DATASHEET

aperon

Identity-centric Security Service Edge (SSE) Platform



Problems of Modern Enterprises

Modern enterprises have increasingly become vulnerable to cyber-attacks due to a significantly expanded attack surface — driven by hybrid work environments, widespread cloud adoption, and the use of personal devices. Traditional security models can no longer keep up. Without a robust Zero Trust Architecture, organizations remain exposed to risks such as misconfigurations, insider threats, and other evolving attack vectors. There are four major vulnerabilities commonly found in enterprises that make them prone to breaches.

1. **Use of passwords** for accessing applications, cloud workloads and network devices makes enterprises prone to credential phishing attacks.
2. **No control on unmanaged devices** (personal devices, BYOD from third-party users) that are accessing enterprise SaaS apps like GSuite, Microsoft 365 or Custom cloud apps.
3. **VPNs used for remote access** to on-premise applications or servers are outdated and pose serious security risks.
4. **Without proper visibility and control, data** in cloud applications becomes vulnerable to unauthorized access or leakage.

Legacy Solutions Can't Secure Modern Enterprises

Traditional Identity & Access Management solutions, Firewall & VPN have several shortcomings.

1. **Use of passwords & traditional MFA** are prone to phishing attacks.
2. **Identity & Access Management** tools are not built for security
3. **Cloud apps** are vulnerable to **data leaks**
4. **Firewalls** don't secure web outside corporate network
5. **VPN** exposes entire network and doesn't secure SaaS apps

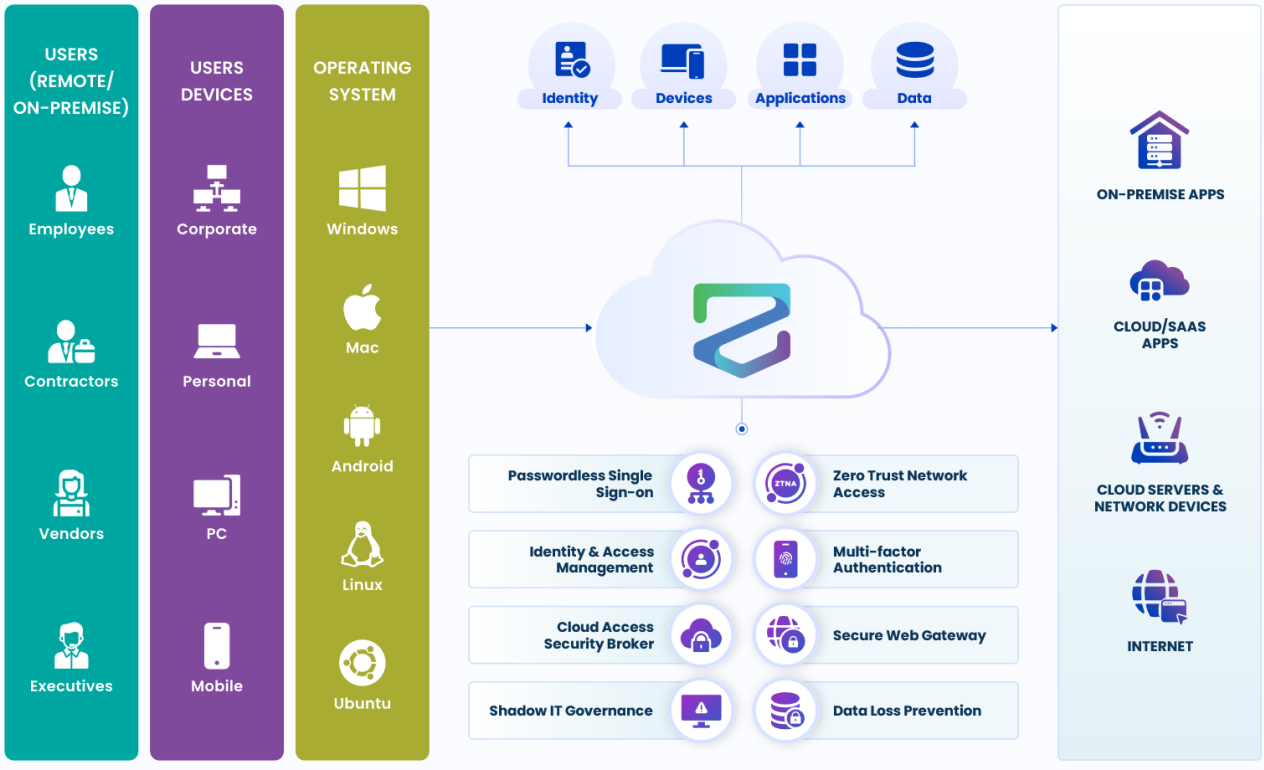
How Zaperon Secures Enterprises?

