WHITE PAPER

Zero Trust + AI

Secure and Optimize Your Organization

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 organizations' 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 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 and machine learning (AI/ML). In a very short time frame, 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.

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, perimeter-based 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 perimeter-based security architecture with AI is like polishing a broken mirror—its sheen may improve, but it remains inherently flawed.

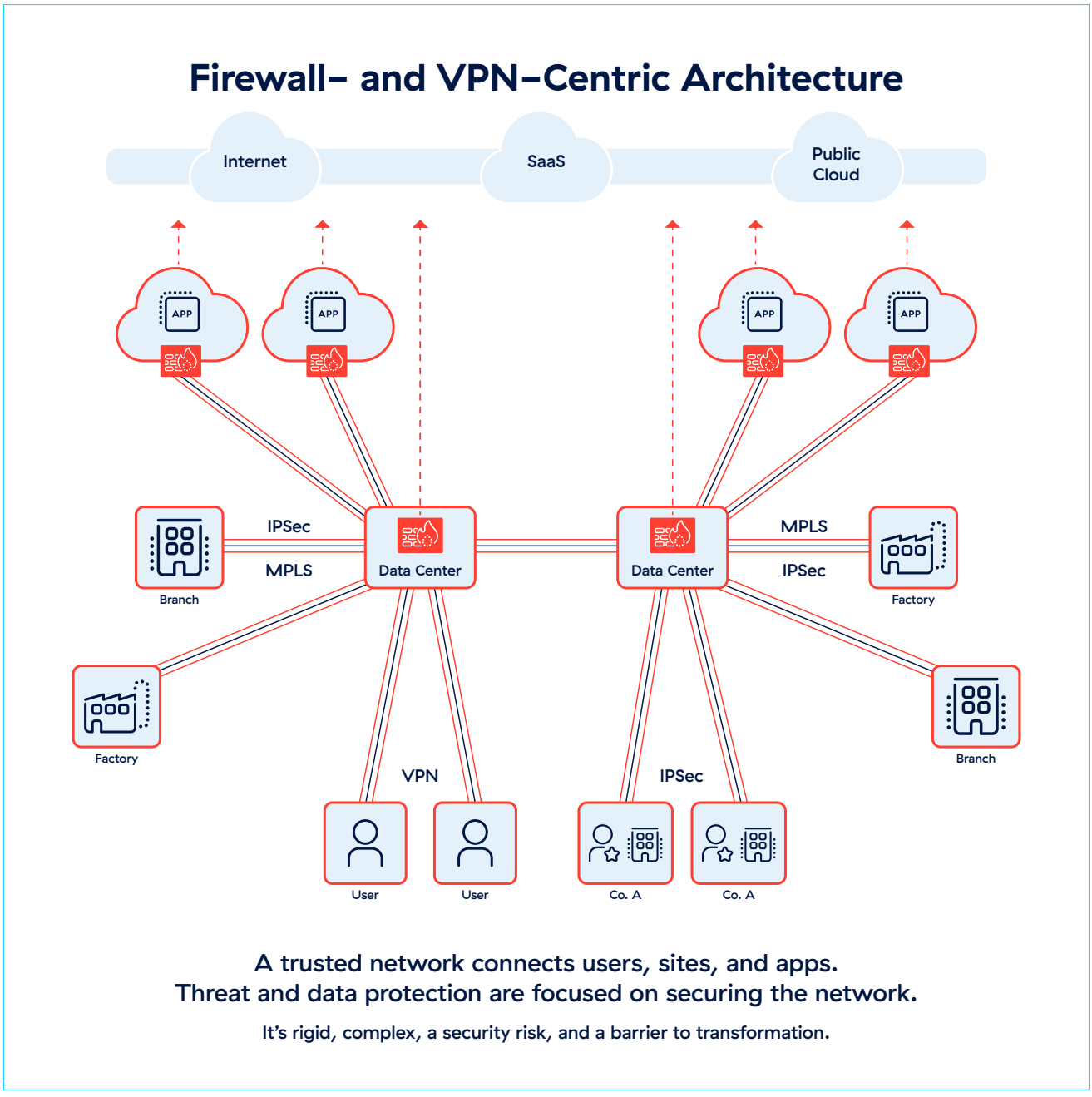

Figure 1: Perimeter-based architecture

Perimeter-based architectures built upon tools like firewalls and VPNs are focused on establishing a secure perimeter around an organization's hub-and-spoke network. This is why they are often called castle-and-moat security models. Perimeter-based 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 86% 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 an inability to scale and inspect encrypted traffic, and 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.

Early 2024 saw a slew of firewall and VPN vulnerabilities from **Ivanti**, **Cisco**, and **Palo Alto Networks**, highlighting the need to retire these tools and embrace zero trust architecture.

