Zero Trust + AI

Secure and Optimize Your Organization

WHITEPAPER

Why Is There a Need for Zero Trust and AI?

The way work gets done today is vastly different from several years ago. It used to be that employees came to the office every day to do their jobs. As they did so, they accessed IT applications and resources hosted in their organization's on-premises data centers. Stated simply, with users, apps, and data all in the office, organizations operated in what was essentially an on-premises-only fashion. However, two mutually reinforcing phenomena forever changed this status quo.

First, the rise of the cloud and software-as-a-service (SaaS) applications like Salesforce and Microsoft 365 meant organizations no longer had to build or manage their IT resources on-premises. Instead, they could use purpose-built apps and tools delivered as services from vendors' clouds. This flexibility significantly enhanced dynamism and cut costs for organizations.

Second, and in large part because of the adoption of cloud apps, users started working remotely. Afterall, IT resources were off-premises and users no longer had to come to the office to access them. Naturally, the global pandemic in 2020 accelerated remote work (and cloud app) adoption as organizations tried to stay productive while complying with shelter-in-place mandates. Once again, increased flexibility served as a boon both to dynamism and cost savings.

These transformations, while incredibly helpful, gave rise to significant challenges around cyber risk and competitive pressure:

- **Cyber risk** increased because traditional network-centric, castle-and-moat security models were not designed for the cloud or remote work, and could not keep pace with the growing sophistication of modern threats.
- **Competitive pressures** increased because enhanced productivity and dynamism became the norm, challenging organizations to operate as efficiently as possible while meeting customers' growing expectations as quickly as possible.

For organizations to succeed today, they must address these twin challenges. As such, another phenomenon that is incredibly important to this conversation is the emergence of artificial intelligence (AI) and machine learning (ML). In a very short timeframe, AI proliferated broadly throughout the modern workplace, across business and cybersecurity solutions alike. While it may seem easy to dismiss AI as the latest marketing buzzword, the truth is that AI holds the key to addressing the dual challenges above—at least, that is, when AI is paired with zero trust. That is why countless organizations around the globe are turning to Zscaler.

> AI holds the key to addressing the dual challenges of cyber risk and competitive pressure—
> at least, that is, when AI is paired with **zero trust.**

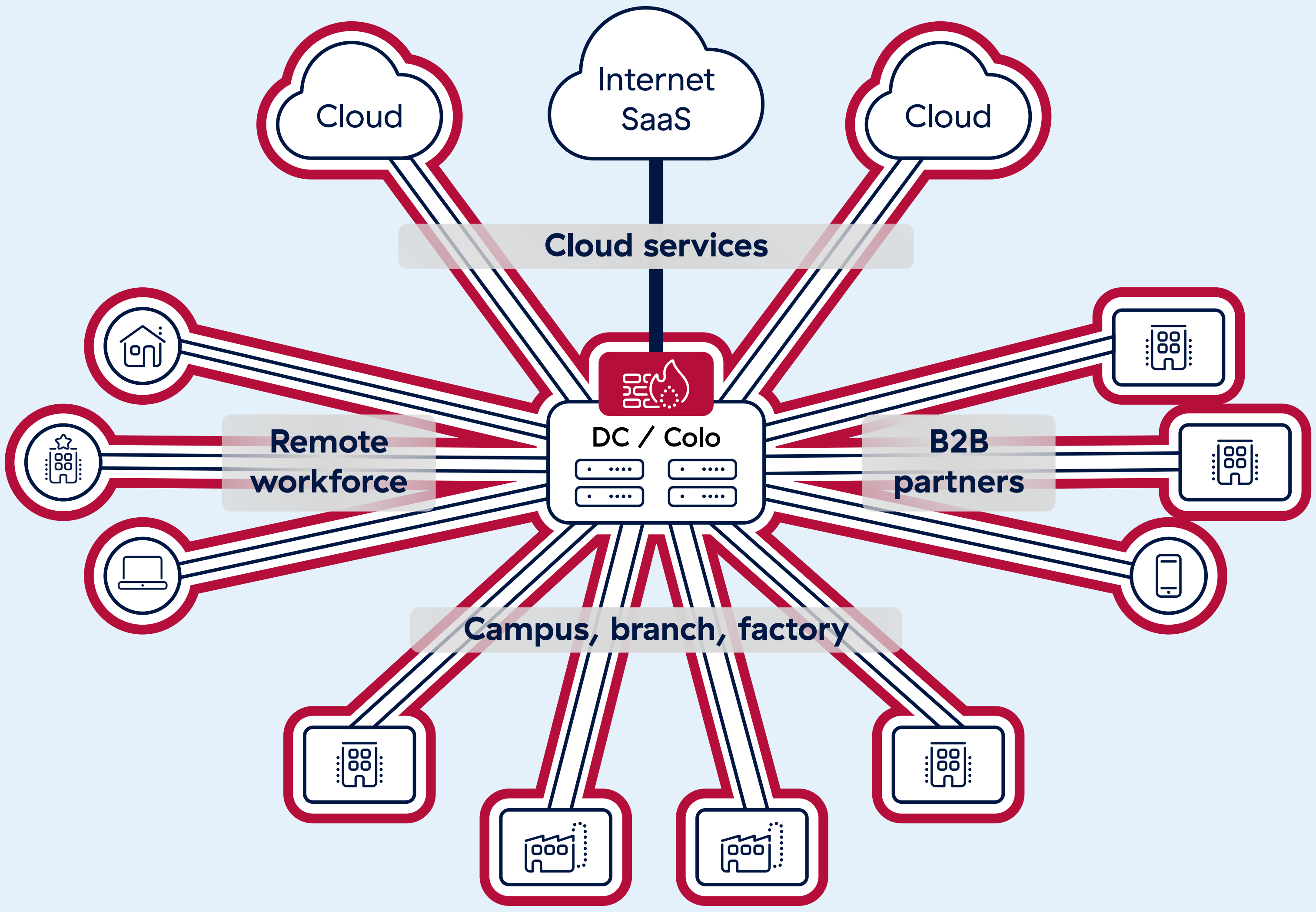
Zero Trust + AI with Zscaler

The cloud native Zscaler Zero Trust Exchange platform delivers a zero trust architecture infused with AI/ML to augment its capabilities. This potent combination of zero trust architecture and AI solves both of the aforementioned problems around rising risk and peaking pressure to do more with less. To understand why, let's discuss each of these elements.

ZERO TRUST ARCHITECTURE

Zero trust is not merely another lever for the status quo; it is not just another security point product. Rather, it is a fundamentally different way of doing things that is distinct from standard, network-centric security architectures, free from the shortcomings of yesterday's methodologies. That is why it is critically important to use zero trust as a foundation for implementing AI in security. Otherwise, attempting to improve a network-centric security architecture with AI is like polishing a broken mirror—its sheen may improve, but it remains inherently flawed.

Traditional Network- and Firewall-Centric Architecture



A trusted private network connects everything.

Security focuses on defending the network with firewalls.

This worked well in the old world, but can now be a liability **(high cost, security risk, poor experience).**