Zaperon is an Identity-centric Security Service Edge (SSE) platform that is built for modern enterprises and protects them from cyberattacks by securing access to their applications, data, cloud infrastructure and network devices from users and devices connecting from any location or network.

At the core of Zaperon's architecture is its identity-first approach, which combines Public Key Infrastructure (PKI), least-privilege access control, and dynamic Zero Trust access policies. Every user and device attempting to access enterprise resources is continuously authenticated and authorized based on multiple factors such as PKI-based digital certificates, user & device identities, user behavior and device posture. By default, access is denied unless explicitly granted. If any anomaly in user behavior or device posture is detected, Zaperon proactively terminates the session and blocks further access in real time — minimizing exposure and saving enterprises from costly breaches and downtime.

Beyond secure access, Zaperon extends its protection to enterprise data across endpoints and cloud environments. The platform prevents data leakage from endpoints by blocking various leakage points including USB, Bluetooth, airdrop, uploading on cloud apps or blocking screen capture. Even data in cloud applications are secured from unauthorized access and download. Access from unmanaged or BYOD devices is also governed.

What makes Zaperon stand out is its unified SSE platform that brings together Zero Trust Network Access (ZTNA), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Identity and Access Management (IAM), Multi-factor Authentication (MFA), PKI-based Passwordless Authentication and Shadow IT governance into a single, seamless solution. It offers centralized visibility and control to IT and security teams, enabling them to simplify operations, respond to threats faster, and ensure compliance with cybersecurity regulations. Zaperon empowers organizations to replace legacy security stacks with a scalable, cloud-native solution purpose-built for Zero Trust security in today's fast-evolving digital environment.



What does Zaperon Offer?

ZERO TRUST NETWORK ACCESS

Enable secure access to on-premise apps & servers from any location without VPNs.

IDENTITY & ACCESS MANAGEMENT

Manage user identity and application access with ease, and provide seamless single sign-on experience to users.

ADVANCED MFA

Deliver phishing-resistant multi-factor authentication with over 15+ contextual factors.

PASSWORDLESS AUTHENTICATION

Provide seamless passwordless access to enterprise apps using proprietary PKI-based digital signature.

CLOUD ACCESS SECURITY BROKER

Protect sensitive data on cloud by preventing unauthorized access, downloading and sharing.

DATA LEAK PREVENTION

Prevent data leaks from endpoints with restrictions on USB, Bluetooth, Airdrop, clipboard usage and cloud uploads.

ACTIVE DIRECTORY INTEGRATION

Easily integrate with existing Active Directory and LDAP for identity synchronization.

GRANULAR ACCESS CONTROL

Restrict access to enterprise apps (SaaS, cloud, on-premise) and servers exclusively from authorized corporate devices.