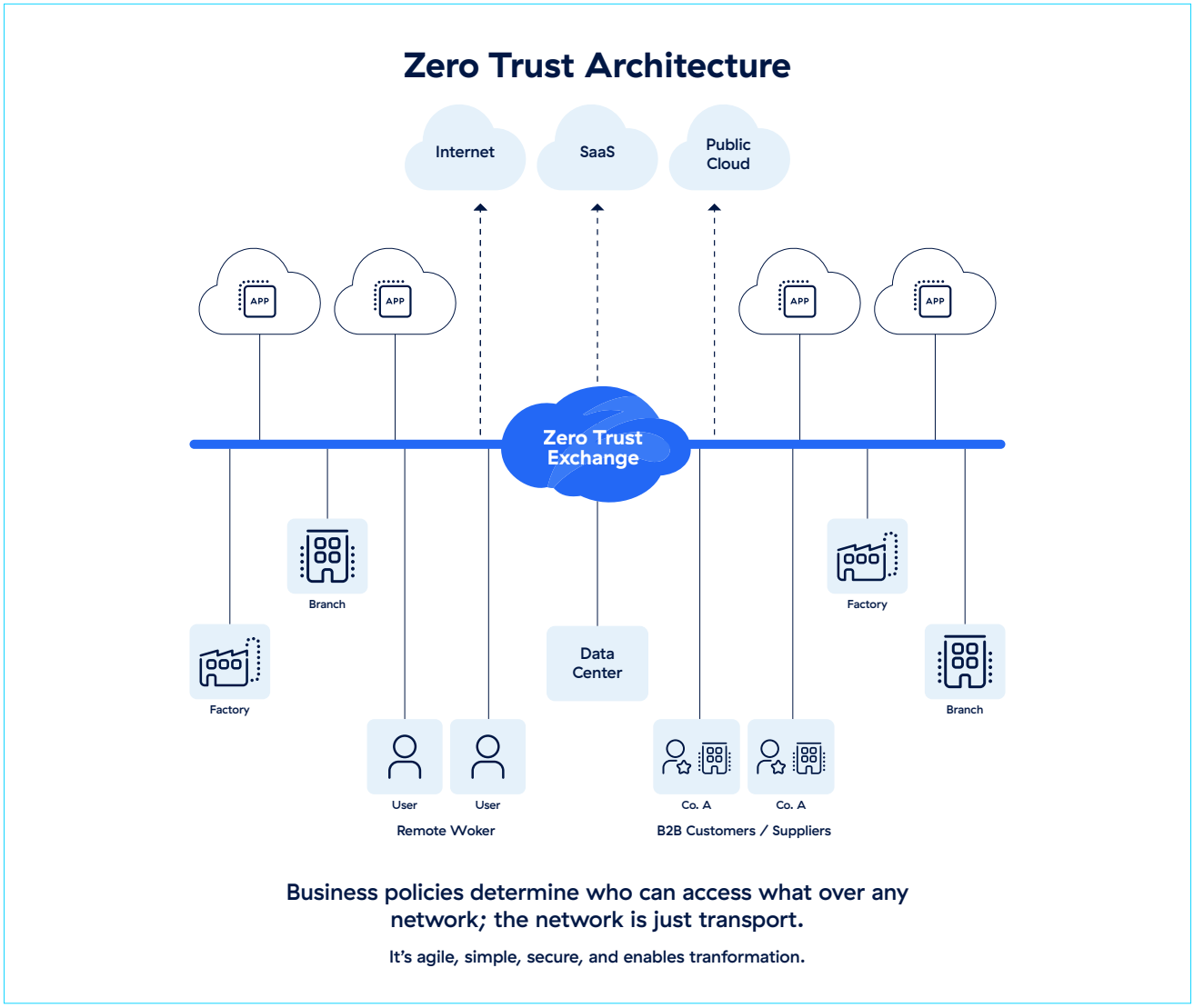

Figure 2: Zero trust architecture with Zscaler

As mentioned previously, zero trust is fundamentally different from perimeter-based architectures. Rather than being like a moat that protects a castle (the network perimeter), zero trust is like an intelligent switchboard that provides secure any-to-any connectivity in a one-to-one fashion—users are connected directly to apps instead of to the network as a whole. Context is used to determine who should be able to access what. In other words, Zscaler decouples security and connectivity from network access, and enforces the principle of least-privileged access. This zero trust connectivity (and a plethora of other functionality) is delivered as a service, at the edge, from the Zero Trust Exchange, Zscaler's high-performance, global security cloud. Backhauling traffic becomes a thing of the past.

With Zscaler, zero trust architecture:

- **Minimizes the attack surface** by stopping endless network expansion, eliminating the need for firewalls, VPNs, and their public IP addresses, and hiding apps behind Zscaler

- **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 users directly to apps they are authorized to access instead of to the network with its many connected resources
- **Blocks data loss**, whether malicious or accidental, across all data leakage paths, including encrypted traffic, cloud apps, and endpoints
- **Cuts cost and complexity** by simplifying networking with direct-to-app connectivity and by eliminating security point products with a comprehensive platform
- **Enhances productivity** by improving user experiences through direct-to-app connectivity 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.

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 inline security cloud, the Zscaler platform delivers secure connectivity as a service to thousands of organizations comprising more than 40 million users globally—not to mention countless workloads, IoT/OT devices, third-party workers, and more. As a result of this scale, Zscaler processes more than 400 billion transactions every day (more than 45 times the number of daily Google searches), as well as 500 trillion daily telemetry signals. Because Zscaler scrutinizes context in order to securely govern access to IT resources, there is rich data surrounding identity, device, content, destination, and network, for every access attempt. Additionally, Zscaler has a wealth of data from ThreatLabz, our internal, leading 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.

The Zscaler Data Fabric is further strengthened by more than 150 prebuilt integrations with a variety of security and business solutions. Security data sources include vulnerability scanners such as Tenable, Qualys, and Wiz, endpoint detection and response (EDR) solutions like CrowdStrike, identity management tools like those of Okta, Ping Identity, and Microsoft, and more than 60 threat intel feeds. Business data sources include SAP for cost and licensing data, Workday for organizational structure information, ServiceNow for configuration management database, and more. Zscaler ingests data from all of these sources, combines it with its proprietary data sets, deduplicates it, and enriches it. There is no need to manually aggregate data from multiple sources into one location—Zscaler handles the process automatically.

