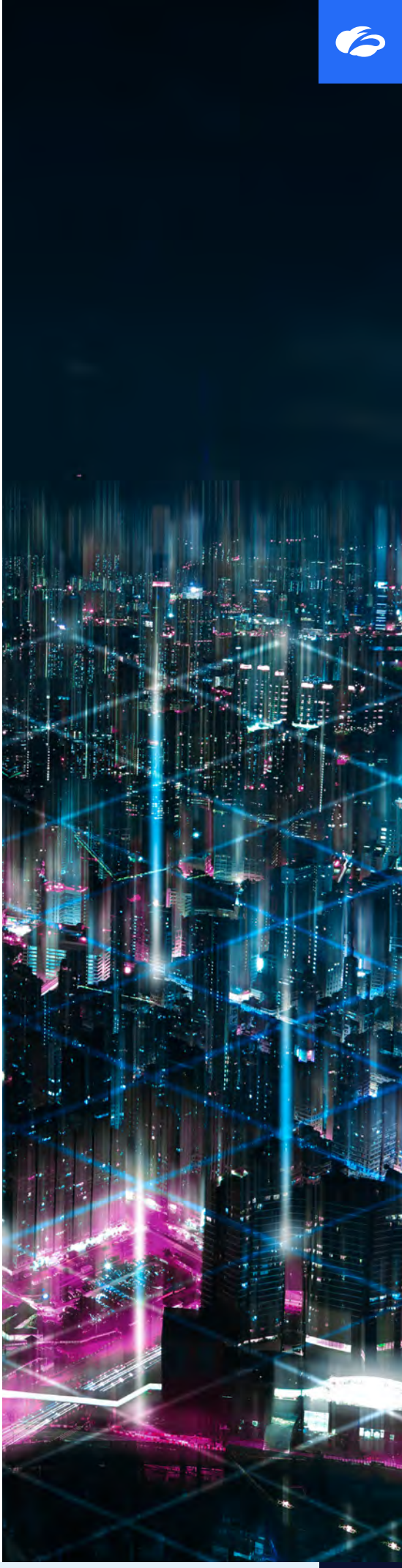
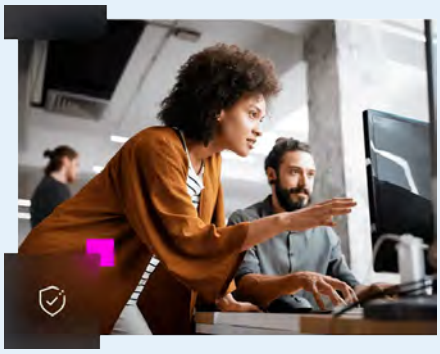
Zscaler G-Cloud 15

Service Definition Document

Contents



Secure, simplify and transform your enterprise with zero trust



Achieve superior protection

Stop cyberattacks, prevent data loss, and securely embrace AI

Increase agility and productivity

Accelerate branch deployments, cloud adoption, and M&A time to value

Reduce costs and complexity

Eliminate firewalls and point products, and slash infrastructure spend

Zscaler Overview

Zscaler is a global leader in cloud security, providing innovative solutions that help organizations securely transform for the digital age. Zscaler enables users, devices, and applications to safely connect, regardless of location, empowering businesses to embrace cloud and mobility with confidence.

Zscaler's cloud-native Zero Trust Exchange is the industry's largest inline security platform, providing scalable, high-performance protection and enabling organizations to confidently embrace digital transformation. Zscaler serves over 9,400 enterprise and public sector customers globally, including many of the world's largest and most respected brands. The platform processes more than 500 billion transactions and prevents over 150 million threats daily, leveraging a cloud-native network with data centres in over 150 locations worldwide.

Zscaler's mission is to make cloud and internet access safe, seamless, and reliable for every user and organization. By delivering security as a cloud service, Zscaler aims to eliminate the risks and complexities of traditional network security methods, enabling secure digital transformation on a global scale.

Objectives

- **Protect Users and Data Everywhere:** Deliver consistent, effective security for all users, devices, and applications, no matter where they are.
- **Enable Zero Trust Security:** Replace legacy perimeter-based approaches with identity- and context-driven access, reducing risks of breaches and unauthorized access.
- **Simplify and Modernize IT:** Streamline security operations, reduce reliance on hardware, and allow IT teams to focus on business outcomes.
- **Improve User Experience:** Provide fast, reliable, and secure access to apps and services, ensuring employee productivity and satisfaction.
- **Support Regulatory Compliance:** Help organizations meet industry regulations and protect sensitive data with robust compliance and monitoring capabilities.
- **Accelerate Cloud Adoption:** Facilitate secure migration and utilization of public cloud and SaaS services, unlocking agility and innovation.
- **Drive Continuous Innovation:** Stay ahead of evolving threats and technology shifts with relentless focus on research, development, and customer needs.

The Zscaler Zero Trust Exchange

Secure user, workload, and device communication between and within the branch, cloud, and data center.