THREAT DETECTION & RESPONSE

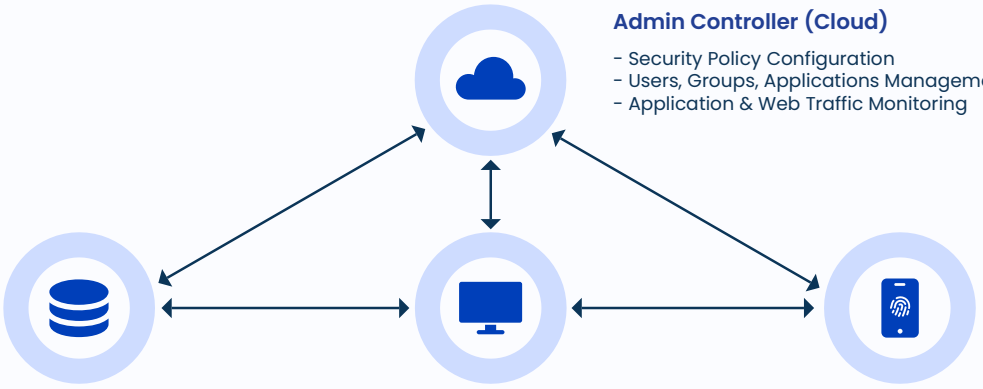
Monitor user activity, application usage, and web traffic patterns in real-time, and get threat alerts for anomalous behavior.

SHADOW IT GOVERNANCE

Detect and block usage of unsanctioned apps across the organization to reduce risk and maintain compliance.



How Zaperon Works?



Admin Controller (Cloud)

- Security Policy Configuration
- Users, Groups, Applications Management
- Application & Web Traffic Monitoring

Cloud Directory

- Centralized user, device and app directory
- Authorization & Authentication

Desktop App + Browser

- Security Policy Implementation
- Device Validation

Mobile Authenticator App

- Multi-factor Authentication
- Location Validation

SUPPORTED PLATFORMS

Operating System	Minimum Hardware Requirement	Minimum Operating System Version
Windows	x64-bit processor, Dual Core, 4GB RAM	Windows 10 (at least build 1809)
macOS	ARM-x64 processors, Dual Core, 4GB RAM	Monterey
Linux	ARM-x64 processors, Dual Core, 4GB RAM	RHEL 7, Ubuntu 22.10, CentOS Linux 7, CentOS Stream 8
Android	3GB RAM	Android 11
iOS	6GB RAM	iOS 12

WORKFLOW

1. IT admin configures security policies through the admin controller – Users, groups, applications, policy restrictions (Antivirus, Operating System, Location, Time, IP range, Data Protection).
2. When user logs in Zaperon desktop app, user identity and device posture are verified, and a PKI-based certificate with encoded user and device parameters is created automatically on the device.
3. Post login, Zaperon triggers multi-factor authentication using Zaperon Verify mobile app. This MFA is resistant to phishing attacks as it validates 15+ factors based on cryptographic signature, user behavior, device posture and context.
4. An authorized user gets passwordless access to all the applications assigned to them via a unified dashboard.
5. Zaperon performs continuous real-time assessments, every 30 seconds, of user behavior, device posture, and access context. If a policy violation or anomaly is detected, access is immediately revoked and IT admins are alerted.
6. All outbound web traffic is routed through Zaperon for inline inspection and analyzed using AI-powered threat intelligence and custom web policies to block malicious content, detect shadow IT, and enforce acceptable use policies.
7. Zaperon protects data across endpoints and cloud applications by enforcing strict DLP controls. It can block unauthorized uploads, downloads, copy-paste actions, USB/Bluetooth/airdrop transfers, protecting sensitive data from intentional or accidental exposure.

How Zaperon Secures Your Data?

In a world where sensitive data moves across users, apps, and clouds at lightning speed, traditional security tools struggle to keep up. Unlike legacy DLP tools that protect only devices or only cloud apps, Zaperon DLP redefines data protection with a Zero Trust, identity-aware approach that prevents data loss across endpoints, email and web eliminating blind spots and preventing insider threats, shadow IT risks, and sensitive file exfiltration from any location or device.

Built on the Zaperon Security Service Edge (SSE) Platform, it combines real-time content inspection, contextual access control and anomaly detection to stop data leaks before they occur whether intentional or accidental.