Figure 1: Network-centric architecture

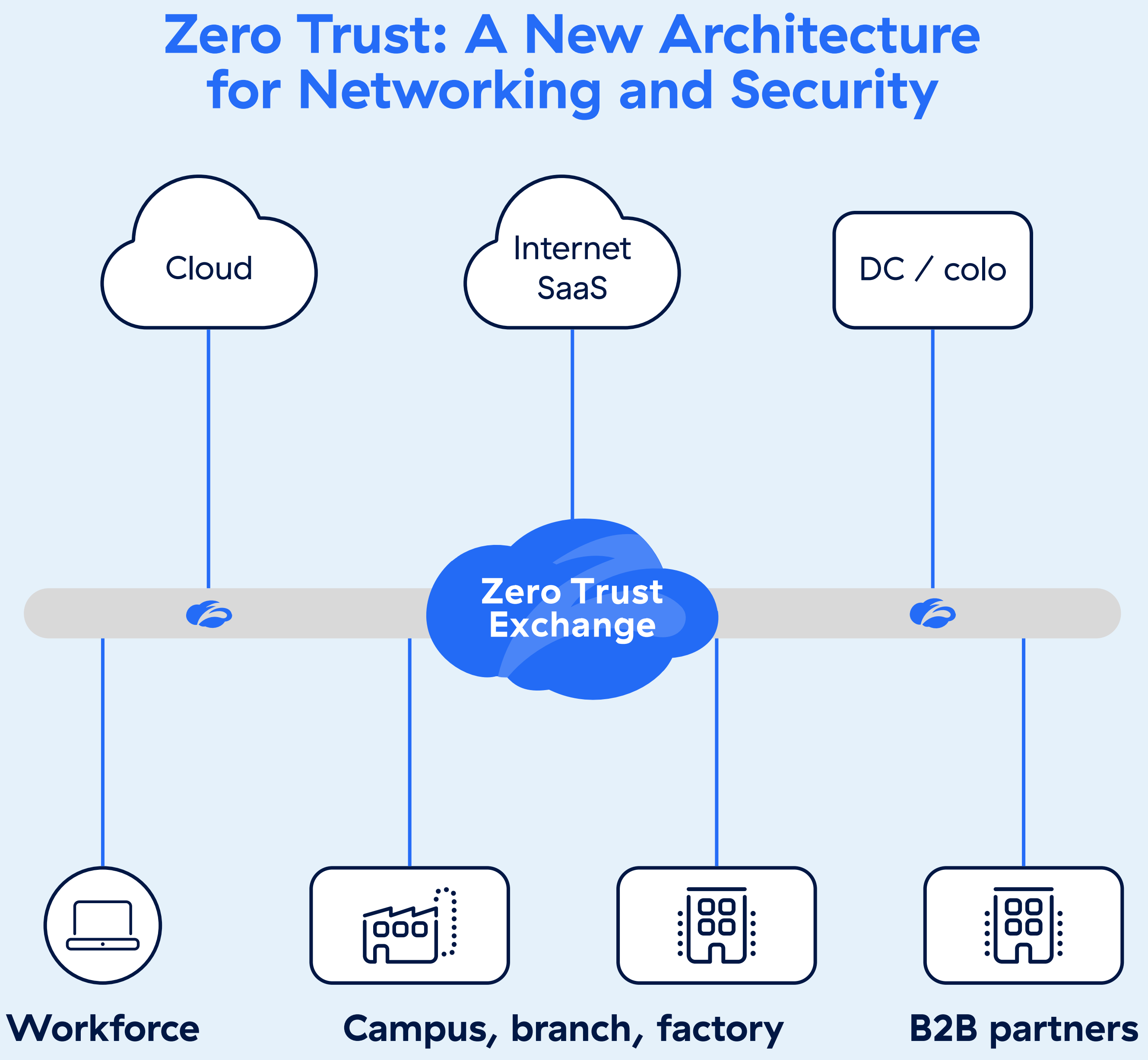
Network-centric architectures built upon tools like firewalls and VPNs are focused on establishing a security perimeter around a trusted hub-and-spoke network that is used to connect everything within an organization. This is why they are often called castle-and-moat security models. Network-centric architectures were designed for the on-premises-only world, before the rise of cloud apps and remote work. When organizations try to use them today, these architectures create a number of challenges::

- **They expand the attack surface** by extending the network to more users, devices, clouds, and locations, and by using firewalls and VPNs, which have public IP addresses.
- **They enable compromise** because their underlying appliances (hardware and virtual) lack the scalability to inspect encrypted traffic at scale, **where 87% of threats hide**.
- **They fail to stop lateral threat movement** because they place users and entities onto the network, where they can access the various connected resources therein.
- **They cannot eliminate data loss** due to the inability to inspect encrypted traffic and the inability to secure modern leakage paths like sharing in SaaS apps.
- **They increase complexity and cost** through myriad security point products and sprawling networks, which are expensive to purchase, configure, and maintain.
- **They harm user productivity** because they require backhauling traffic to a centralized data center, which adds latency that disrupts digital experiences.

A regular drumbeat of **CVEs** for various **firewall** and **VPN** solutions highlights the need to retire traditional tools and embrace zero trust architecture.

As mentioned previously, zero trust is fundamentally different from network-centric architectures. Rather than being like a moat (a perimeter) that protects a castle (a trusted network), zero trust is like an intelligent switchboard that provides secure any-to-any communications in a one-to-one fashion—users and other entities are connected directly to their destinations instead of to the network as a whole. And instead of relying on IP addresses, context and risk are used to determine who should be able to access what.

In other words, Zscaler decouples security and connectivity from the network, and enforces the principle of least-privileged access. This zero trust communication (and a plethora of other functionality) is delivered as a service, at the edge, from the Zscaler Zero Trust Exchange, the world's largest cloud security platform. As a result, backhauling traffic to a centralized data center becomes a thing of the past. Instead, organizations get zero trust everywhere, across workforces, branches, and clouds.



An exchange / switchboard connects users, devices, and workloads using business policies—over any network.

It offers lower TCO, superior security, and a great experience.

Figure 2: Zero trust architecture with Zscaler

With Zscaler, zero trust architecture:

- **Minimizes the attack surface** by stopping endless network expansion, eliminating firewalls, VPNs, and their public IPs, and hiding apps behind the Zero Trust Exchange
- **Stops compromise** through a high-performance security cloud that scales as needed to inspect any volume of encrypted traffic and enforce real-time policies
- **Prevents lateral threat movement** by connecting entities directly to destinations they are authorized to access——not to the network and its many connected resources
- **Blocks data loss,** whether malicious or accidental, across all data leakage paths, including encrypted traffic, cloud apps, endpoints, and email
- **Cuts costs and complexity** by simplifying networking with direct-to-app connectivity and simplifying security with a platform that eliminates legacy tools and point products
- **Enhances productivity** by improving user experiences with direct-to-app access that eliminates backhauling, and the routing of traffic via the shortest path to its destination

For all of these reasons, zero trust is the ideal architectural foundation for implementing AI/ML in cybersecurity.

LEADERSHIP IN AI

Zscaler has distinct advantages in the area of AI/ML. This is largely because AI is only as effective as the data from which it is able to learn; garbage in, garbage out, as the old adage goes.

As the world's largest cloud security platform, the Zscaler Zero Trust Exchange secures the traffic of thousands of organizations globally, amounting to more than 50 million users as well as countless workloads, IoT/OT devices, third-party workers, and more. As a result of this scale, Zscaler's 160 global points of presence process more than 500 billion transactions every day (more than 50 times the number of daily Google searches), and more than 500 trillion daily telemetry signals. Because Zscaler scrutinizes context in order to securely govern access to IT resources, there is rich data surrounding device, content, destination, network, and more for every access attempt. That said, Zscaler does not use customer data to train its AI models. Each customer owns their proprietary information or personal data (usernames, email addresses, device IDs, etc.) in the Zscaler logs. Zscaler only uses data or metadata that does not contain customer or personal data for AI model training. More on that topic can be found **here**.

In addition to the above, Zscaler has a wealth of data from **ThreatLabz**, our world-class threat research team, which constantly studies cybercriminals' latest tactics, techniques, and technologies. This equips Zscaler with years of research about cyberthreats, how they work, and their increasing sophistication. Last but not least, some of Zscaler's AI-driven solutions are also powered by the Zscaler Data Fabric for Security, which will be discussed in more detail further below.

With this massive, highly relevant (de-identified) data set training purpose-built large language models (LLMs), Zscaler can accelerate the application of data to decision-making. AI-driven solutions across the Zero Trust Exchange feature enhanced analytics, automation, and efficacy. Throughout the rest of this white paper, we will detail the various ways the Zscaler platform leverages AI/ML to solve modern challenges, helping you to secure and optimize your organization.

Securing and Optimizing Your Organization with Zscaler

Cloud Sandbox AI Instant Verdict

If organizations are to stay secure as cyberthreats become more advanced, they need to implement real-time detection and mitigation for zero day attacks. Without doing so, they risk falling victim to cybercriminals who use constantly evolving techniques to bypass security measures.