Stop Cyberattacks	Secure Data	Secure AI	Automate Ops
Become invisible to attackers Prevent Compromise Prevent Lateral Movement	Find, classify, and Assess Data Security Posture Prevent Data Loss Across All Channels	Secure the Use of Public AI Secure Private AI Apps and Models Secure Agent Communications	Accelerate Security Operations Optimize Digital Experiences
Zero Trust Everywhere			

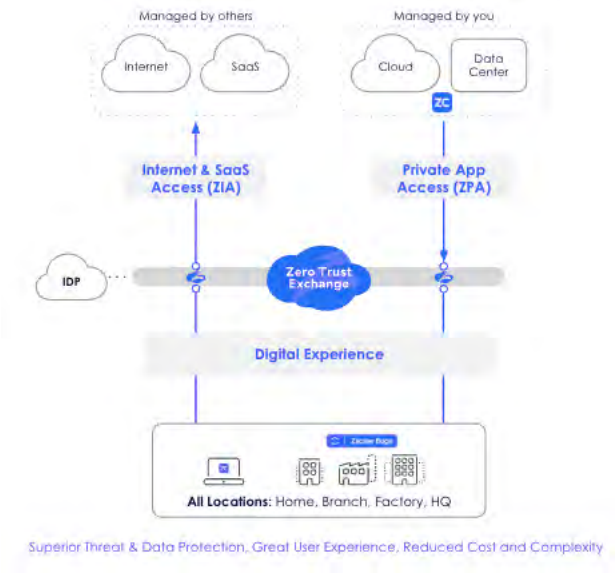
The Zscaler Platform provides solutions in 6 key areas:

- **Zero Trust for Users**
- **Zero Trust Branch**
- **Zero Trust Cloud**
- **Data Security**
- **Secure AI**
- **Security Operations**

Zscaler Zero Trust For Users

Overview

Zero Trust for Users is a cloud-native, AI-powered solution designed to protect users and data in today's highly distributed, cloud-first environments. It ensures that every connection between users and applications, whether SaaS, internet, or private-is continuously validated, context-aware, and tightly segmented. Unlike traditional perimeter models, Zscaler blocks threats, eliminates lateral movement, and stops data loss, all while optimizing end-user productivity and simplifying IT operations.



Key Features

- **Comprehensive AI-Powered Threat Protection:** Inline inspection of all user traffic (including encrypted/SSL traffic) across all ports and protocols. Advanced AI/ML engines block known and unknown threats, ransomware, phishing, and file-based attacks in real time.
- **Zero Trust Network Access (ZTNA):** Secure, direct access to private apps—without ever placing users on the network or exposing apps to the internet. Granular user-to-app segmentation stops lateral movement and reduces attack surface.
- **Agentless and Agent-Based Access:** Seamless connectivity for both managed (corporate) and unmanaged (BYOD, contractor, partner) devices via browser isolation and client-based access methods, enabling strong security for every access scenario.
- **Unified Policy Engine:** Single-pane policy enforcement for user, device, application, location, and risk posture—across web, SaaS, and private applications.
- **Cloud Browser Isolation:** Protects data and stops malware by isolating risky or sensitive sessions in the Zscaler cloud, enabling agentless, zero trust access for BYOD and B2B use cases without breaking user experience.
- **Data Protection (DLP and CASB):** Inline data loss prevention for all user traffic (web, SaaS, email); secure GenAI and SaaS app usage; identify, control, and protect sensitive data—at rest, in use, and in motion.
- **Digital Experience Monitoring:** End-to-end, AI-driven visibility and troubleshooting of user experience across devices, networks, apps, and ISPs, ensuring productivity and rapid issue resolution.
- **Privileged and Third-Party Access:** Secure, agentless, time-bound access for vendors, contractors, and partners—without VPNs or exposing internal resources, with comprehensive session controls.
- **Deception and Attack Surface Minimization:** Integrated deception technology to lure attackers and expose threats, with private applications hidden to external adversaries.
- **Rapid, Scalable Deployment:** Cloud-native architecture allows for deployment in hours or days, scaling seamlessly to thousands of users across regions.