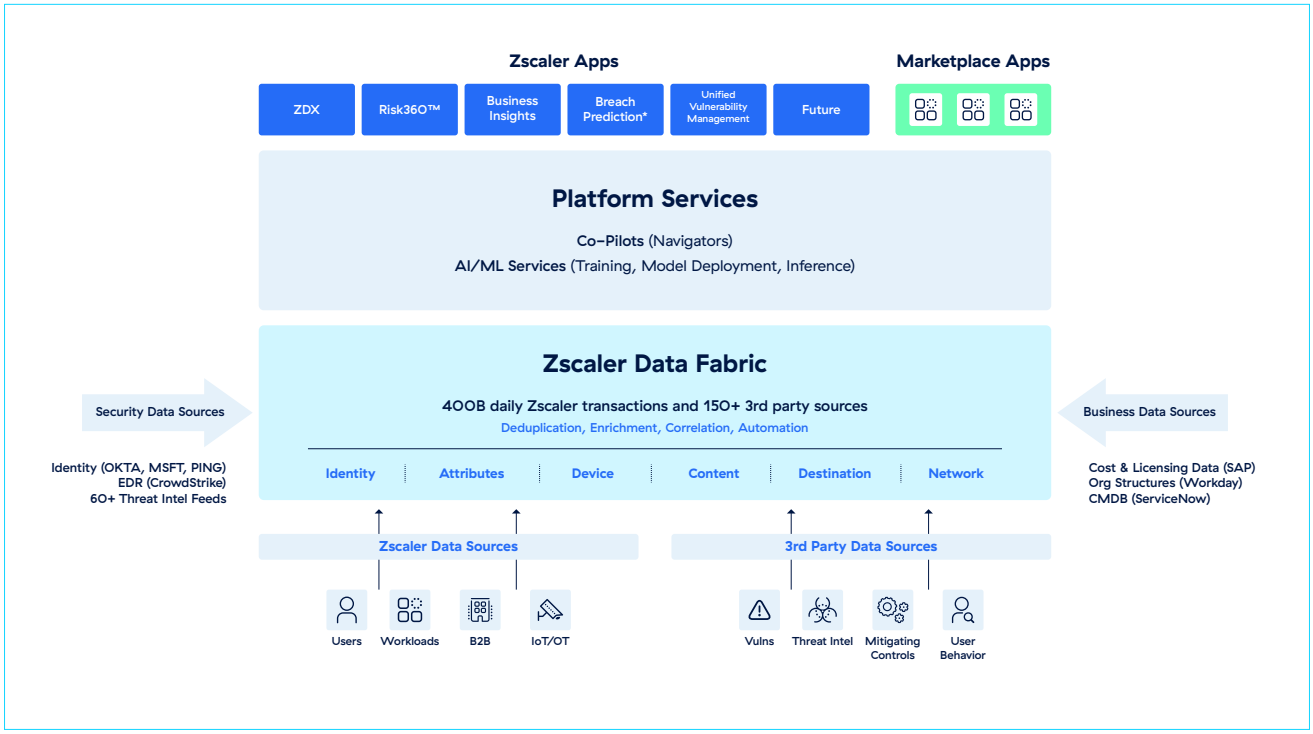

Figure 3: Zscaler's leadership and advantage in AI

With this massive, highly relevant 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 Your Organization with Zscaler

Zero trust architecture, in and of itself, significantly enhances security and decreases cyber risk by overcoming the weaknesses of perimeter-based architectures. However, combining the strength of zero trust architecture with leading, AI-infused security functionality further strengthens organizations' defenses against cybercriminals and advanced threats. Zscaler offers both zero trust architecture and AI-driven capabilities to reduce risk and, as an added benefit, enhance productivity for users and administrators alike.

Cloud Sandbox AI Instant Verdict

With the increasing sophistication of cyberthreats, organizations need real-time detection and mitigation capabilities. Otherwise, they can easily be compromised by clever cybercriminals with elusive, ever-evolving techniques. Sandbox technology is designed to detonate potentially malicious files in a safe environment, away from the user, to determine if said files are safe to access.

Unfortunately, traditional sandbox analysis methods inherently entail a tradeoff between security and productivity. If sandbox criteria are too lax, malicious files can make their way onto user devices and compromise the organization. If sandbox criteria are too strict, it is more likely that benign files will be sandboxed, user access will needlessly be prevented for several minutes, and productivity will be disrupted.

The Zero Trust Exchange breaks the sandboxing status quo and its innate security–productivity tradeoffs by leveraging the power of AI. The integration of ML into the cloud native Zscaler Sandbox ensures increased detection fidelity for customers, as the ML model has been trained and fine-tuned based on years of analysis and interactions with over 550 million file samples.

When admins enable the "AI Instant Verdict" setting with the click of a button, high-confidence malicious files with an AI/ML threat score of 91 to 100 are blocked automatically—without requiring the user to wait while the file is detonated elsewhere. This provides immediate protection against zero-day file-based threats while ensuring that users can stay productive. Additionally, instantly blocking high-confidence malicious files minimizes the number of potential patient zero incidents to investigate, reducing the workload for SOC teams and allowing them to focus their time on other critical security tasks. In other words, organizations can stay safe from evolving threats while ensuring that SOC teams and end users have their time optimized.

