SECURE EDGE DATASHEET

Product Overview

As distributed workforces become prevalent, the way we secure the network edge is changing, giving way to new cloud-based architectures. With so many options available, organizations need the flexibility to leverage existing investments and seamlessly transition to a cloud-delivered architecture securely and at their own pace. Juniper Secure Edge provides full-stack Security Service Edge (SSE) capabilities to protect access to web, SaaS, and on-premises applications and provide users with security that follows them wherever they go. When leveraged with Juniper's AI-Driven SD-WAN, Juniper Secure Edge provides a best-in-suite SASE solution that helps deliver seamless and secure end-user experiences that leverage existing architectures and grow as you expand your SASE footprint.

Product Description

Juniper® Secure Edge secures the workforce wherever they are with consistent threat protection and an optimized network experience, and security policies that follow users wherever they go. It leverages a single-stack software architecture to keep latency low. User and device traffic is inspected once and applied in one configured service with Firewall as a Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA) and advanced threat prevention. Users have fast, reliable, and secure access to the data and resources they need, ensuring great user experiences. IT security teams gain seamless visibility across the entire network, all while leveraging their existing investments, helping them transition to SASE at a pace that is best for your business.

Secure Edge capabilities are all managed by Security Director Cloud, Juniper's simple and seamless management experience delivered in a single user interface (UI). Organizations can manage security anywhere and everywhere, on-premises and in the cloud from the cloud, with unified policy management that follows users, devices, and data wherever they go. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

When you add this together with Juniper's unique AI-driven SD-WAN solution, you have a cost-effective and reliable way to adopt a SASE architecture, regardless of where you are on that journey.

Architecture and Key Components

Organizations can support their workforce from anywhere with Juniper Secure Edge. Whether they are in the office, at home, or on the road, Juniper Secure Edge provides secure access to the data and resources workers need with consistent security policies that follow users and devices without having to copy over or recreate rule sets.

Juniper Secure Edge provides support for remote users wherever they are by routing them to the nearest Secure Edge Point of Presence (PoP).

Similarly, for campus and branch users where Juniper AI-Driven SD-WAN is deployed, you can connect each site to the nearest Secure Edge PoP. Additionally, you can offload your security services to the Secure Edge cloud. This process provides you with the benefits of several unique Juniper technologies, including Session Smart Routing™, App Control, AppQoS, Mist™ AI insights, anomaly detection, and automated troubleshooting.

These services, combined with Juniper's full-stack SASE offering, enable organizations to protect data and provide users with consistent and secure access, whether in the office, at the campus, or on the move.

Figure 1: Secure Edge securely connects users in any location directly to application resources they need without sending traffic back to a centralized location for traffic inspection and threat protection.

Juniper Secure Edge creates a seamless SASE experience powered by AI that can take organizations from wherever they are — whether starting on-premises or in the cloud — and creates a common networking and security policy framework. By building on Juniper's expertise in using AI to optimize the network experience, Secure Edge leverages AI to enhance the experience for security practitioners so that risk decreases while simultaneously improving the end-user experience.

It allows organizations to leverage their existing technology investments, whether customers are starting on-premises with campus and branch use cases, in the cloud with remote workforce use cases, or a hybrid approach.

Features and Benefits

Firewall-as-a-Service (FWaaS)

FWaaS identifies applications and inspects traffic for exploits and malware with over 99.8% effectiveness.

Juniper's FWaaS provides all next-generation firewall (NGFW) features as a service, delivered via Juniper's managed cloud. It leverages public cloud points of presence, ensuring fast access to data anywhere users are, whether they are "on the network" or not. This unique architecture enables Secure Edge to provide traffic inspection and control with ultra-low latency.

Secure Web Gateway (SWG)

SWG protects web access by enforcing acceptable use policies and preventing web-borne threats.

Juniper's SWG provides web traffic control through granular URL-based policies, content inspection, selective SSL decryption, and Encrypted Traffic Insights to protect against web-based attacks even when decryption isn't possible. The SWG filters out non-compliant websites and removes malware from allowed web traffic. To accomplish this, the SWG includes URL filtering, intrusion prevention, selective SSL inspection, and machine-learning-based malware detection that also profiles HTTPS connections for malicious traffic.

Cloud Access Security Broker (CASB)

CASB provides visibility into SaaS applications and granular controls to ensure authorized access, threat prevention, and compliance.

Juniper's CASB secures SaaS applications from unauthorized or inadvertent access, malware delivery and distribution, and data exfiltration. It discovers sanctioned and non-sanctioned SaaS applications in use and provides visibility and granular controls to ensure authorized access, actions, threat prevention, and compliance.