Key Features

UNIFIED DATA PROTECTION

Monitor and protect sensitive data across endpoints, SaaS, and web channels from a single policy console.

IDENTITY-CENTRIC POLICIES

Apply DLP rules based on user identity, device trust, and data sensitivity, not just location or network boundaries.

AI-POWERED CONTENT INSPECTION

Automatically detect sensitive information like PII, PHI, financial data, or source code using AI/ML and advanced pattern recognition.

INLINE DATA CONTROL

Enforce policies on data in motion blocking uploads, email attachments, or copy-paste actions before they reach unauthorized destinations.

SEAMLESS ENDPOINT & CLOUD COVERAGE

Integrates with Windows and browser-based workloads; supports major cloud platforms like Microsoft 365, Google Workspace, AWS, and Slack.

GRANULAR VISIBILITY & AUDITING

Gain full visibility into data flow, user actions, and policy violations with real-time dashboards and exportable compliance reports.

ZERO TRUST INTEGRATION

Part of the Zaperon Security Service Edge (SSE) suite, ensuring consistent DLP enforcement alongside CASB, ZTNA, and SWG modules.

INSIDER THREAT DETECTION

Detect risky or anomalous user behavior that might signal insider threats leveraging comprehensive DLP event reporting.

REGULATORY COMPLIANCE

Simplify adherence to regulations like DPDP Act, GDPR, HIPAA, PCI-DSS, and ISO 27001 through automated policy mapping and reporting.

Zaperon Advantage

Zaperon's Identity-centric SSE platform delivers unified security across Identity, Data, Web, and Zero Trust on any device and operating system. It ensures seamless protection for SaaS, on-premise, mobile, cloud, and network resources, offering complete control from a single dashboard.

UNIFIED PLATFORM

Zaperon platform offers

- Identity Security
- Zero Trust Security
- Data Security
- Web Security

OPERATING SYSTEM AGNOSTIC

Zaperon works seamlessly on

- Windows
- Mac
- Linux
- Android
- iOS

COMPREHENSIVE COVERAGE

Zaperon secures access to

- SaaS apps
- Legacy on-premise apps
- Mobile apps
- Cloud servers
- Network devices



How is Zaperon better than competitors?

Solution Category	Competitor	Problems with Existing Solutions	Zaperon Advantages
Traditional SSE	Zscaler, Palo Alto, Netskope	Users need passwords to access the applications, making organizations vulnerable to cyberattacks.	Zaperon allows access to applications using secure RSA-standard passwordless technology.
		Doesn't have identity access management capability and relies on integration with Okta or premium Entra ID license.	Offers end-to-end zero trust security with passwordless authentication, identity access management and AI-based continuous risk analysis to detect security threats.
		Only target large enterprises leaving a whitespace in mid-sized firms and startup segments.	Zaperon has products suited for organization of all sizes - startups, SMEs and enterprises
Identity & Access Management	Okta, OneLogin, Azure AD, MiniOrange	Only offers convenience with single sign-on but there are no security checks for access to applications.	Zaperon provides both single sign-on convenience and comprehensive security by continuously monitoring users, devices and applications.
		Performs no security checks to restrict users from connecting via insecure devices, putting organization data at risk.	Both user and device security parameters are assessed continuously to eliminate any vulnerabilities.
		Biometric-based passwordless authentication doesn't give IT admins any control as biometrics belong to the user.	Zaperon's PKI-based passwordless technology gives IT admins full control over their users and devices.
		Authentication of the user is done only once, leaving organizations blind to any cyberattacks that happen later.	Continuous risk analysis is done every 10 minutes to detect & flag in real-time any anomaly in user behavior and device security parameters.
		Product pricing plans are complicated.	Zaperon subscription plans are simple and all-inclusive.
		No provision to prevent data leak from cloud applications and endpoints.	Zaperon protects data in cloud applications and prevent data leak from endpoints' USB ports.
		Don't offer any visibility and control on web traffic.	Zaperon analyzes web traffic using AI-powered threat intelligence and custom web policies to block malicious content and detect shadow IT.