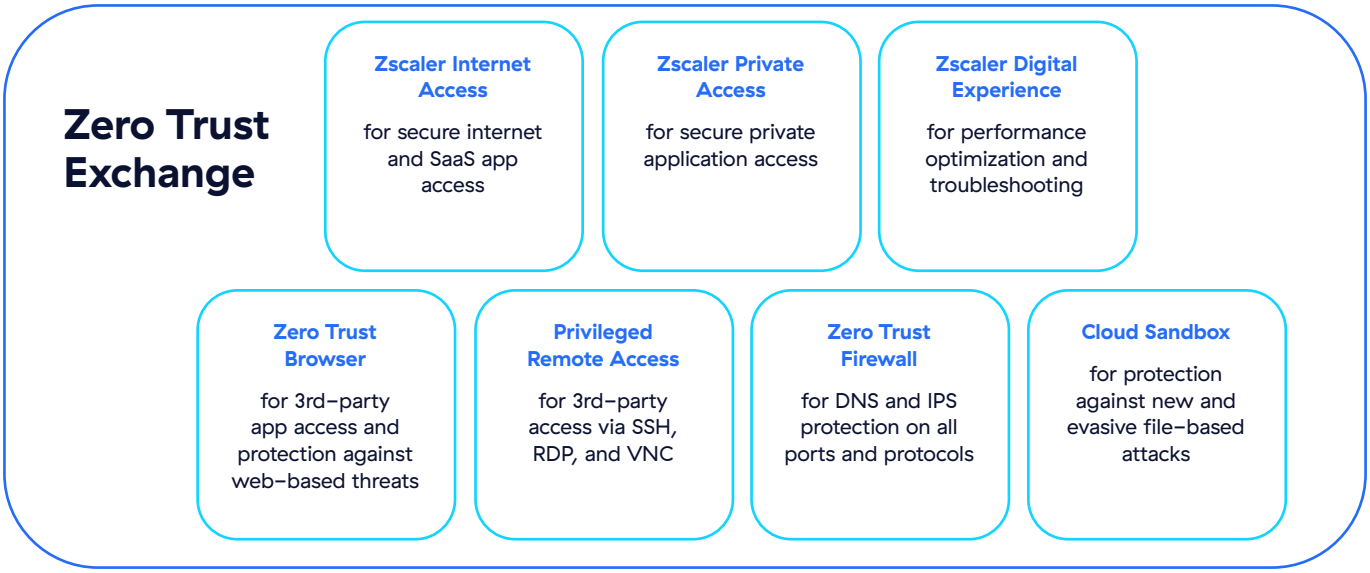
Use Cases

- **Replacing Legacy VPN and Firewalls:** Eliminate hardware VPNs and network firewalls for all users, including remote, hybrid, and branch location employees.
- **Securing the Hybrid Workforce:** Provide consistent, secure access and protection to users regardless of location—office, home, or on the road.
- **Enabling BYOD and B2B Access:** Grant contractors, partners, and employee-owned devices secure, monitored access to applications, without complex VDI setups or third-party browsers.
- **Protecting Data Everywhere:** DLP and CASB ensure sensitive information is safeguarded across email, SaaS, web, and GenAI tools, meeting compliance and privacy needs.
- **Accelerating M&A Integration:** Quickly onboard acquired businesses, users, and partners with secure access and unified policies, eliminating integration complexity.
- **Optimizing User Experience:** AI-driven digital experience monitoring and direct-to-app connections reduce support tickets and improve productivity.

Customer Benefits

- **Dramatically Reduced Attack Surface:** Applications are never exposed; users connect only to authorized resources. Zscaler eliminates lateral threat movement and legacy VPN/firewall vulnerabilities.
- **Superior Cyber Threat and Data Protection:** Real-time, AI-powered threat intelligence and comprehensive DLP stop ransomware, phishing, insider threats, and data loss—no matter where users or data reside.
- **Faster, Better Employee Experience:** Direct, optimal connections and proactive monitoring accelerate app performance and minimize downtime, boosting productivity.
- **Cost Reduction and Simplification:** Cloud-driven platform eliminates hardware, patching, and network management burdens, consolidating tools and lowering TCO.
- **Future-Proof Digital Transformation:** Rapid onboarding, flexible policies, and unified control adapt to cloud migration, remote work, business expansion, and regulatory change.

The Zscaler Platform provides everything required to connect all users to resources securely.

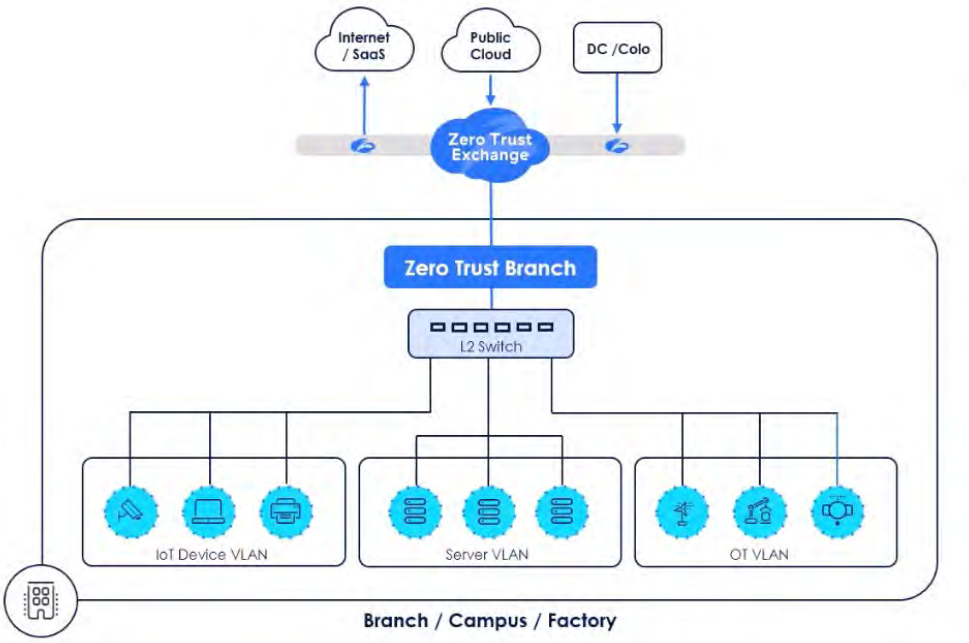


Zscaler Zero Trust Branch

Overview

Zero Trust Branch leverages Zscaler Zero Trust Exchange (ZTE) and integrated branch appliances deployed at branch sites to deliver secure, direct-to-cloud access and robust east-west security. It eliminates traditional VPNs and overlay routing, managing traffic forwarding across multiple ISP links for high availability and resilience. The solution ensures that all cloud and branch traffic is securely forwarded to the ZTE for inspection and granular access control based on user identity and traffic destination, preventing lateral threat movement within the network.