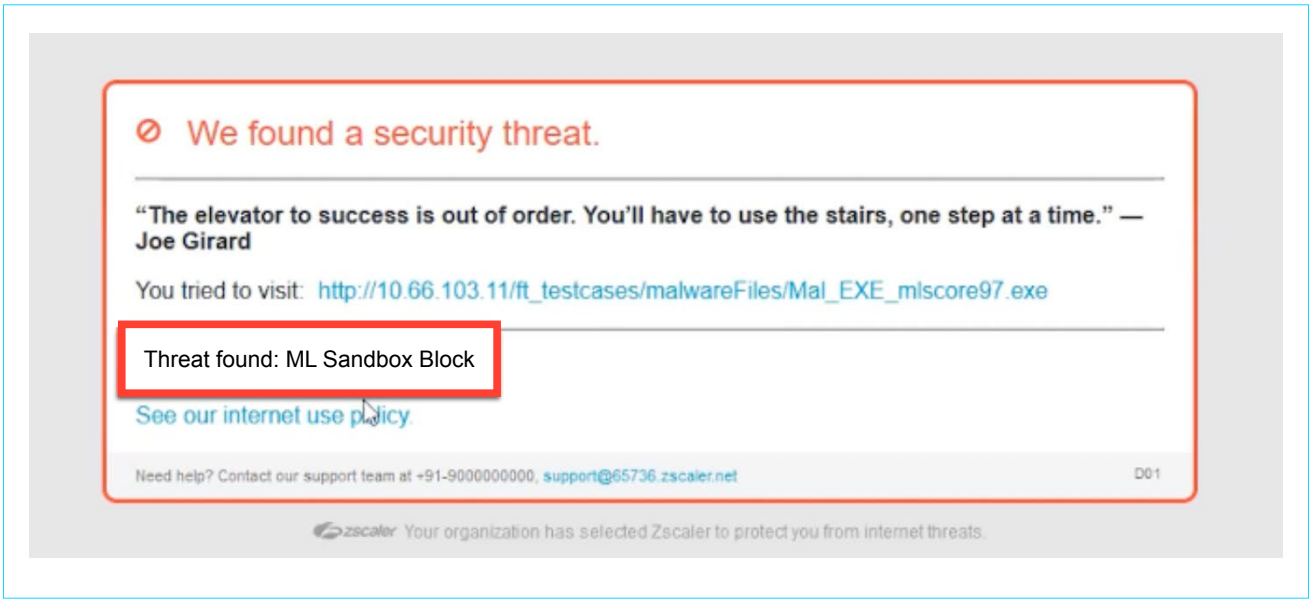

Figure 4: AI Instant Verdict user notification

Smart Browser Isolation

Cybercriminals use malicious websites to load dangerous content onto users' browsers and devices, creating beachheads for mounting their 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. Unfortunately, this approach has crucial weaknesses. First, trustworthy, time-tested websites can still unknowingly serve malicious content; for example, through advertisements or zero pixel iframes placed by cybercriminals. Additionally, blocking all newly registered domains disrupts user productivity by preventing access to new but legitimate web-based tools as well as existing, trustworthy websites that merely feature updated domains—in both cases, the resulting influx of help desk tickets disrupts IT's productivity as well.

Zscaler Smart Browser 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. 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 Smart Browser 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 pixels of the session are sent from the Zscaler cloud to the end user's device. The streams of images of the isolated session still give what appears to be the regular user experience, but the user does not interact directly with the website, so 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 the 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.

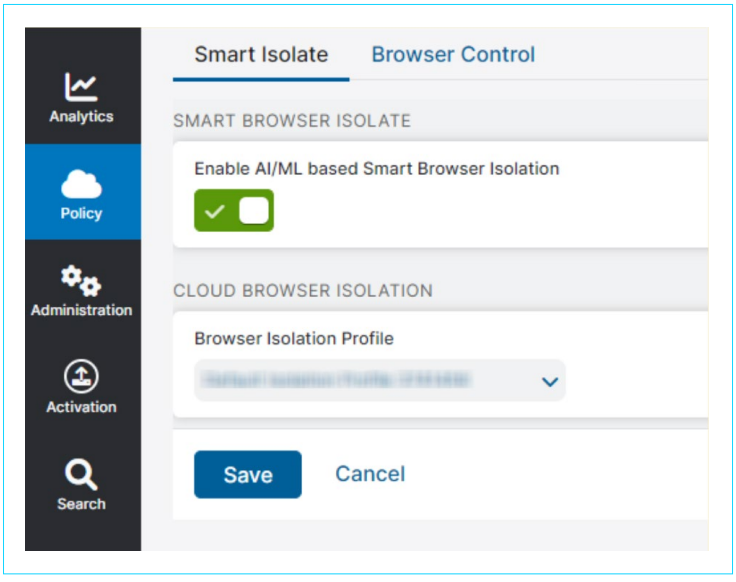

Figure 5: One-click enablement of Smart Browser Isolation

AI-Powered 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 App Segmentation. By harnessing artificial intelligence, Zscaler automatically creates ideal app segments for customers.

AI-Powered 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 App Segmentation represents a fundamentally different approach to segmentation. It accurately identifies and limits access to sensitive apps both proactively and automatically. By simplifying the segmentation process, it eliminates the complexities, errors, and risks associated with traditional methods. This, in turn, reduces the management burden of manual configuration, which saves time and resources for IT teams, enabling them to focus their efforts on other critical security tasks.