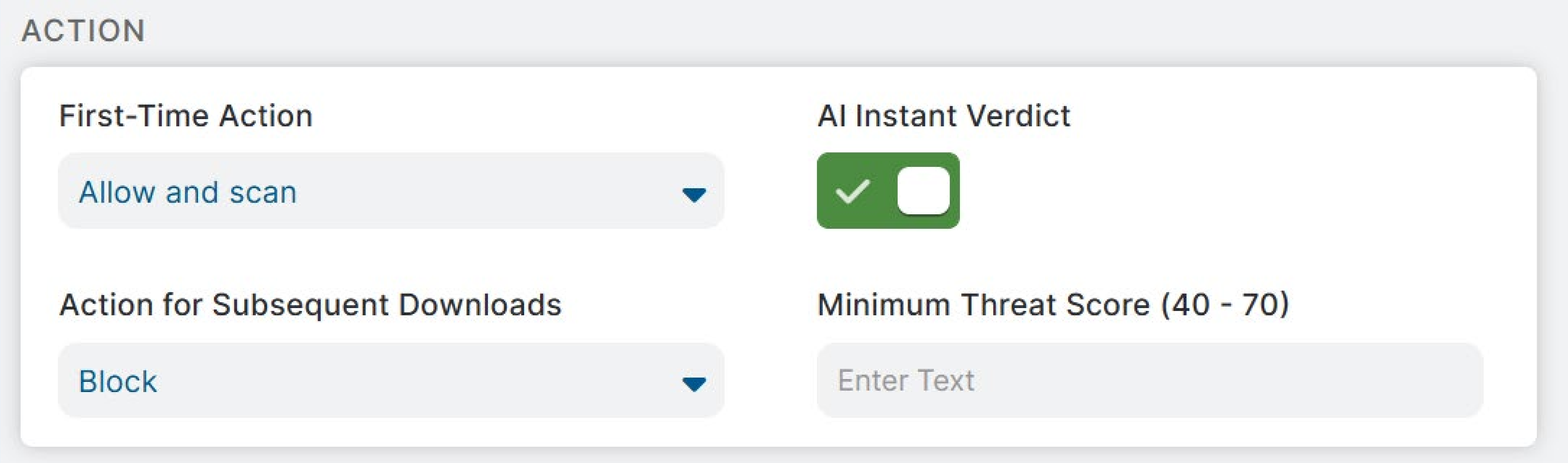
Sandbox technology plays a key role in the pursuit of real-time zero day protection. When users attempt to access something, a sandbox safely analyzes potentially malicious files in a controlled environment in order to ensure that they are safe before granting users access.

However, traditional sandbox methods often come with a tradeoff between security and productivity. If the rules are too relaxed, harmful files can slip through and compromise systems. On the other hand, overly strict criteria can block harmless files, delaying user access, disrupting workflows, and reducing productivity.

The Zero Trust Exchange revolutionizes sandboxing by eliminating traditional security-productivity tradeoffs through AI-powered innovation. By integrating machine learning into Zscaler's cloud native sandbox, it delivers high-confidence verdicts within seconds, leveraging years of analysis and interactions with over 600 million file samples.

With the Zscaler Cloud Sandbox, enabling the “AI Instant Verdict” setting is as simple as clicking a button. This feature automatically blocks high-confidence malicious files with an AI/ML threat score of 91 to 100—without making users wait for file detonation. It offers immediate protection against zero day file-based threats while keeping users productive.

By instantly blocking these threats, the risk of patient zero incidents is greatly reduced, minimizing investigation efforts for SOC teams. This allows them to focus on more critical tasks while still ensuring that the organization remains protected from evolving cyberthreats. In short, AI Instant Verdict not only enhances security but also optimizes time for both SOC teams and users.



ACTION

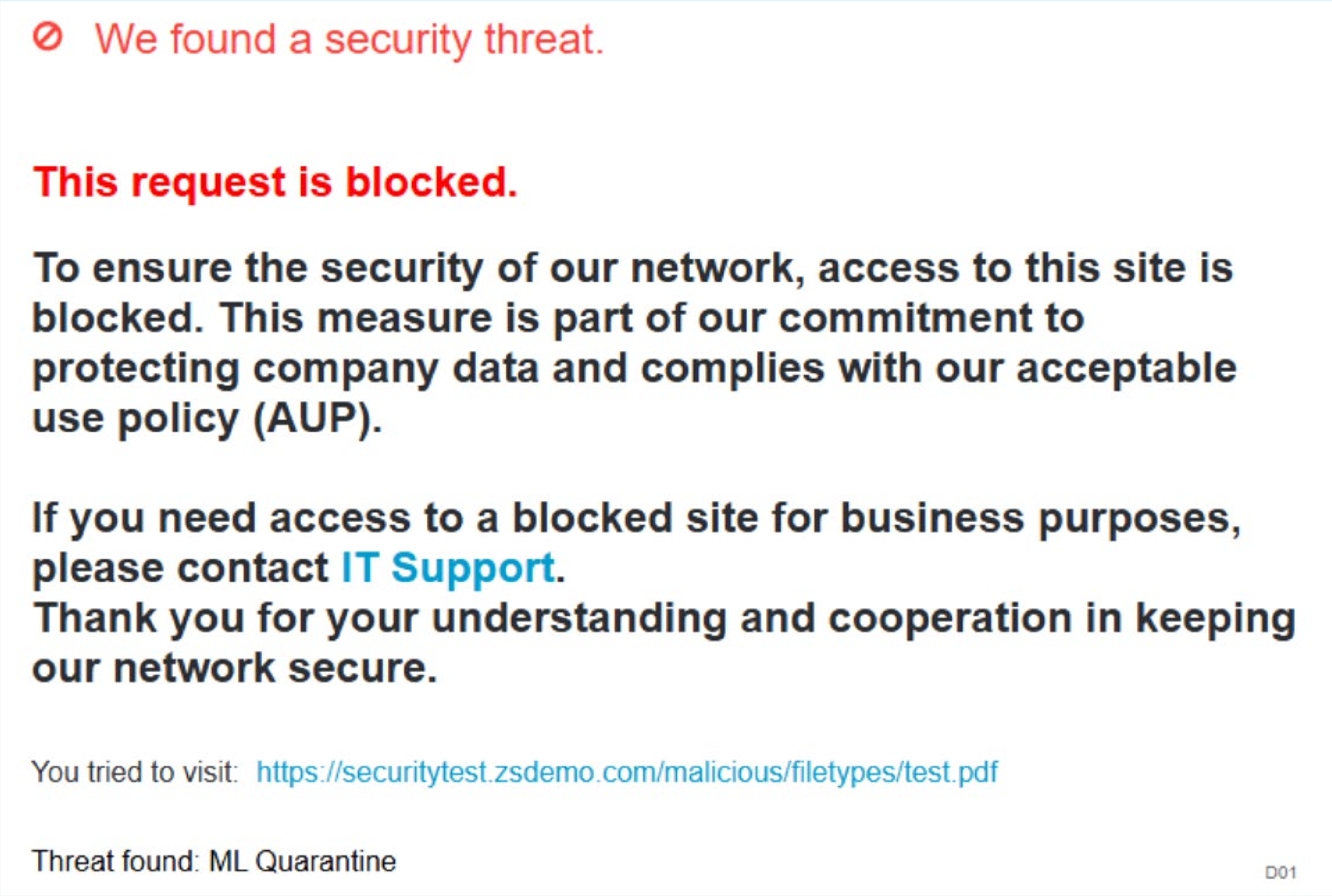
First-Time Action: Allow and scan

AI Instant Verdict: ✓

Action for Subsequent Downloads: Block

Minimum Threat Score (40 - 70): Enter Text

Figure 3: AI Instant Verdict being enabled



We found a security threat.

This request is blocked.

To ensure the security of our network, access to this site is blocked. This measure is part of our commitment to protecting company data and complies with our acceptable use policy (AUP).

If you need access to a blocked site for business purposes, please contact IT Support.
Thank you for your understanding and cooperation in keeping our network secure.