Zero Trust Branch: Café-like simplicity



Secure Internal & External Comms.

- Zero Trust connectivity between sites
- Zero Trust connectivity within the same site
  - Ring-fence every endpoint

VPN, NAC, and Firewall free Enterprises

- Eliminate implicit trust due to VPN
- Discover all branch assets
- Identify based restricted access

Café like simplicity for the Branches

- Eliminate multiple point products (VPNs, Firewalls, NAC, asset discovery, etc.)
- Eliminate complex network routes
- Manage from a single pane of glass

Key Features

- **Unified SD-WAN & Security Integration:** Combines high-performance Software-Defined Wide Area Network with zero trust principles to provide secure network and application access.
- **Agentless Device Segmentation:** Automatically discovers, classifies, and isolates every device (including IoT, OT, headless legacy devices) within the branch to prevent lateral threats without needing complex traditional segmentation solutions.
- **Direct-to-Cloud Architecture:** Enhances application performance and productivity by replacing complex site-to-site VPNs with direct cloud connectivity.
- **Comprehensive Security Inspection:** Applies Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) policies centrally to all branch traffic for secure internet and private app access.
- **Minimized Attack Surface:** Places private applications behind the Zero Trust Exchange, making them undiscoverable and inaccessible from the internet.

- **Plug-and-Play Deployment:** Includes Zero Touch Provisioning (ZTP) to simplify and speed up deployment.
- **Fine-Grained Policy Controls:** Enforces forwarding policies for internet and non-internet traffic with identity and application-based controls.
- **Enhanced Device Visibility:** Automatically discovers and classifies shadow IoT devices based on traffic profiles.
- **Clientless OT Access:** Simplifies secure access to operational technology resources via browser-based SSH, RDP, and VNC connections.
- **Resilient Network Architecture:** Terminates ISP connections at the branch and intelligently manages traffic forwarding for maximum availability.

Use Cases

- **Secure Branch Networking:** Protect all branch locations with unified, zero trust policies and inspect all traffic—including east-west (between devices at the branch) and north-south (from the branch to the cloud).
- **IoT/OT and Device Security:** Instantly discover, segment, and isolate potentially risky or legacy branch devices (e.g., IoT sensors, cash registers, HVAC controls) without traditional segmentation projects.
- **Direct and Secure Cloud Access:** Remove bottlenecks of backhauling traffic to data centres; users at branch offices get optimized, policy-enforced access to SaaS and private cloud applications.
- **Operational Technology Access:** Enable secure remote maintenance and monitoring of OT systems without exposing them publicly or requiring endpoint software.
- **Resilient, High-Availability Branch Connectivity:** Simplify multi-ISP management and ensure continuous, optimized access for both critical applications and users.