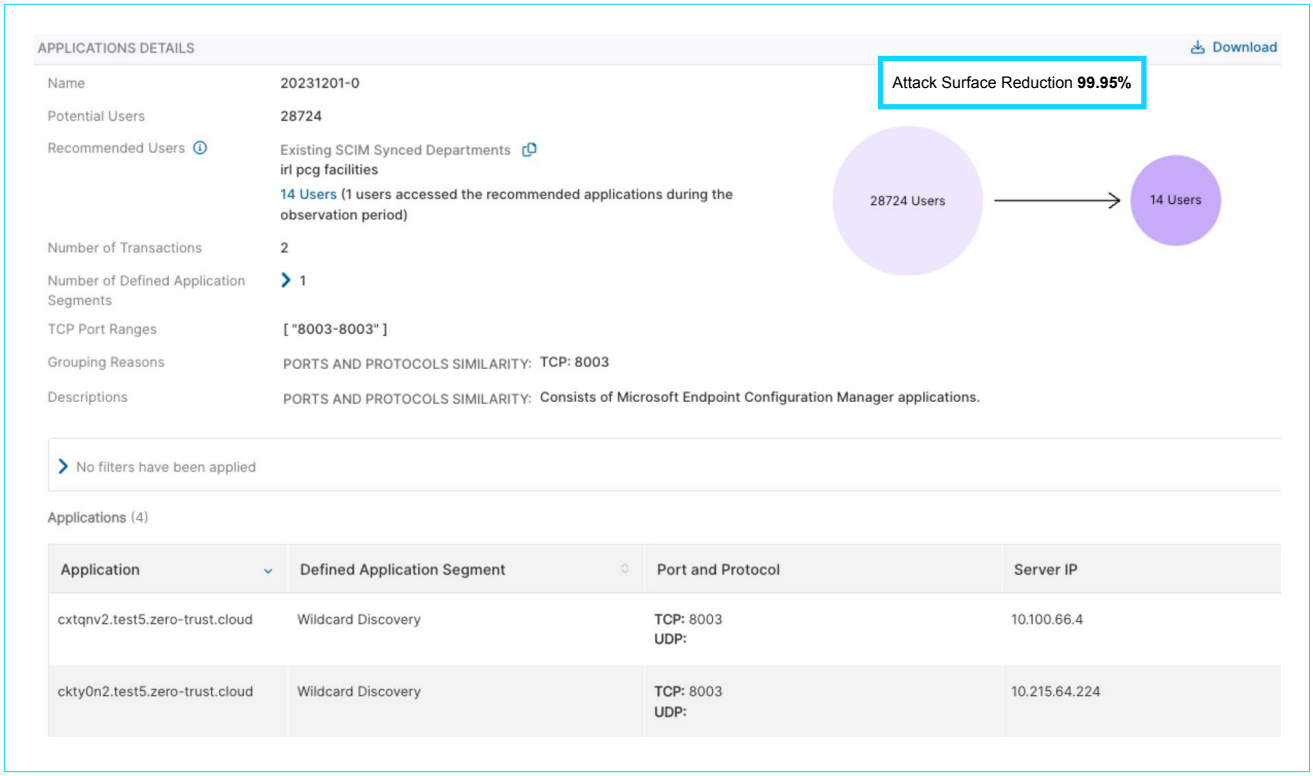

Figure 6: AI-Powered App Segmentation recommendation

AI 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 point products—separate network, cloud, web, and endpoint data loss prevention (DLP) solutions—to secure distributed data has proven to be ineffective. 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, 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 AI Auto Data Discovery, organizations can accelerate their ability to automatically find, classify, and control data as it is created and wherever it goes. Zscaler AI has been thoroughly trained to identify sensitive files and data in any context, whether that is at rest within SaaS, IaaS, or PaaS, in use on a user's endpoint, or in motion to the web via encrypted traffic. Admins don't need to duplicate rules across disjointed tools, or even configure dictionaries or data classification policies in Zscaler, to find sensitive data. The solution is comprehensive in reach and automated in execution, minimizing visibility gaps that other tools leave behind and cutting down on errors from manual rule creation.

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 Auto Data Discovery 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.