You tried to visit: https://securitytest.zsdemo.com/malicious/filetypes/test.pdf

Threat found: ML Quarantine

Figure 4: AI Instant Verdict user notification

Zero Trust Browser Smart Isolation

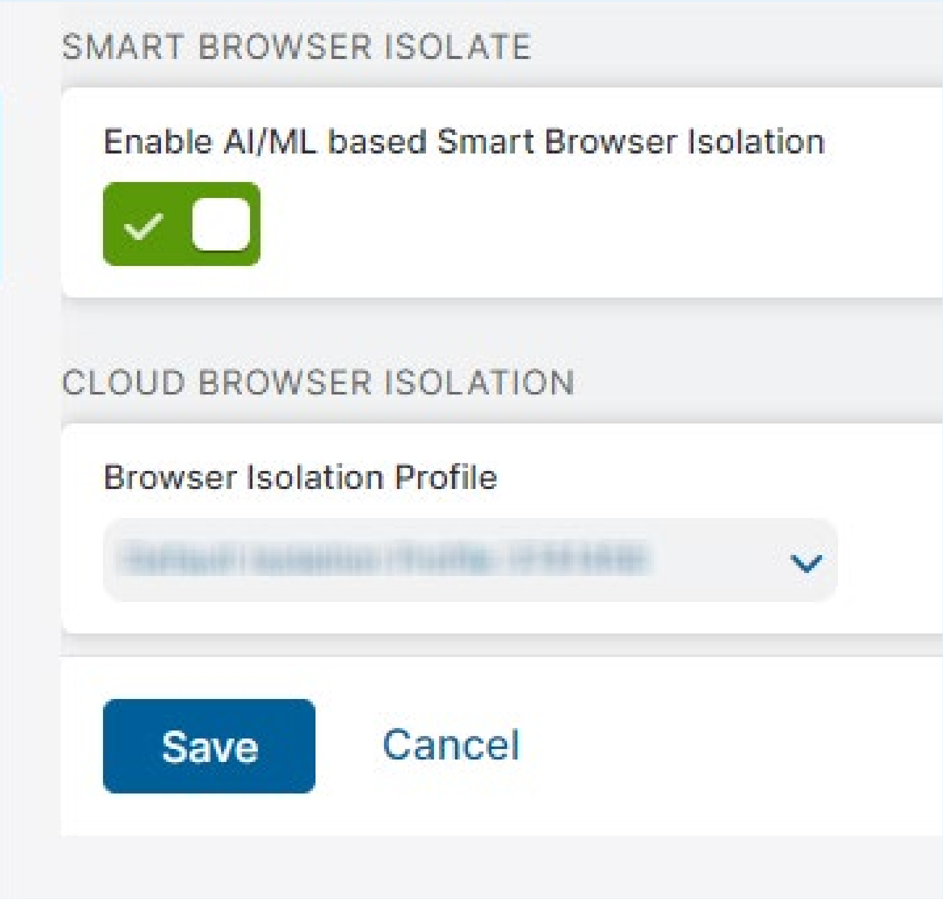
Cybercriminals use malicious websites to load dangerous content onto users' browsers and devices, creating beachheads for mounting attacks on the users' organizations. URL filtering tools that can block access to various websites are the go-to solutions for addressing this problem. Typically, this is done by filtering known-malicious websites as well as newly registered domains that are not yet proven trustworthy.

However, the above approach creates two problems. First, attackers find ways to work around it. That's because trustworthy, time-tested websites can still unknowingly serve malicious content; for example, through advertisements or zero pixel iframes placed by cybercriminals. Second, blocking newly registered domains interrupts end user experiences by preventing access to new but legitimate web-based tools as well as existing, trustworthy websites that merely feature updated domains. In either case, the resulting influx of help desk tickets created for users' threat infections and productivity disruptions means that IT's productivity is disrupted, as well.

Zscaler's Zero Trust Browser Smart Isolation overcomes these security and productivity challenges. The solution is dubbed "Smart" because it incorporates AI and ML models that empower it to automatically recognize potentially malicious web content in a web page—even without a policy explicitly applied to that page. As a result, organizations are able to stay ahead of emerging threats with newly registered domains as well as threats hidden within trusted domains.

With Zero Trust Browser Smart Isolation, when a user visits a web destination that AI determines to have a high likelihood of being malicious, the user's session is "isolated." This means that the web session is spun up in the Zero Trust Exchange and only web commands of the session are sent from the Zscaler cloud to the end user's device. Streams of images of the isolated session still give the regular user experience, but the user does not interact directly with the website.

As a result, active content does not reach their endpoint. This means that attempted threat downloads cannot make their way onto the device, and potential data leakage can be controlled by preventing file uploads and text pasting. This vastly decreases risk—without excessive blocking that prevents access to legitimate web tools that users need. That means fewer help desk tickets and better productivity for end users and IT alike.



SMART BROWSER ISOLATE

Enable AI/ML based Smart Browser Isolation: ✓

CLOUD BROWSER ISOLATION

Browser Isolation Profile

Figure 5: One-click enablement of Zero Trust Browser Smart Isolation

AI-Powered User-to-App Segmentation

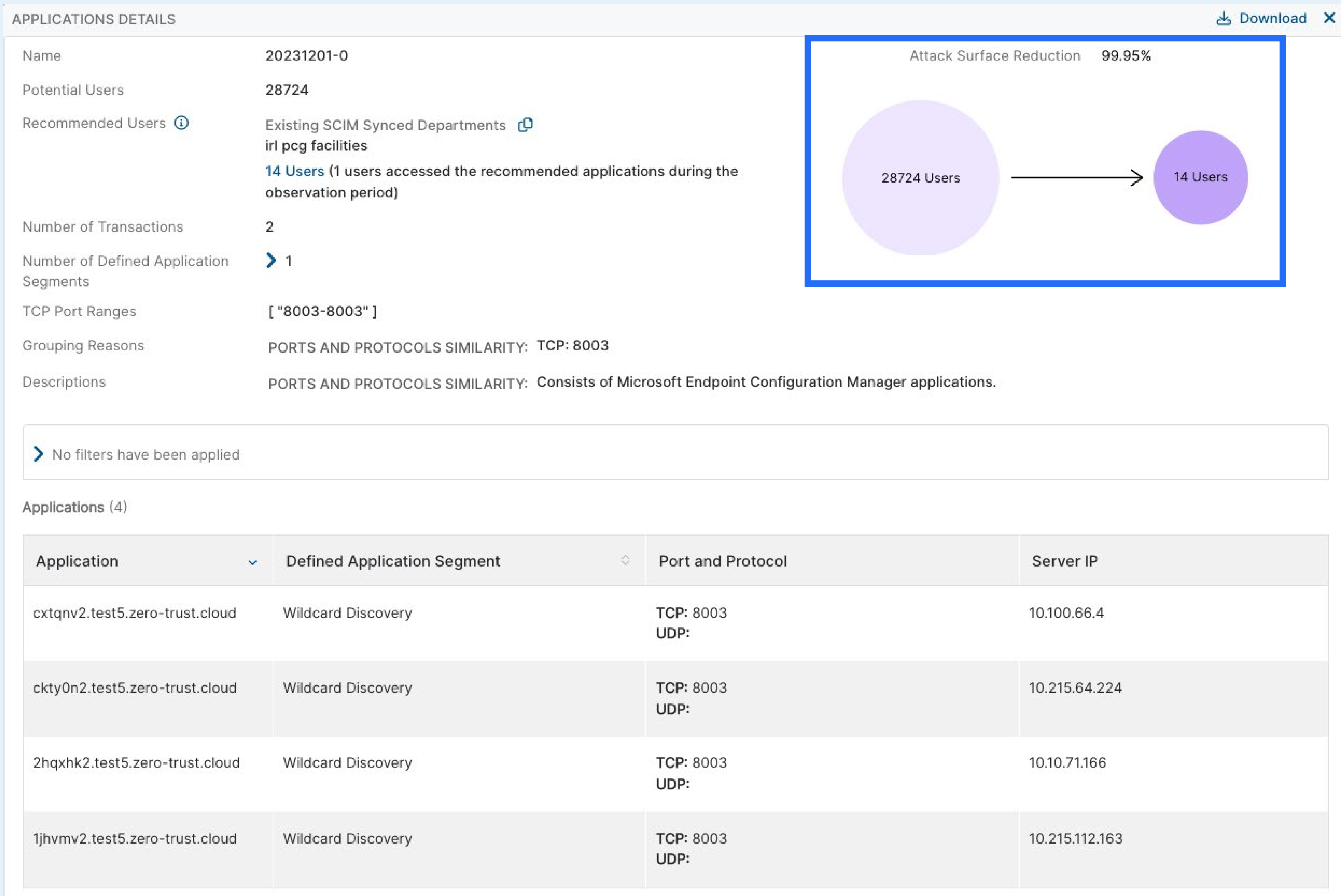
Organizations that rely on network-centric security architectures built with traditional tools like firewalls face a significant challenge in stopping lateral threat movement. As mentioned earlier, lateral movement refers to the way that attackers on the network can move across connected resources and access the sensitive data within them. Without effective segmentation to prevent this, the blast radius of an attack can be extensive, enabling large-scale data breaches as well as significant reputational and financial damage.

