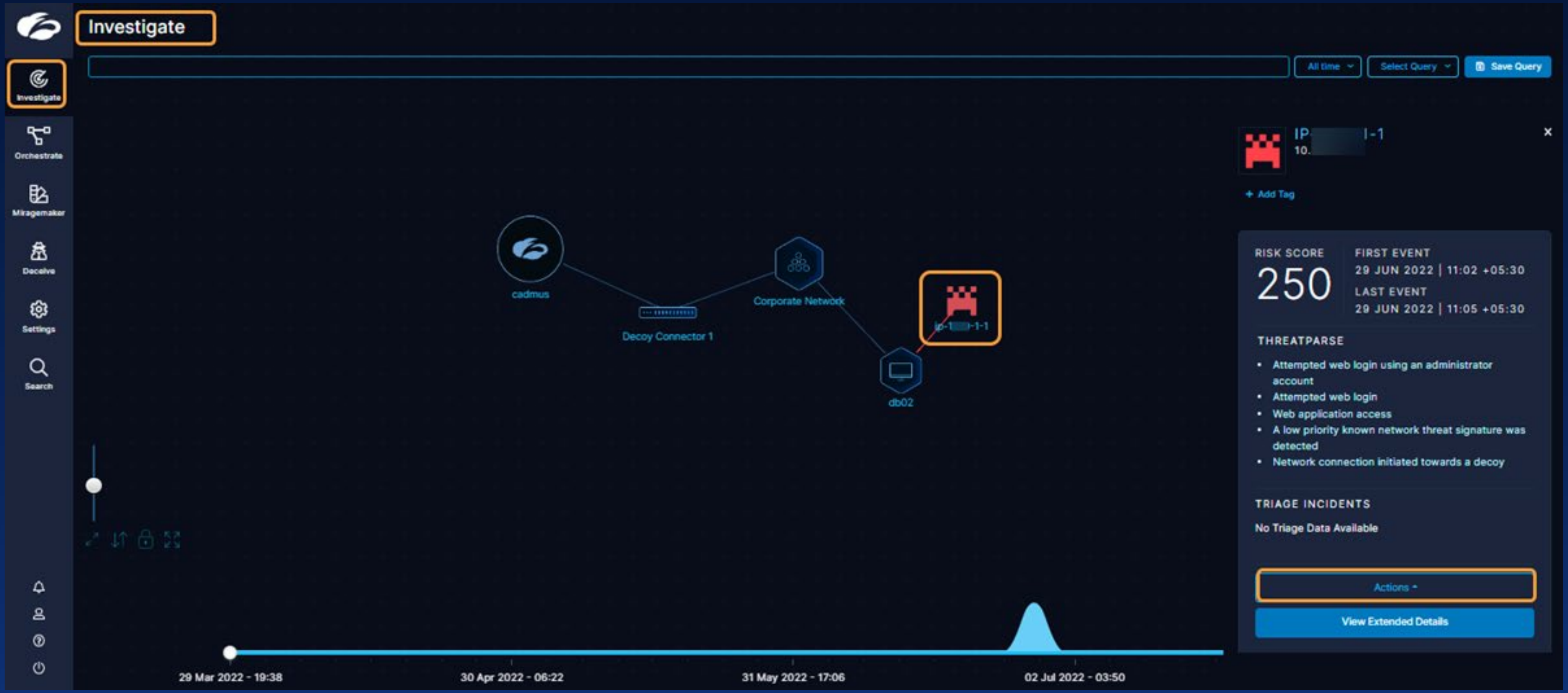
Score Explanation

Base Score	Value	Score Share %	Score Change
CVSS	7.5	+25%	+1.9
EPSS	7.2665	+5%	+0.4
Original Severity Score	6.9	+30%	+2.1
Score Adjustments	**Value**	**Score Share %**	**Score Change**
Has Falcon EDR	True	-2.1%	-0.2
Asset Has PII	True	+4.2%	+0.4
Asset Risk	Severe	+4.2%	+0.4
Business Criticality	9	+4.2%	+0.4
Network Protection	Firewalled	-0.2%	-0.0
Vuln Mitigated by ZIA	True	-2.1%	-0.2
Threat Detected on Decoy	True	+20.9%	+2.1
ZIA Protected	True	-2.1%	-0.2
Open To Web, Host Based Firew:		0%	0
Final Score			7.0 High

https://www.zscaler.com/products-and-solutions/vulnerability-management

Deception

Bad actors can be good at evading security, but they tend to investigate and attack assets they find. Deception brings high fidelity telemetry on both attacker presence and tactics. This is valuable SOC intelligence to help hunting and remediation.



IP[redacted]l-1
10.

RISK SCORE
250

FIRST EVENT
29 JUN 2022 | 11:02 +05:30

LAST EVENT
29 JUN 2022 | 11:05 +05:30

THREATPARSE

- Attempted web login using an administrator account
- Attempted web login
- Web application access
- A low priority known network threat signature was detected
- Network connection initiated towards a decoy

TRIAGE INCIDENTS

No Triage Data Available

https://www.zscaler.com/products-and-solutions/deception-technology

Session Take Aways

1 Zscaler acts prudently and ethically when it comes to data use in AI. **No customer data is used to train global AI models**.

2 Zscaler uses **AI to automate foundational functions** to scale with massive changes that occur on the Internet both in structure and attack horizon.

3 Risk management and security operation capabilities use **advanced AI to extend and correlate Zscaler and 3rd- party telemetry**, often in a security fabric.

Thank You

Controlware
Security Day

Danke für Ihre Aufmerksamkeit.
Wir freuen uns über Ihr Feedback!

Bitte geben Sie den ausgefüllten Bogen am Empfang ab und erhalten Sie als Dankeschön ein kleines Präsent.