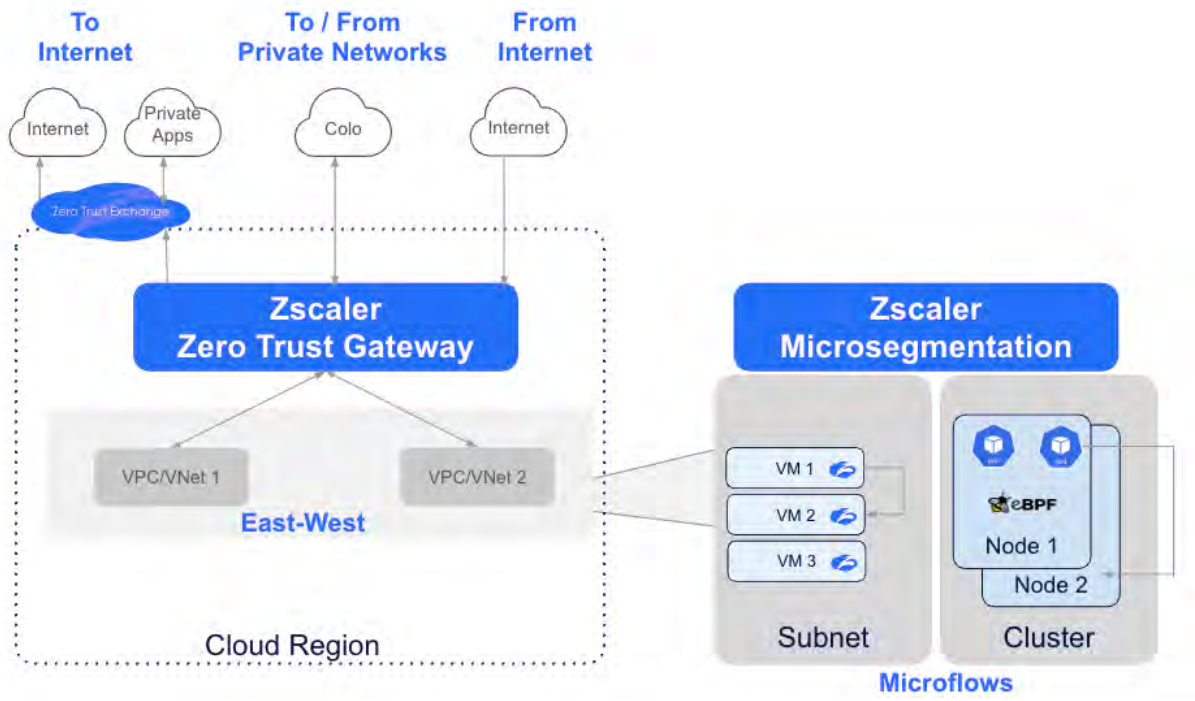
Customer Benefits

- **Zero Trust Everywhere:** Provides zero trust security for all users, devices, servers, and IoT/OT assets regardless of location.
- **Improved Application Performance:** By eliminating complex VPN overlays and routing, applications perform better with increased productivity for users.
- **Reduced Network Complexity and Costs:** Simplifies branch networking by removing the need for VPNs, firewalls, and complex routing.
- **Enhanced Security Posture:** Prevents lateral threat movement within and across branches and shields private apps from internet exposure.
- **Greater Operational Efficiency:** Automated device segmentation and Zero Touch Provisioning reduce operational overhead.
- **Flexible and Scalable:** Supports branches of all sizes from small offices to large campuses and data centres with seamless integration to the Zscaler cloud.

Zscaler Zero Trust Cloud

Overview

Zscaler Zero Trust for Cloud enables organizations to secure every traffic path for workloads, whether traffic is flowing east–west (between VPCs, VNets, subnets, or containers within/between cloud regions) or north–south (to and from the internet or data centres). The platform ensures that only explicitly authorized workloads can communicate, and all traffic is inspected for threats and data loss, regardless of location or cloud provider. This enables a consistent, powerful security posture for cloud migrations, hybrid IT, SaaS, and more—everywhere, at scale.



Key Features

- **Cloud-Native Zero Trust Gateway:** Secure workload traffic (ingress, egress, and lateral/E-W) using Gateway endpoints managed by Zscaler—a true SaaS experience that removes the burden of infrastructure deployment and maintenance.
- **Unified Policy Across Cloud and Data Centre:** Apply common security policies for data centres, public clouds (AWS, Azure, GCP), and SaaS environments. Support for macro- to micro-segmentation enables precise access control for every application and service.
- **Comprehensive Threat and Data Protection:** Inline inspection of all workload traffic with cloud-scale TLS inspection, advanced threat protection, and full data loss prevention. Blocks zero-days, malware, and unauthorized data movement.
- **Dynamic, Identity-Driven Segmentation:** Segment workloads and apply least-privilege access policies based on IP, FQDN, VPC/VNet, tags, and application context—limiting lateral movement and hiding resources from discovery.

- **Flexible Deployment:** Consume as a Zscaler-managed service (no VMs to manage) or deploy using Zscaler-provided cloud templates for greater control. Integrates seamlessly with native cloud constructs (Transit Gateway, GWLB, endpoints, and tags).
- **Scalable, Fault-Tolerant, and Fast:** Built on Zscaler's global cloud, supports auto-scaling and dynamic routes for large, multi-cloud environments—ensuring performance and reliability.

Use Cases

- **Secure Cloud Workload Egress (North-South Traffic):** Protect virtual machines (VMs), containers, and serverless instances accessing the internet or SaaS apps. Consistent policies and continuous threat/data protection for all outbound traffic.
- **East-West Security and Micro segmentation:** Prevent unauthorized lateral movement within and between cloud environments by segmenting and policing all workload-to-workload traffic.
- **Multi-Cloud and Hybrid Security:** Unify security policy and visibility across AWS, Azure, GCP, on-premises data centres, and colocation environments. Streamline M&A integration and secure hybrid IT at scale.
- **Mission Critical Application Protection:** Enforce strict access controls and data policies around sensitive apps (e.g., SAP S/4HANA), ensuring only verified workloads or users can connect, even during cloud transformation projects.
- **Cloud Data Loss Prevention:** Stop leakage of sensitive data from workloads with deep inline DLP and threat inspection for files, emails, and API calls.