Unfortunately, organizations typically struggle to implement and maintain robust network segmentation practices. Traditional methods rely on manual configuration, which is prone to human error and can result in misconfigurations that leave critical assets exposed. Additionally, the dynamic nature of modern networks, with the increasing adoption of cloud services and remote work, makes it challenging to keep up with the constant changes in network topology and user access requirements. This complexity increases management overhead and further hampers the ability to implement effective segmentation strategies.

As explained previously, zero trust architecture with Zscaler means providing access directly to applications instead of to the network. This zero trust segmentation helps prevent lateral movement for users, workloads, branch sites, and devices. To further reduce the potential blast radius of any breach, Zscaler offers AI-Powered User-to-App Segmentation. This feature uses machine learning to automatically discover private applications and analyze user-to-application traffic flows. Based on this analysis, it intelligently recommends optimal segmentation policies.

AI-Powered User-to-App Segmentation works by continuously monitoring and analyzing user behavior and application usage. It leverages ML algorithms to identify patterns and anomalies so that it can determine which employees require access to which apps. For example, if only a small subset of employees accesses a finance app, Zscaler will automatically create a segment that restricts access to that group of users. This targeted approach greatly reduces the opportunity for lateral movement across applications.

AI-Powered User-to-App Segmentation represents a fundamentally different approach to segmentation. It streamlines the creation of granular zero trust access policies and reduces the management burden of manual configuration. This saves time and resources for IT teams, enabling them to focus their efforts on other critical security tasks. It also automates the enforcement of least-privileged access, ensuring users can only reach the applications required for their roles. As a result, it significantly reduces the internal attack surface, prevents lateral movement, and accelerates an organization’s journey to a true zero trust security posture.



Name	20231201-0
Potential Users	28724
Recommended Users	Existing SCIM Synced Departments irl pcg facilities 14 Users (1 users accessed the recommended applications during the observation period)
Number of Transactions	2
Number of Defined Application Segments	1
TCP Port Ranges	["8003-8003"]
Grouping Reasons	PORTS AND PROTOCOLS SIMILARITY: TCP: 8003
Descriptions	PORTS AND PROTOCOLS SIMILARITY: Consists of Microsoft Endpoint Configuration Manager applications.

Attack Surface Reduction 99.95%

No filters have been applied

Applications (4)

Application	Defined Application Segment	Port and Protocol	Server IP
cxtqnv2.test5.zero-trust.cloud	Wildcard Discovery	TCP: 8003 UDP:	10.100.66.4
ckty0n2.test5.zero-trust.cloud	Wildcard Discovery	TCP: 8003 UDP:	10.215.64.224
2hqxhk2.test5.zero-trust.cloud	Wildcard Discovery	TCP: 8003 UDP:	10.10.71.166
1jhvmv2.test5.zero-trust.cloud	Wildcard Discovery	TCP: 8003 UDP:	10.215.112.163

Figure 6: AI-Powered User-to-App Segmentation recommendation

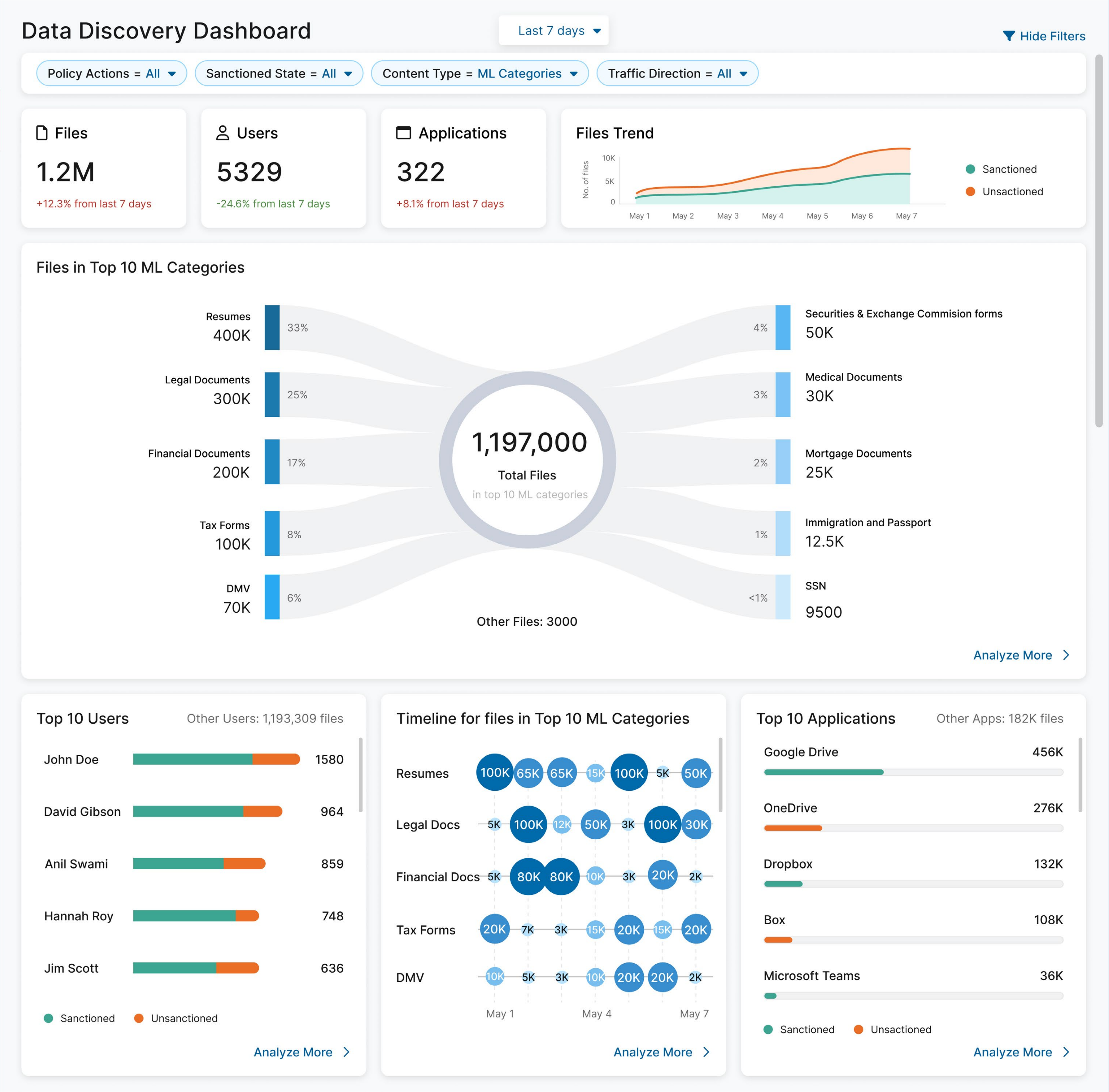
LLM Classification for auto data discovery

Today's digital landscape represents a significant challenge to data security. Data is widely distributed outside of the traditional data center, continually stored and accessed across the web, cloud applications, and remote user devices. As a result, organizations are grappling with a new reality that makes it difficult to identify what sensitive information is going where. This makes it increasingly difficult for CISOs and data protection teams to ensure that data is secured.

Relying on legacy point products with traditional classification to secure data has become increasingly untenable. In addition to accuracy challenges caused by traditional regex classification, these tools typically operate in silos, leading to visibility gaps and slow response times. Beyond that, they require manual duplication of policies across disjointed solutions with disparate capabilities, which is an error-prone, time-consuming process. Ultimately, this piecemeal approach increases the risk of data loss as well as cost and complexity.

With Zscaler's AI-powered LLM Classification, organizations can accelerate their ability to automatically find, classify, and control sensitive data of all types—as it is created and wherever it goes. Zscaler AI and LLMs have been thoroughly trained to identify new and unknown data types using language processing. From strategic business reports to various types of health or finance content, data can now be identified without relying on specific key regex identifiers—across inline, at-rest, and in-use channels. As an alternative to regex, LLM Classification empowers data security teams to protect new types of data with improved accuracy. Additionally, admins don't need to duplicate rules across disjointed tools (or even configure dictionaries or data classification policies in Zscaler) to find sensitive data. As a result, organizations can achieve faster, more accurate data discovery and protection, ensuring that sensitive information is secured across all data leakage channels.