Data Loss Prevention (DLP)

DLP classifies and monitors data transactions and ensures business compliance requirements and data protection rules are followed.

Juniper DLP enables organizations to discover and protect sensitive data in their cloud applications. Its extensive DLP support includes structured and unstructured data, data classification, exact data match (EDM), and optical character recognition (OCR).

It provides granular visibility and control over data housed in cloud applications and prevents sensitive data from leaving the network either inadvertently or as part of an attack.

Zero Trust Network Access (ZTNA)

With ZTNA, ops teams can ensure that wherever users are, they have secure access to their data and applications when needed. Risk must be assessed at that moment and inform the level of access the user should have at that moment.

Juniper ZTNA provides secure, least privileged access to corporate applications, wherever they may be – on-premises or in the public cloud. It leverages security policy decision-making that considers context types such as user and device identity, geographic location, and threat level. Even for approved sessions, Secure Edge continues to monitor for threats and anomalies, ensuring that corporate apps and data are always protected.

Advanced Threat Prevention

As the threat landscape evolves and security risks accelerate, you can no longer rely on a single device at the network edge to identify and block threats. Instead, you need a threat-aware network that frees your security analysts to focus on hunting unknown threats and further reduces risk to your organization.

Advanced Threat Prevention discovers zero-day malware and malicious connections, including botnets and command and control (C2), even when traffic cannot be decrypted. It enforces granular mechanisms, such as file quarantine and reduced access rights.

As part of Juniper's Advanced Threat Prevention, Juniper SecIntel provides threat intelligence to all points of connection across the network to block malicious traffic, creating a threat-aware network. SecIntel can be deployed at the WAN edge, across wired and wireless LANs to increase threat visibility, and at enforcement points within the network to reduce risk.

Secure User Access

Support the remote workforce in the office, at home, or on the road with fast and secure user access to the data and resources people need to do their jobs effectively. Security policies are based on identity and follow the user wherever they go.

Organizations that love their existing identity solutions don't have to rip and replace them. Secure Edge integrates with all leading identity providers, such as Okta and Azure Active Directory, via Security Assertion Markup Language (SAML) 2.0.

The follow-the-user policy provides automated access to third-party contractors through granular risk-based controls, locking down third-party access as an attack vector. Secure Edge policy can be configured so that third-party access to resources requires additional verification, and access can be automatically revoked according to a scheduled end date. Contractors and third parties will no longer have access once their contracts are complete.

Users have seamless and secure access to corporate resources without jumping through hoops associated with multiple authentication portals or backhauling traffic to a data center.

Administrators can control their risk level by ensuring that consistent security policies are applied to users, whether accessing sensitive resources from their couch or browsing the Internet from the office.

Single-Policy Framework

Juniper Secure Edge, managed by Security Director Cloud uses a single policy framework that enables security policies to be created once to follow users, devices, and data wherever they go. Customers don't have to start from scratch when adopting cloud-delivered security. With our three-click wizard, customers are able to leverage existing campus edge policies and translate them into an SSE policy with ease. Because it uses a single policy framework regardless of the deployment model, Secure Edge, applies existing security policies from traditional deployments to its cloud-delivered model in just a few clicks, reducing misconfigurations and risk.

Whether securing remote users, campus and branch locations, private cloud, public cloud, or hybrid cloud data centers, Juniper provides unified management and unbroken visibility across all architectures. This makes it easy for ops teams to easily and effectively bridge their current investments with their future architectural goals, including SASE. Customers can manage security anywhere and everywhere, on-premises, in the cloud, and from the cloud, with security policies that follow users, devices, and data wherever they go, all from a single UI.

Juniper has been consistently validated by multiple third-party tests as the most effective security technology on the market for the past four years, with 100% security efficacy across all use cases.

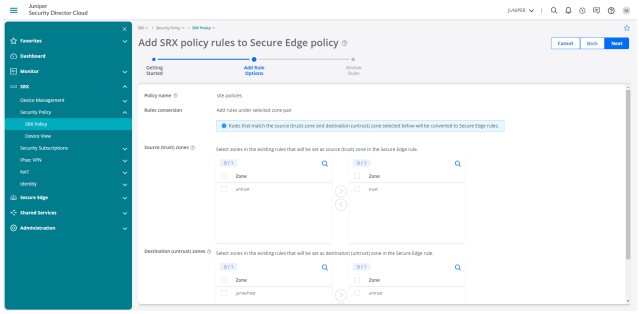

Figure 2: Unified management coupled with a single policy framework ensures security policies created for physical or virtual firewall deployments can easily and automatically apply to sites where Secure Edge delivers those same policies as a service.