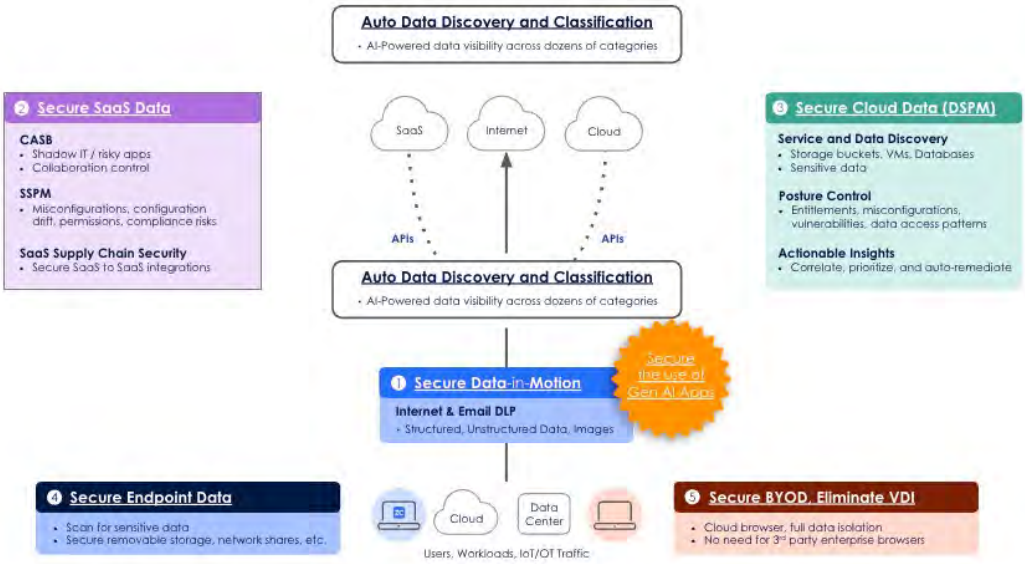
Customer Benefits

- **Reduced Operational Complexity and Cost:** Eliminate DMZs, firewalls, NAT gateways, and site-to-site VPNs, lowering both capital and operating expenses. No need to manage or maintain security VMs—Zscaler manages all gateway instances, auto-scaling, and updates for you.
- **Cloud-Consistent Security:** Uniform policies and visibility for all cloud and data center workloads, improving compliance and reducing human error risks. Achieve regulatory requirements (e.g., GDPR, HIPAA) with granular controls and audit-ready visibility.
- **Minimize Attack Surface:** Applications and resources are hidden from the internet and unauthorized workloads, drastically reducing the exposure to threats, zero-days, ransomware, and lateral movement.
- **Rapid Deployment and Scalability:** Secure thousands of workloads in minutes with simple deployment options and zero customer-owned infrastructure. Adapt quickly to business needs—new apps and environments are protected out of the box.
- **Operational Agility:** Enable fast, frictionless cloud migration, digital transformation, and M&A integration—security follows workloads wherever they go, always with the same powerful controls and visibility.
- **Lower Cost and Improved Resource Allocation:** Avoid over-provisioning for peak traffic, pay only for what you use, and leverage chargeback models for business units

Zscaler Data Security

Overview

Zscaler Data Security is a unified, cloud-native platform designed to discover, classify, and secure sensitive data wherever it resides or moves—on the endpoint, across the internet, SaaS, public cloud, email, and BYOD devices. This solution helps organizations proactively mitigate data exposure risks, enable business innovation (including safe adoption of AI), reduce attack surfaces, and simplify compliance in a hybrid, cloud-first world. By consolidating data protection into a single, AI-powered platform, Zscaler makes security easier, more effective, and less costly, especially as organizations confront data sprawl, regulatory pressure, and emergent risks like GenAI.



Key Features

- **Comprehensive Data Discovery and Classification:** AI-powered automatic discovery of sensitive data across endpoints, cloud, SaaS, email, web, and public cloud. Includes advanced classification (EDM, IDM, OCR) for structured, unstructured, and even image data—without requiring complicated manual rules.
- **Unified Data Loss Prevention (DLP) Across All Channels:** Real-time inline inspection and protection for data in motion (internet, email, SaaS, GenAI applications, etc.) and data at rest (endpoints, SaaS, IaaS), all managed from a single policy console. Ensures consistent enforcement across the organization—reducing gaps, false positives, and cost.
- **GenAI and Microsoft Copilot Security:** Deep visibility into all Generative AI use, including prompt capture and classification. Flexible, granular controls to allow safe, productive adoption of GenAI tools while preventing accidental or risky exposure of sensitive data. Seamless integration with platforms like Microsoft Copilot to control access, avoid data oversharing, and maintain compliance.
- **Endpoint DLP and Device Control:** Lightweight agent extends robust DLP to endpoints—protecting against data loss via USB, printers, personal cloud sync, network shares, etc.—even offline. Provides encryption, device inventory, and user coaching to drive compliant behaviours automatically.

- **SaaS and Cloud Security (CASB, SSPM, DSPM):** Unified CASB secures data in SaaS applications; SaaS Security Posture Management (SSPM) and Data Security Posture Management (DSPM) identify and remediate risks from misconfigurations and oversharing, governing both sanctioned and shadow IT apps and third-party integrations.
- **Advanced Workflow Automation:** Smart workflows automate incident response, alerting, and user/manager notifications, reducing investigation time and admin workload. Supports integration with ticketing and collaboration systems such as Slack, Teams, and ServiceNow.
- **Browser Isolation for BYOD and B2B:** Seamless, agentless isolation for SaaS and private applications allows secure access from unmanaged devices, ensuring no data is downloaded or copied to endpoints outside your control.
- **Centralized Policy, Visibility, and Reporting:** Consistent policy definition, enforcement, and reporting for all users, locations, and channels—backed by powerful analytics, incident dashboards, and SIEM integrations.
- **Compliance-Focused Architecture:** Support for regulatory requirements (GDPR, HIPAA, PCI-DSS, etc.) with role-based access, data residency controls, encryption in transit/at rest, and robust audit capabilities.