In addition to providing enhanced protection, AI-powered LLM Classification also reduces the complexity of overseeing data security. As mentioned above, the number of point product dashboards is minimized, the need for manual policy duplication is eliminated, and DLP dictionaries don't even need to be configured. AI-driven automation reduces the need for specialized expertise while helping organizations deploy and administer data protection programs more quickly. The end result is both improved security and enhanced productivity for admins.



Data Discovery Dashboard

Last 7 days

Hide Filters

Policy Actions = All | Sanctioned State = All | Content Type = ML Categories | Traffic Direction = All

Files
1.2M
+12.3% from last 7 days

Users
5329
-24.6% from last 7 days

Applications
322
+8.1% from last 7 days

Files Trend

Files in Top 10 ML Categories

Category	Files	Share
Resumes	400K	33%
Legal Documents	300K	25%
Financial Documents	200K	17%
Tax Forms	100K	8%
DMV	70K	6%
Securities & Exchange Commision forms	50K	4%
Medical Documents	30K	3%
Mortgage Documents	25K	2%
Immigration and Passport	12.5K	1%
SSN	9500	<1%

1,197,000
Total Files
in top 10 ML categories

Other Files: 3000

Analyze More

Top 10 Users — Other Users: 1,193,309 files

User	Files
John Doe	1580
David Gibson	964
Anil Swami	859
Hannah Roy	748
Jim Scott	636

● Sanctioned ● Unsanctioned

Analyze More

Timeline for files in Top 10 ML Categories

Resumes	100K	65K	65K	15K	100K	5K	50K
Legal Docs	5K	100K	12K	50K	3K	100K	30K
Financial Docs	5K	80K	80K	10K	3K	20K	2K
Tax Forms	20K	7K	3K	15K	20K	15K	20K
DMV	10K	5K	3K	10K	20K	20K	2K

Analyze More

Top 10 Applications — Other Apps: 182K files

Application	Files
Google Drive	456K
OneDrive	276K
Dropbox	132K
Box	108K
Microsoft Teams	36K

● Sanctioned ● Unsanctioned

Analyze More

Figure 7: Auto data discovery dashboard

As a final note when it comes to protecting data, **Zscaler Data Security Posture Management (DSPM)** can be navigated via Zscaler Copilot. Admins can ask questions in plain text about the safety of their data and receive responses with granular insights.

Risk360

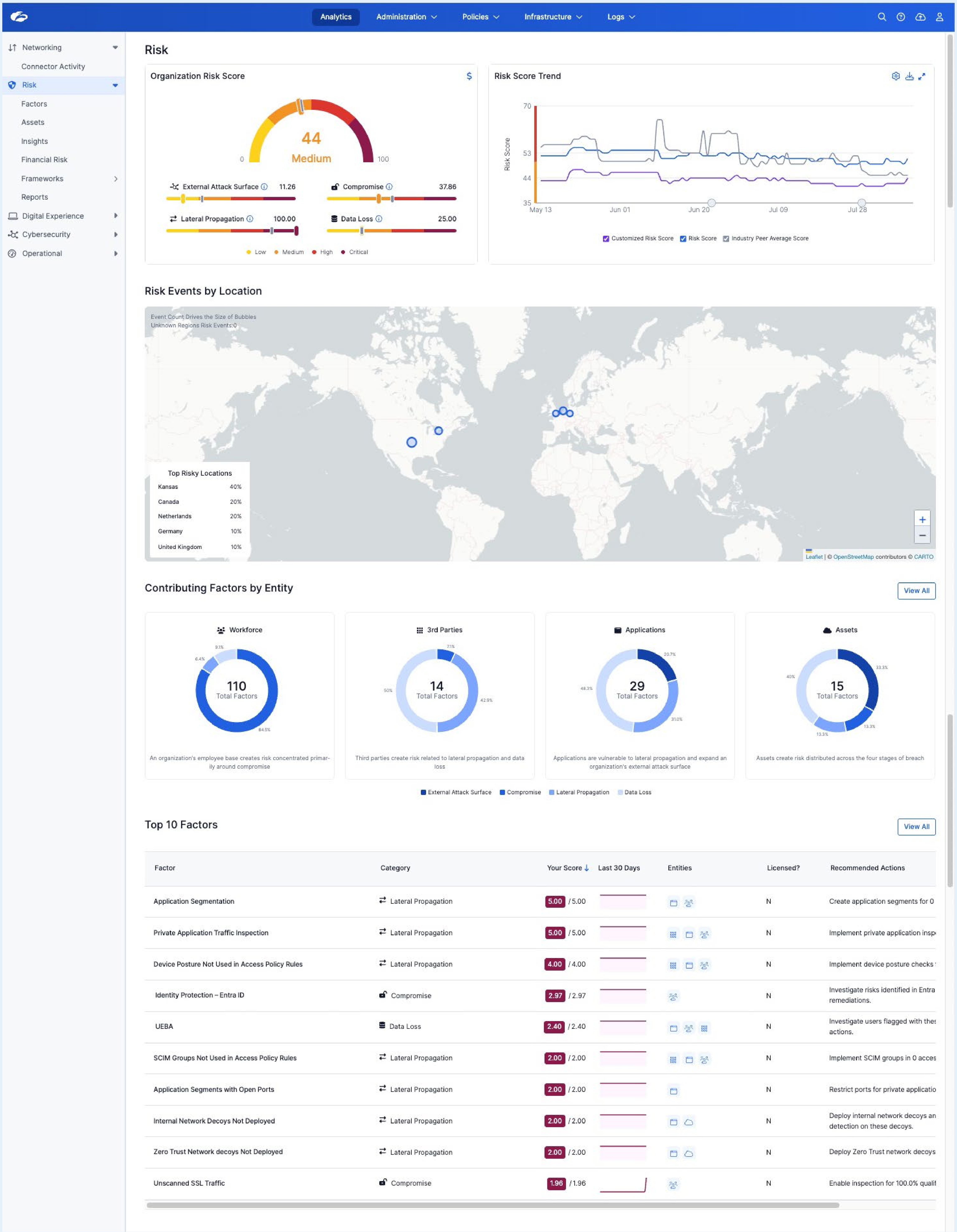
In today's rapidly evolving digital landscape, organizations are grappling with ever-increasing complexity and an ever-growing number of misconfigurations and security gaps. Making matters worse, cybercriminals are constantly refining their methods, embracing the latest malicious techniques, and enhancing the sophistication of their attacks. Trying to recreate zero trust architecture with network-centric tools like firewalls is an oxymoronic endeavor that inevitably falls short in providing a comprehensive view of these risks (not to mention, it increases risk in key ways described earlier). And even for organizations who do truly deploy a zero trust architecture, it can be challenging to verify that they are minimizing risk as much as possible.

To address this challenge, Zscaler offers Risk360, a comprehensive and actionable framework that delivers insightful cyber risk quantification of a customers' adherence to zero trust policies. Zscaler is uniquely positioned to provide this because, as mentioned elsewhere in this white paper, it processes all of its customers' traffic inline and delivers zero trust everywhere, across workforces, branches, and clouds. In other words, it has a unique vantage point from which it can assess risk across the entire IT ecosystem—without the need for manual data aggregation or stitching reports together.

Risk360 automatically leverages real-time data from an organization's Zscaler environment as well as years of security research from ThreatLabz, Zscaler's world-class threat research team. It intelligently scrutinizes risk across 115 zero trust factors that range from GenAI usage and DLP policy configuration to the number of decoys or honeypots deployed across an organization. With all of this information, it quantifies risk holistically as well as for each of the four key steps of the cyberthreat attack chain: attack surface exposure, potential for compromise, possibility of lateral movement, and likelihood of data loss.

The solution offers intelligent cybersecurity maturity assessments that replace expensive consulting initiatives and give companies a better idea of how far along they are on their zero trust journeys. It also provides intuitive visualizations of risk and security posture, granular information about individual risk factors, financial exposure details, board-ready reporting, and actionable insights that can immediately be put into practice for superior risk mitigation.

With Risk360, organizations can systematically assess and minimize risk throughout their zero trust journey, reduce the administrative burden, and alleviate management overhead. In other words, this solution is yet another example of Zscaler's ability to secure and optimize organizations with the power of zero trust and AI.