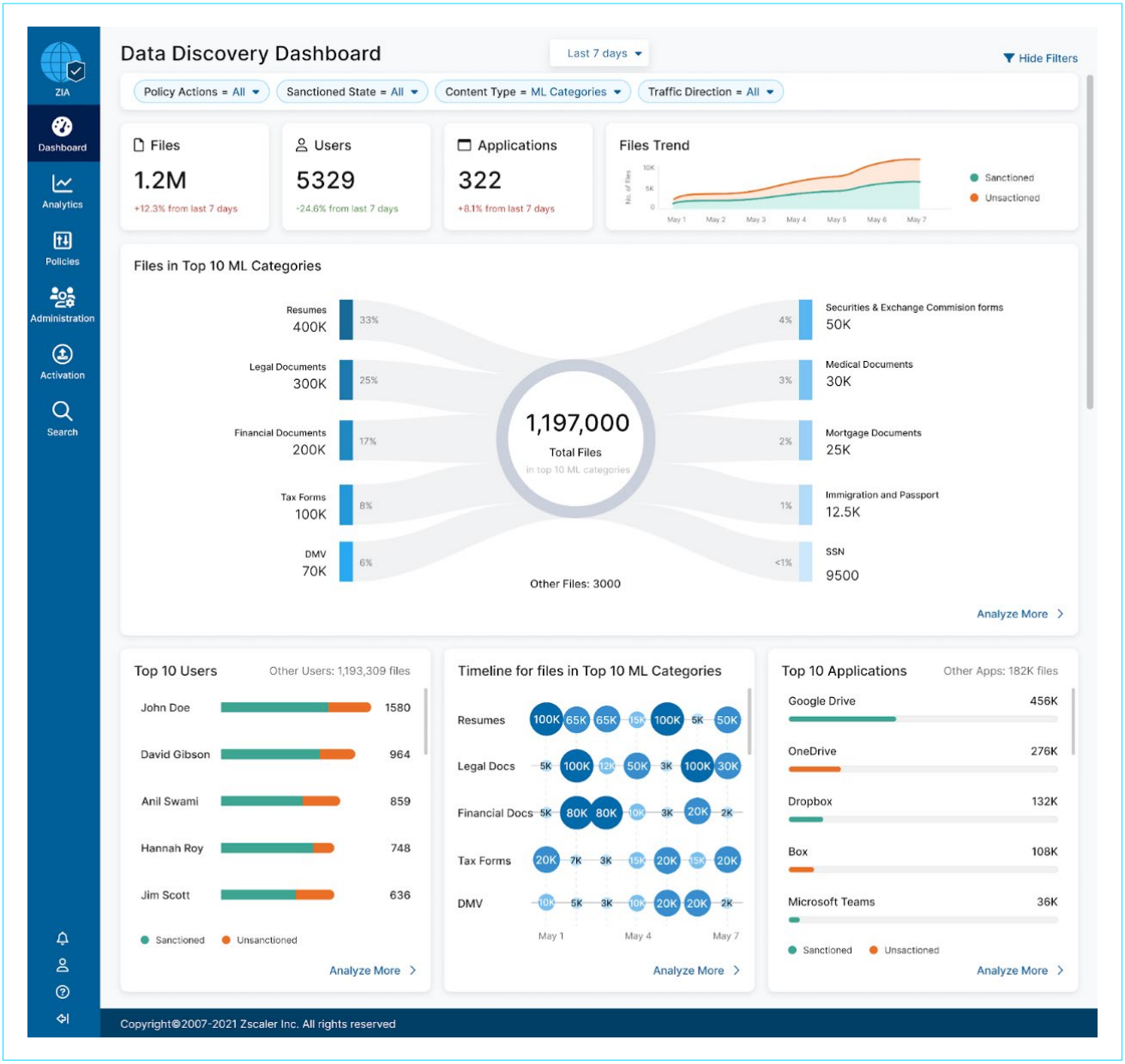

Figure 7: AI Auto Data Discovery dashboard

Optimizing Your Organization with Zscaler

The cloud-delivered Zscaler platform provides security and connectivity as a service, meaning that all customer traffic flows through the Zero Trust Exchange. Because of its unique inline perspective and prebuilt integrations with more than 150 security and business solutions, Zscaler can generate powerful insights and offer fully automated, real-time, AI-driven analytics and decision-making—without the complexity of data aggregation and collection. In other words, leveraging both zero trust and AI with Zscaler does more than enhance security: it also optimizes organizations in the following ways.

Zscaler Digital Experience (ZDX)

Users around the world are quick to embrace cloud applications and hybrid work because they provide superior flexibility compared to traditional, on-premises-only environments. However, digital transformation also creates a complex constellation of networking and routing links spanning the entire globe, ISPs, home Wi-Fi networks, employee-owned devices, SaaS apps, and more—much of which is outside the corporate network perimeter. As a result, this evolution creates two significant problems for any organization's productivity.

First, each new cloud, network, device, or location increases complexity and adds one more potential point of failure. As a result, digital experiences (and user productivity) are more likely to be interrupted. Second, multifaceted environments mean disjointed visibility into digital experiences. Device, network, and app monitoring tools used by different teams only see fragments of the app delivery chain. This leaves blind spots between the user's device and the app, and requires separate teams to manually export and correlate data from each tool. Consequently, help desk teams have to dedicate inordinate amounts of effort to resolve issues, wasting valuable time for them and the end user.

Zscaler Digital Experience (ZDX), part of the Zero Trust Exchange, was designed to address the above problems. By leveraging Zscaler's inline proxy architecture, ZDX has the necessary foundation to break down monitoring silos for devices, networks, and apps, and provide full end-to-end visibility into user experiences.

The solution uses the above visibility to fuel AI-powered root cause analysis, which automatically troubleshoots user experience issues, uncovers their underlying origins, and expedites resolution—with the click of a button. This same AI is leveraged by an incident dashboard that provides automated correlation to detect hidden problems impacting multiple users, whether issues stem from apps, Wi-Fi, ISPs, endpoints, or something else. More recently, ZDX added self-service for users. An AI engine running in the Zscaler Client Connector agent notifies users of issues like poor Wi-Fi or high CPU utilization and suggests ways they can resolve the issues themselves, without opening tickets. Finally, all of this functionality has been extended to natural language processing via ZDX Copilot, so admins can ask questions of a generative AI assistant that helps them automate tasks, draw digital experience insights, and perform deep analyses.

This potent combination of capabilities streamlines troubleshooting for IT teams and ensures that users receive the most productive digital experiences possible.