Use Cases

- **Proactive Data Discovery and Risk Mitigation:** Find sensitive data everywhere—cloud, endpoints, SaaS, public cloud—and remediate exposure risks before they become incidents.
- **Prevent Data Loss Across All Channels:** Block exfiltration via web, email, SaaS, USB, print, and more. Inspect all SSL/TLS traffic at scale with minimal performance impact.
- **Enable Safe Adoption of GenAI/AI Tools:** Discover shadow use of AI apps, capture user prompts, and apply DLP controls to prevent oversharing or regulatory violations by GenAI apps like ChatGPT or Microsoft Copilot.
- **Streamline and Modernize DLP:** Replace a patchwork of legacy DLP and point products with a unified, cloud-managed platform for lower costs, better coverage, and faster operations.
- **Simplify Compliance and Audit Readiness:** Centralize monitoring, reporting, and policy enforcement to efficiently demonstrate compliance—across cloud, endpoints, and everywhere data travels.
- **Secure BYOD and Third-Party Access:** Provide secure, restricted access to sensitive apps/data for contractors, partners, and personal devices—without complex VDI or risk of data leakage.

Customer Benefits

- **Complete Visibility & Control:** Gain real-time visibility into data flows, shadow IT, and sensitive information everywhere—including cloud platforms, endpoints, BYOD, and AI tools.
- **Reduced Business & Regulatory Risk:** Proactively identify, classify, and protect all sensitive data, minimizing data loss, reducing likelihood of breaches, and easing the compliance burden.
- **Modern, Cloud-Native, and Cost-Efficient:** Replace costly, legacy DLP point products with an integrated SaaS model, decreasing operational overhead and enabling rapid scaling—without new hardware or complex agents.
- **Faster Incident Response:** Automated workflows, advanced analytics, and centralized management lead to faster investigations, streamlined forensics, and less alert fatigue.
- **Empowered Business Innovation:** Safely accelerate digital transformation, cloud adoption, and GenAI initiatives—enabling productivity without sacrificing data security.
- **Proven ROI:** Customers report dramatic improvements—including full data risk visibility within weeks, fast ROI (e.g., up to $2.1M in annual savings), and 173% more incidents proactively identified vs. legacy solutions

Securely Embrace AI

Overview

The Zscaler GenAI Security portfolio empowers organizations to harness the productivity and innovation of generative AI—such as ChatGPT, Microsoft Copilot, and thousands of other AI/ML tools—confidently and securely. The solution is designed to help companies safely embrace both public AI (e.g., SaaS GenAI) and enterprise-managed private AI, providing advanced visibility, robust control, and comprehensive data protection to minimize risk while boosting business performance.

Zscaler Secure AI goes beyond simple blocking or allowing AI tools. It delivers fine-grained policies and real-time protection that allow you to:

- Find and govern shadow AI usage across your entire environment.
- Control and guide employees' use of sanctioned AI applications.
- Deploy powerful guardrails for data protection and compliance when leveraging public or private AI models.
- Safely accelerate business creativity and innovation.

Key Features

- **AI & GenAI Application Discovery:** Automatically identifies all AI and GenAI apps in use ('Shadow AI') by any user or department.
- **Prompt Capture & Classification:** Monitors prompts sent to GenAI apps; classifies them to understand sensitive context, intent, or potential risk.
- **Granular App Usage Controls:** Enforces fine-grained controls: allow, block, or isolate specific apps/users/departments.
- **Integrated Data Loss Prevention (DLP):** Inspects all GenAI app traffic and blocks sensitive content (PII, code, regulated data) from being exposed within AI prompts, responses, or uploads.
- **Browser Isolation for AI Apps:** Allows safe use of AI tools in a contained, secure browser environment. Prevent users from copying, pasting, uploading or downloading data where policy dictates.
- **Microsoft Copilot and SaaS AI Security:** Deep integration with MS Copilot and other SaaS AI agents to enforce labelling, correct permissions, and ensure safe use of AI via OneDrive and Purview labels.
- **Private AI App Runtime Protection ("AI Guard"):** Defends custom/private LLMs and AI apps against prompt injection, jailbreak attacks, PII/data leakage, and toxic or inappropriate outputs. Inline guardrails protect both prompts and responses and create a full audit log.
- **Comprehensive AI Inventory & Security Posture Management (AI-SPM):** Builds an inventory of all internal AI agents, models, data sources, and maps their risks (e.g., access permissions, vulnerabilities, supply chain). Assesses AI adoption against frameworks like NIST AI RMF and EU AI Act.