Risk

Risk Events by Location

Top Risky Locations

Kansas	40%
Canada	20%
Netherlands	20%
Germany	10%
United Kingdom	10%

Contributing Factors by Entity

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

Third parties create risk related to lateral propagation and data loss

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

Assets create risk distributed across the four stages of breach

Top 10 Factors

Factor	Category	Your Score ↓	Last 30 Days	Entities	Licensed?	Recommended Actions
Application Segmentation	Lateral Propagation	5.00 / 5.00			N	Create application segments for 0
Private Application Traffic Inspection	Lateral Propagation	5.00 / 5.00			N	Implement private application insp
Device Posture Not Used in Access Policy Rules	Lateral Propagation	4.00 / 4.00			N	Implement device posture checks
Identity Protection – Entra ID	Compromise	2.97 / 2.97			N	Investigate risks identified in Entra remediations.
UEBA	Data Loss	2.40 / 2.40			N	Investigate users flagged with thes actions.
SCIM Groups Not Used in Access Policy Rules	Lateral Propagation	2.00 / 2.00			N	Implement SCIM groups in 0 acces
Application Segments with Open Ports	Lateral Propagation	2.00 / 2.00			N	Restrict ports for private applicatio
Internal Network Decoys Not Deployed	Lateral Propagation	2.00 / 2.00			N	Deploy internal network decoys an detection on these decoys.
Zero Trust Network decoys Not Deployed	Lateral Propagation	2.00 / 2.00			N	Deploy Zero Trust network decoys
Unscanned SSL Traffic	Compromise	1.96 / 1.96			N	Enable inspection for 100.0% qualit

Figure 8: The Risk360 dashboard

Zscaler Security Operations (SecOps)

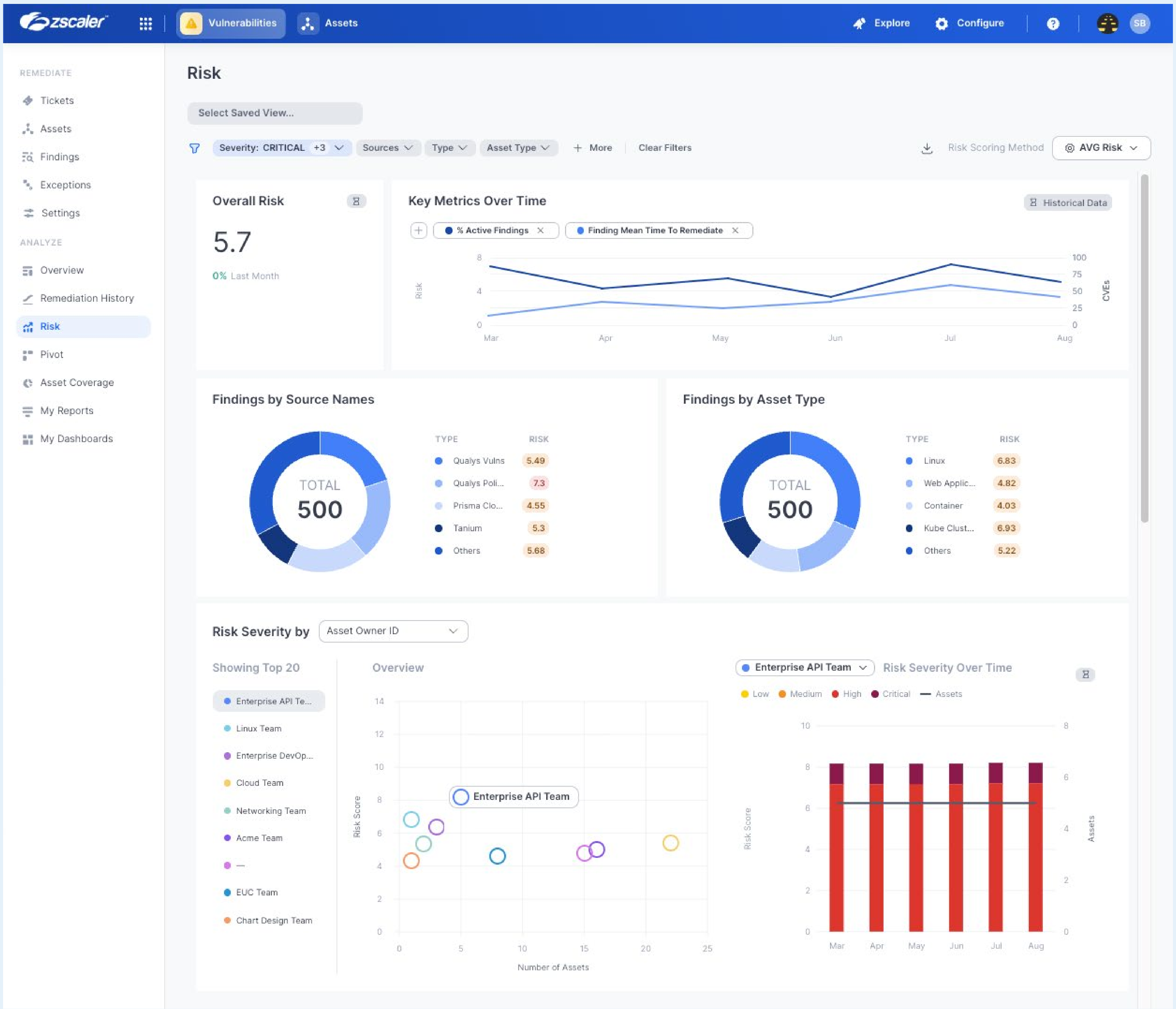
In today's fast-evolving cyber landscape, security teams are often hampered by fragmented tools and siloed workflows. Exposure management teams focus on identifying and reducing vulnerabilities, while threat management teams respond to emerging incidents—but they are typically disconnected, unable to share critical context and other data efficiently. This separation leads to redundant effort, blind spots in risk coverage, and missed opportunities for effective response. Without a joint foundation, organizations rely on outdated manual processes and patchwork spreadsheets that fail to provide a unified, actionable view of security posture.

Zscaler Security Operations (SecOps) fundamentally reimagines this paradigm. Built upon the powerful Zscaler Data Fabric for Security, it unifies exposure and threat management, breaking down silos and enabling holistic risk reduction. The Data Fabric for Security harmonizes data from sources throughout your environment: Zscaler telemetry, vulnerability scanners, endpoint detection tools, configuration management databases (CMDBs), cloud solutions, and beyond. Using advanced analytics and AI, the platform deduplicates findings, maps relationships, contextualizes assets, and seamlessly combines disparate inputs for transparent risk scoring and prioritization.

Zscaler's flagship SecOps solutions, Asset Exposure Management and Unified Threat Management, deliver transformational capabilities across the security operations lifecycle. With Asset Exposure Management, organizations gain a complete, real-time inventory of every asset in their environment, enabling them to quickly uncover risky and non-compliant assets and ensure that coverage gaps are closed. Unified Threat Management empowers teams to correlate exposures with active threats, prioritize vulnerabilities in full business context, and remediate top issues using customizable, bi-directional workflows that are integrated directly with ticketing and configuration systems.

With these solutions (and **others** in the Zscaler SecOps portfolio), AI-driven automation initiates risk mitigation policies as soon as issues are detected, saving time and reducing the likelihood of human error. For example, if an asset is missing an owner in the CMDB, Zscaler can automatically trigger an update based on data from other sources. Similarly, remediation tickets are grouped by what is needed to resolve them and are sent to the right team via the ITSM tools they already use. In addition, exception management, compliance tracking, and dashboard reporting are streamlined to provide CISOs, analysts, and managers with instant visibility and control.

By leveraging Zscaler Security Operations solutions and the Data Fabric for Security that powers them, organizations can finally eliminate operational silos, achieve true risk reduction, and build a resilient, unified security operations program that is ready to address today's challenges and adapt to tomorrow's threats.