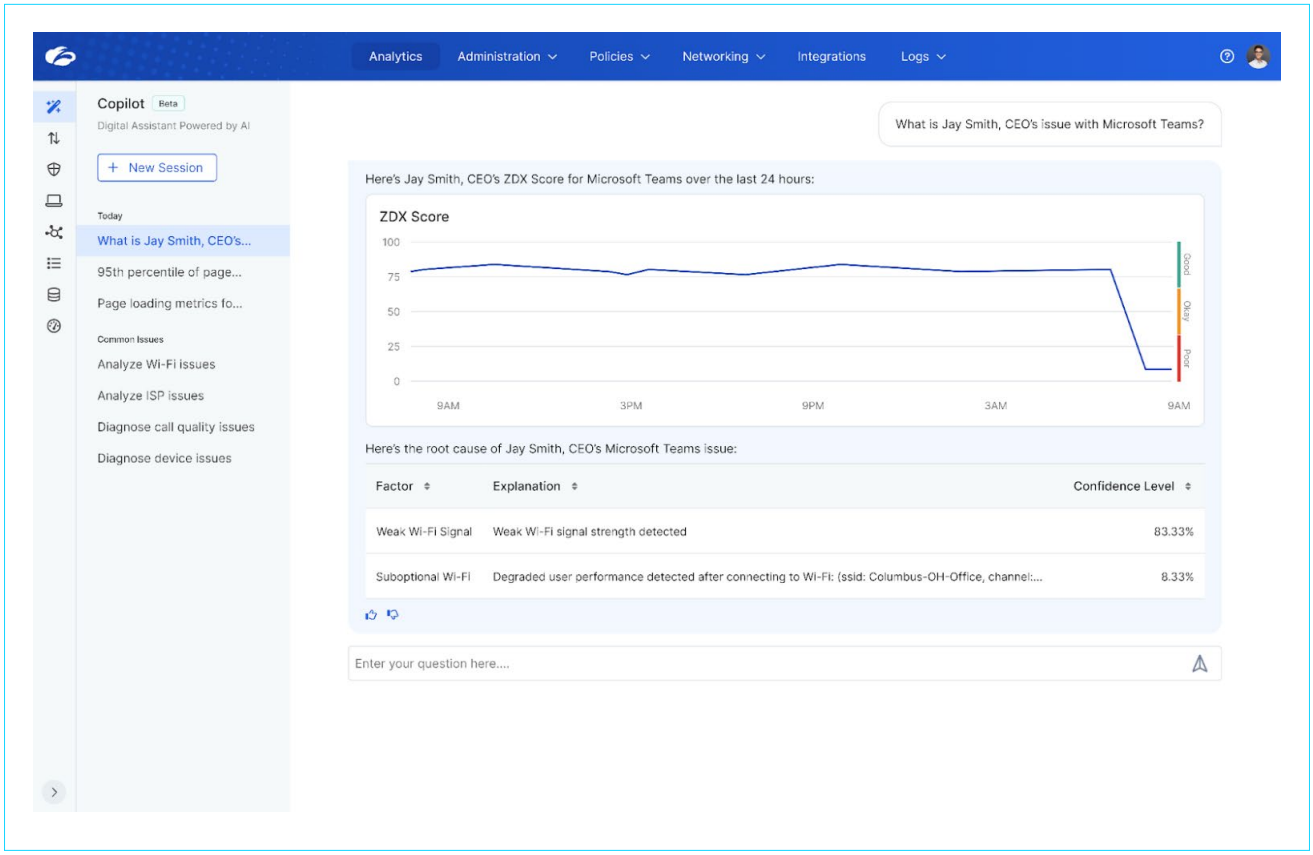

Figure 8: ZDX Copilot responding to a prompt

Business Insights

SaaS applications enhance productivity and flexibility for organizations. But the ease with which they can be deployed also creates challenges around managing and optimizing SaaS usage. Having separate licenses for redundant SaaS applications like Box, Dropbox, and Google Drive increases SaaS spend as well as operational overhead. Unused SaaS licenses and seats waste resources, as well.

Remote and hybrid work also serve as boons to employee flexibility and productivity. However, altering where work gets done inherently means that the traditional patterns of office utilization change significantly. As a result, organizations struggle to identify how they can best manage their use of office space—and resources and finances are inevitably wasted.

Organizations must gain visibility into their SaaS and office usage if they are to optimize their operations and eliminate unnecessary costs. But the usual ways of obtaining this visibility are often manual, time-consuming, and prone to inaccuracies. Siloed data and fragmented tools make it difficult for IT, procurement, and facilities teams to make informed decisions that drive savings.

Zscaler Business Insights provides organizations with accurate, comprehensive visibility into their SaaS apps and workplaces. This is done through the power of the Zero Trust Exchange, Zscaler's inline security cloud, which processes all customer traffic and can see who is working, where and when, and which resources they are using. Prebuilt integrations with business solutions like SAP and Workday enrich Zscaler data with information about cost, licensing, and organizational structure. AI leverages the combined dataset and enables functional leaders to make data-driven decisions that lead to more efficient resource allocation and spending.

For optimizing SaaS, Business Insights delivers complete visibility into application usage. It identifies redundant apps and provides insights about SaaS app engagement, plans and seats purchased, and active users. When it comes to workspace planning and optimizing the use of the office, Business Insights offers helpful information on office space trends, such as the days and times workers are on site, as well as which departments come into the office.

Business Insights allows organizations to make informed decisions so they can embrace SaaS and hybrid work more efficiently.

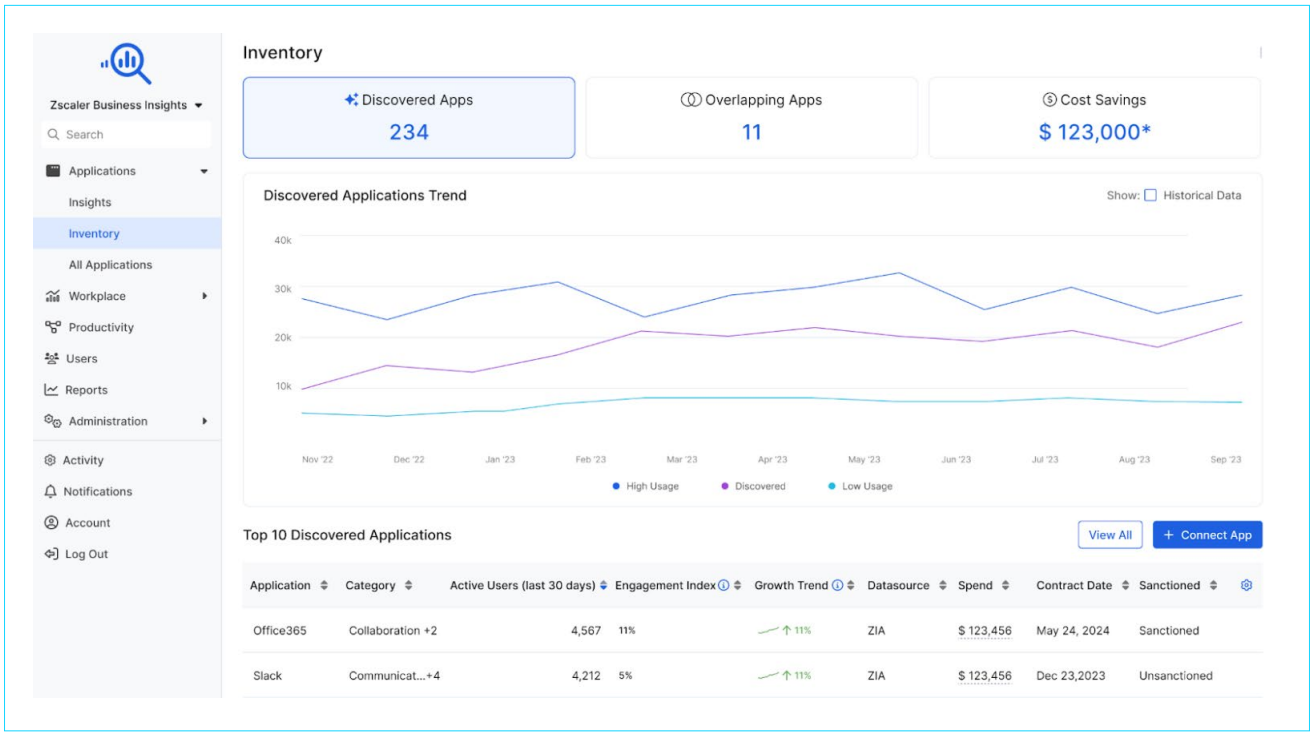

Figure 9: The Business Insights dashboard

Risk360

In today's rapidly evolving digital landscape, organizations are grappling with ever-increasing complexity and an ever-growing number of vulnerabilities. Making matters worse, cybercriminals are constantly refining their methods, embracing the latest malicious techniques, and enhancing the sophistication of their attacks. Traditional security tools and manual processes fall short in providing a comprehensive view of these risks. That's because siloed security dashboards and fragmented data make it difficult for security leaders to holistically assess and remediate risks effectively.