Use Cases

- **Shadow AI Discovery & Risk Mitigation:** Identify every GenAI/AI tool in use (including unsanctioned ones) and what data they're accessing.
- **Control & Enable Safe GenAI Usage:** Allow approved AI apps but block/limit risky user actions (uploads, downloads, pastes, etc.).
- **Prompt Inspection and Data Loss Prevention:** Monitor prompts and uploads in real time; block sensitive data or noncompliant use.
- **Coach and Educate End Users on AI Risk:** Automated user notifications and workflow automation guide users on best GenAI practices.
- **Copilot and SaaS AI Security:** Ensure Microsoft Copilot and other workplace SaaS AIs don't access or share sensitive data inappropriately—manage permissions, label hygiene, and control over-privileged access.
- **Runtime Protection for Private AI:** Guardrails for enterprise-built AI models and chatbots; defend against prompt injection, adversarial attacks, PII leakage, malicious URLs, and off-topic/toxic outputs.
- **Comprehensive AI Security Posture Management (AI-SPM):** Inventory, assess, and remediate AI & data risks across your enterprise, support for NIST AI RMF and regulatory compliance.

Customer Benefits

- **Accelerate Innovation Securely:** Enable safe, policy-driven use of GenAI to unlock productivity and creativity without putting sensitive data at risk.
- **Close Shadow AI Gaps:** Automatically find and control all unsanctioned AI usage; mitigate business risks of ungoverned AI.
- **Granular, Real-Time Data Protection:** Block sensitive or regulated data from ever reaching risky GenAI tools, with DLP that works everywhere—web, SaaS, endpoints, email, and private AI.
- **User Empowerment and Policy Flexibility:** Allow the business to use AI/GenAI wherever appropriate, but with robust guardrails and user coaching.
- **Full Visibility and Compliance Readiness:** Audit every AI interaction, prompt, response, and related data movement to support compliance and governance (GDPR, HIPAA, EU AI Act, NIST AI RMF, and more).
- **Secure Private and In-House LLMs:** Defend custom and internal AI models in runtime from adversarial misuse, data leaks, malicious URLs, and noncompliant outputs—prevent prompt injections and ensure business-aligned operation.
- **Faster, Unified AI Security Operations:** Incident workflow automation and integrated reporting reduce investigation time and operational overhead.

Security Operations

Overview

Zscaler's Security Operations offerings are designed to transform traditional security operations into a unified, cloud-delivered, and AI-powered function, enabling security teams to achieve greater efficiency, faster response, and better risk management in dynamic digital environments. The solution brings together best-in-class threat detection, automated response, and asset risk visibility under one platform, making it easier to defend against advanced threats while simplifying operational complexity.

Key Features

- **Next-Gen, AI-Powered Threat Detection and Response**
  - Leverages Zscaler's cloud-native Data Fabric for Security, machine learning, and Agentic AI to detect, correlate, and respond to threats—across all users, devices, and assets.
  - Enhanced by innovations such as Managed Detection & Response (MDR) from Red Canary, ensuring rapid incident handling and superior detection.
- **Automated Remediation Workflows:** Streamlines repetitive tasks and response activities, freeing SOC teams to focus on complex investigations.
- **Unified View of Security Posture:** Integrates context-rich data from Zscaler and third-party sources, offering real-time, centralized visibility and metrics across the enterprise attack surface.
- **Asset Exposure Management (AEM):** Collects and tracks asset data, inventories coverage, and identifies risk across on-prem, cloud, and remote environments. Enables policy definition and rapid remediation of violations.
- **Unified Vulnerability Management (UVM):** Centralizes vulnerability tracking, prioritization, and remediation, simplifying exposure management within the SOC.

- **Open API Integration:** Seamlessly connects Zscaler SecOps telemetry with leading SIEM, EDR, and third-party security tools for orchestrated analytics and response.
- **Real-Time Identity Attack Surface Monitoring:** Identity Threat Detection and Response (ITDR) delivers visibility into Active Directory (AD) and identity risks, alerts on credential misuse, and strengthens Zero Trust policies.
- **Data Fabric for Security:** Harmonizes, enriches, and correlates security data for actionable insights and AI/ML-driven analytics.

Use Cases

- **Transform SOC Operations:** Replace siloed, manual threat detection and triage with automated, AI-driven workflows for faster, more accurate incident response.
- **Reduce Attack Surface & Risk:** Identify and remediate vulnerable assets, misconfigurations, and risky user permissions across the enterprise—closing exposure gaps proactively.
- **Streamline Compliance:** Centrally manage security policies, reporting, and audit trails—making regulatory adherence and risk quantification more efficient.
- **Accelerate Cyber Threat Response:** Leverage MDR, automated playbooks, and unified data flows to act rapidly on detected threats, minimizing business impact.
- **Simplify Security Tooling:** Consolidate legacy solutions into a single, cloud-managed platform; unify asset risk, security posture, and remediation workflows.

Customer Benefits

- **Greater SOC Efficiency:** Automate routine tasks, reduce alert fatigue, and enable security analysts to focus on high-value investigations.
- **Faster Mean Time to Resolution:** AI-powered correlation and workflow automation slash the time from threat detection to full remediation.
- **Comprehensive Risk Visibility:** Real-time dashboards and risk scoring for assets, users, and vulnerabilities across all environments.
- **Reduced Complexity & Costs**
  - Eliminate redundant tools and manual processes, lowering TCO and IT overhead.
- **Future-Ready Security Operations:** Adapt quickly to new threats and technology shifts with scalable cloud innovations, continuous AI research, and integration flexibility.