TYPE	RISK
Qualys Vulns	5.49
Qualys Poli...	7.3
Prisma Clo...	4.55
Tanium	5.3
Others	5.68

TYPE	RISK
Linux	6.83
Web Applic...	4.82
Container	4.03
Kube Clust...	6.93
Others	5.22

Figure 9: Zscaler SecOps' Unified Vulnerability Management dashboard

Zscaler Digital Experience (ZDX)

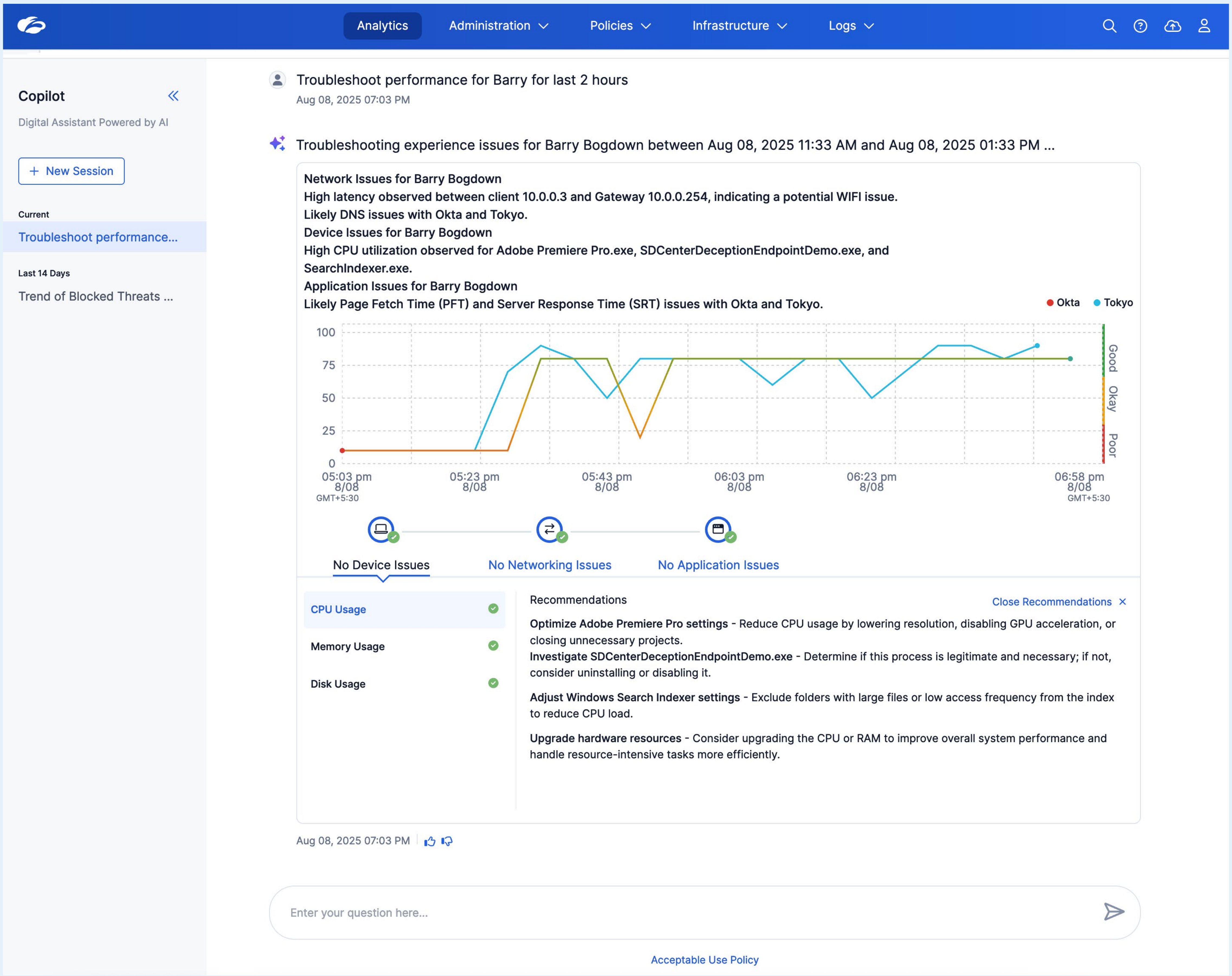
Digital transformation has shattered the traditional network perimeter, creating a complex constellation of ISPs, home Wi-Fi networks, unmanaged devices, and SaaS apps. For IT teams, this introduces two urgent challenges that impact business productivity:

1. **More failure points:** Every new cloud, network path, or device is a potential point of failure that can disrupt the user experience.
2. **Fragmented visibility:** Having disparate monitoring tools for devices, networks, and apps creates blind spots and requires manual correlation of data, slowing troubleshooting.

Zscaler Digital Experience (ZDX) was designed to master this modern complexity. By leveraging Zscaler's unique inline cloud proxy architecture, it provides complete end-to-end visibility—from any device, across any network, to any application. This eliminates blind spots and provides the high-quality, comprehensive data needed for transformative AI capabilities.

ZDX's AI engine uses its holistic visibility to transform network operations teams from reactive firefighting to proactive oversight, delivering:

- **Automated anomaly detection:** With the ZDX Incidents Dashboard, AI automatically correlates performance deviations across thousands of users, devices, and locations. It can detect a hidden problem—like a degraded ISP peer or a faulty Wi-Fi access point in an office—and proactively alert the NetOps team before support tickets are submitted.
- **Deep network intelligence:** When an alert is triggered, ZDX Network Intelligence provides AI-powered analysis of network paths and ISP performance. It visually maps connectivity, baselines performance of ISPs, and pinpoints the source of latency or packet loss, whether it's on the first, middle, or last mile.



Troubleshoot performance for Barry for last 2 hours
Aug 08, 2025 07:03 PM

Troubleshooting experience issues for Barry Bogdown between Aug 08, 2025 11:33 AM and Aug 08, 2025 01:33 PM ...

Network Issues for Barry Bogdown
High latency observed between client 10.0.0.3 and Gateway 10.0.0.254, indicating a potential WIFI issue.
Likely DNS issues with Okta and Tokyo.
Device Issues for Barry Bogdown
High CPU utilization observed for Adobe Premiere Pro.exe, SDCenterDeceptionEndpointDemo.exe, and SearchIndexer.exe.
Application Issues for Barry Bogdown
Likely Page Fetch Time (PFT) and Server Response Time (SRT) issues with Okta and Tokyo.

Recommendations

Optimize Adobe Premiere Pro settings - Reduce CPU usage by lowering resolution, disabling GPU acceleration, or closing unnecessary projects.
Investigate SDCenterDeceptionEndpointDemo.exe - Determine if this process is legitimate and necessary; if not, consider uninstalling or disabling it.

Adjust Windows Search Indexer settings - Exclude folders with large files or low access frequency from the index to reduce CPU load.

Upgrade hardware resources - Consider upgrading the CPU or RAM to improve overall system performance and handle resource-intensive tasks more efficiently.

Aug 08, 2025 07:03 PM

Figure 10: Zscaler Copilot responding to a prompt for ZDX

With the power of AI, ZDX also helps service desk teams to resolve tickets quickly and avoid unnecessary escalations. It provides:

- **Conversational AI for instant answers:** Instead of manually parsing logs, service desk teams can use Zscaler Copilot to resolve tickets in seconds. They can simply ask: "Troubleshoot Barry's issue with Google Drive in the last 2 hours." Copilot uses the ZDX AI engine to instantly analyze Barry's full digital experience chain and provide clear, actionable diagnosis.

- **One-click root cause analysis:** ZDX provides AI-powered root cause analysis that automatically pinpoints the underlying origin of any user experience issue with a single click. This lets L1 support guide users through a resolution, such as clearing a browser cache or disabling a problematic extension, without needing to escalate to NetOps.

By combining comprehensive visibility with targeted AI, ZDX transforms IT operations. The result is a dramatic reduction in MTTR, fewer escalations, and a more productive and satisfied user base.

Wrap-Up

The dual challenges of cyber risk and competitive pressure are more intense than ever before. To survive, organizations have to stop cyberthreats and data loss, as well as make sure that they are operating as efficiently as possible. Fortunately, the combination of zero trust and AI is a potent duo that is perfectly suited for addressing both of these challenges.

As the original pioneer and continued innovator in zero trust architecture, Zscaler systematically reduces risk for countless customers around the globe. Its Zero Trust Exchange platform boasts unprecedented scale and manifold integrations that foster strategic advantages in data and AI/ML. In other words, with Zscaler, you can secure and optimize your organization like never before.

If you would like to learn more about zero trust and why Zscaler is uniquely positioned to deliver on the promises of this modern architecture, register for one of the upcoming installments of our monthly webinar, "Zero Trust 101: Start Your Journey Here." It is part one of a three-part series that is designed to guide you throughout the entirety of your zero trust journey.

Or, if you would like to see the AI capabilities discussed throughout this white paper (and more), you can request a custom demo.

zscaler™

Zero Trust Everywhere