Enterprise Use Cases

S. No.	Customer	Use case	How Zaperon is helping
1	Financial Services Firm	Sensitive customer data on SaaS application Microsoft 365 could be accessed from any personal device. As a result, confidential information from personal devices could be leaked or downloaded.	As per their organization policy, Zaperon restricted access to Microsoft 365 apps – Outlook, OneDrive, etc. to only corporate-sanctioned devices and provided granular control so only authorized users had access.
2	Healthcare Provider	Only Finance team should be able to access Tally hosted on a cloud via Remote Desktop. Other employees should not be able to access the remote server.	Zaperon made access to remote server passwordless. At the same time, security is enhanced by enforcing access policies to ensure only authorized personnel could access remote server that hosted Tally application.
3	Electrical Equipment Manufacturer	Access to SAP applications should be permitted to employees only from Windows Desktop PCs during office times that are different for each of their 3 manufacturing plant locations.	With Zaperon, IT Admin could enforce Location and Plant-specific Time controls on each corporate-owned Windows desktop that allowed access to SAP only during office timings.
4	Fintech Startup in B2B lending	Employees were accessing unsanctioned applications on their corporate devices without the knowledge of IT admins, increasing security risks and SaaS costs for the organization.	Zaperon scans all the devices in organization and generate a Shadow IT report, providing visibility to IT admin on application usage and giving them control to block malicious applications.
5	BPO Provider	Customer service agents should be able to access their authorized applications on the same desktop PC while working in different shifts.	Zaperon provided flexibility by adding user-specific PKI-signature on the same Desktop for each customer service agent, segregating their log on profiles and allowing enforcement of different policies for application access.
6	Electrical Wire Manufacturer	Distributors & vendors accessed in-house order management application which posed a security risk as there was no visibility on the users accessing the application.	Zero Trust framework of Zaperon allowed access to vendors & distributors seamlessly while providing visibility to admins.
7	Automotive Component Manufacturer	Despite strict password policies, employees were creating guessable passwords, noting them on notepads and sharing with peers. As a result, organization became vulnerable to phishing attacks.	Zaperon, with its proprietary PKI-based technology, made access to all the applications Passwordless. Additionally, MFA through Zaperon Verify app helped in preventing account takeovers.
8	IT Service Firm	IT admins can't control which websites, web applications users can access on their corporate devices when not in office as firewall policies are not effective in such scenarios.	Zaperon enables IT admins to restrict corporate devices so users can access only approved URLs.
9	Management Consulting Firm	Remote employees used VPN to access Google Workspace for storing and sharing confidential documents. It was a security threat as VPN didn't provide application-level access control for SaaS applications to IT admin.	Zaperon replaced VPN with a more secure remote access which allowed admin to apply security policies to Google Workspace and on-prem applications that were earlier accessible via VPN.
10	Automotive Gear Manufacturer	Firm had SAP on-premise while all other applications were on cloud. It was challenge to control user access to all the applications.	Zaperon provided single platform for granular access control of all types of applications – on-premise, cloud and SaaS.

Zaperon

Zaperon is an Identity-centric Security Service Edge (SSE) platform designed to secure access to applications, data, and cloud infrastructure from any user or device, regardless of location or network. It continuously enforces access policies based on user behavior, device posture, and contextual parameters, ensuring least-privilege access while preventing lateral movement. By minimizing attack surface, proactively detecting anomalies, and providing real-time visibility, Zaperon fortifies hybrid IT environment. Organizations can proactively manage access, reduce risks from credential based threats, and safeguard sensitive information, making security adaptive, scalable, and resilient against evolving cyber threats.

+1 202 600 5234
+91 8800 170387
sales@zaperon.com
www.zaperon.com

© 2025 Zaperon, Inc.
All Rights Reserved.