Compliance with security regulations adds another layer of difficulty. Organizations must provide evidence of sufficient risk management practices as part of demonstrating adherence to industry regulations. However, without a unified and integrated risk management framework, organizations struggle to map their security controls onto regulatory requirements, making it difficult to report on risk posture and exhibit compliance.

To understand risk and demonstrate compliance, security admins are tasked with aggregating information from various disjointed sources and building reports. But this painstaking, manual process wastes time and increases management overhead.

To address these challenges, Zscaler offers Risk360, a comprehensive and actionable framework that delivers powerful cyber risk quantification. Risk360 automatically leverages real-time data from an organization's Zscaler environment, external sources, and years of security research from the world-class Zscaler ThreatLabz threat research team. There is no need for manual data aggregation or stitching reports together.

Risk360 gives a holistic view of an organization's security posture and quantifies the risk associated with attack surface exposure, potential for compromise, possibility of lateral movement, and likelihood of data loss. It offers AI-driven 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. The solution provides intuitive risk visualizations, granular information about risk factors, financial exposure details, board-ready reporting, and actionable insights that organizations can immediately put into practice for risk mitigation. It also assists with security compliance through prebuilt mappings to frameworks like MITRE ATT&CK and NIST CSF, as well as reporting support for SEC Regulation S-K Item 106.

With Risk360, organizations can systematically assess and minimize risk, ensure regulatory compliance, 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.

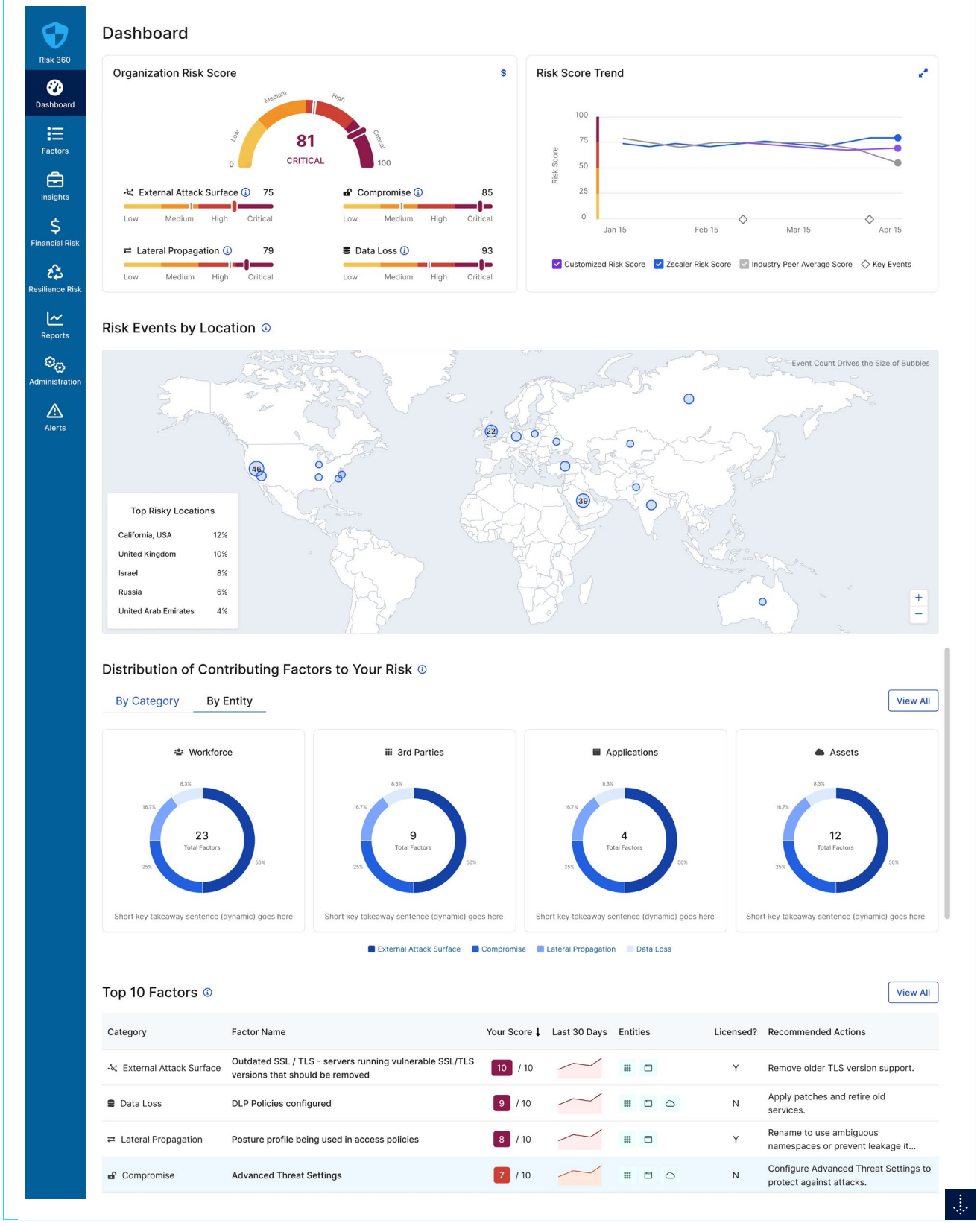

Figure 10: The Risk360 dashboard

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.

Four Points Technology

www.4points.com

sales@4points.com

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.