Leverage Existing Investments

Transitioning to a cloud-based security architecture shouldn't mean abandoning existing IT investments. Secure Edge allows organizations to transition to a Secure Access Service Edge (SASE) architecture at their own pace. It doesn't force administrators to toggle between separate management platforms for on-premises and cloud-delivered security. All deployment, configuration, and management are done through Security Director Cloud—the same management platform that manages all SRX Series firewalls.

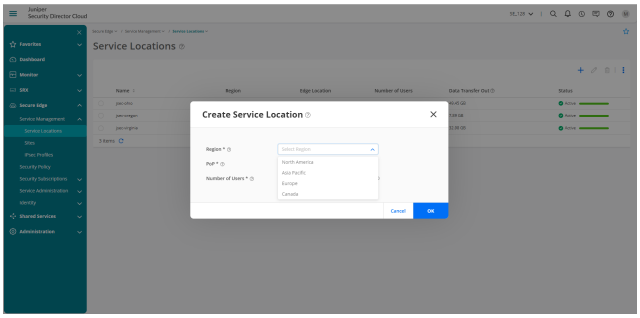

Figure 3: Easily manage site deployment and configuration, user authentication, and policies from anywhere through an easy-to-use Web interface.

Security Assurance

Whether it's a rule for a traditional firewall policy or a policy delivered as a service, rules must be placed in the proper order, so they're effective when needed. However, rules can quickly add up, leading to outdated, shadowed, and therefore ineffective rules. Also, duplicates require hours from administrators who must sort through hundreds or even thousands of rules before they can confidently make changes.

Because Secure Edge is managed through Security Director Cloud, duplicate and shadowed rules are automatically surfaced before they're committed. Rule hit counts are highlighted so administrators can quickly make changes, ensuring that new and existing policies are effective for the intended users at the intended time.

Proven Security Effectiveness

It's not enough that a cloud-delivered FWaaS, SWG, CASB, DLP, ZTNA, and advanced threat prevention are easy to use. The security services controlling traffic and user access and inspecting threats must also be effective. The threat prevention features delivered as-a-service by Secure Edge are the same threat prevention features delivered on the physical, virtual, and containerized SRX Series firewalls. These features, including intrusion prevention, anti-malware, advanced threat prevention via Juniper Advanced Threat Prevention Cloud, and Encrypted Traffic Insights, have been proven over 99.8% effective against server- and client-side exploits and 100% effective against malware by multiple third-party tests.

Delivering Best-in-class SSE

Juniper Secure Edge delivers best-in-class SSE as part of a full-stack SASE solution that empowers organizations to transition to a SASE architecture regardless of where they are on their SASE journey.

Juniper offers full-stack WAN edge and SSE that leverage the power of the cloud to optimize both the network and security experience.

Dynamic policies can be created to center around a user or group of users, or device or group of devices, so that access and threat protection rules are applied consistently regardless of geographic or network location. Administrators do not need to duplicate or recreate rule sets, helping increase operational efficiency and furthering Zero Trust initiatives within organizations.

Table 1: Secure Edge Features and Benefits

Feature	Benefit
Application visibility and control	Facilitates instant recognition and control of application access, including Software as a Service (SaaS) applications: the application name, description of the service, and inherent level of risk, regardless of port, protocol, or encryption method.
Secure Web Gateway	Ensures Web traffic remains free of web-borne threats and provides direct Internet access to users wherever they're located through a Secure Web Gateway functionality with SSL/TLS proxy and inspection capabilities.
Cloud Access Security Broker	Provides visibility into SaaS applications and granular controls to ensure authorized access, threat prevention, and compliance. Secures SaaS applications from unauthorized or inadvertent access, malware delivery and distribution, and data exfiltration.
URL filtering	Provides Web traffic categorizations that can be incorporated into application and security policy to automatically protect users from web-borne threats, such as drive-by malware downloads, phishing sites, and exploit kits. Secure Edge URL filtering also helps organizations maintain compliance by controlling Web access and preventing unwanted browsing activity.
Content filtering	Inspects e-mail, webpages, and files for unwanted and malicious content. Administrators can granularly control what content is allowed, restricted, or blocked within security policies.
SaaS Security	Provides greater visibility and control over SaaS applications, including data, usage, compliance, threat prevention and access, monitors and controls user behavior, and minimizes potential risks associated with use of unsanctioned apps, or "shadow IT."
Data Loss Prevention	Monitors and protects sensitive data as it transits between networks, users, and services, and at rest within SaaS applications. Prevents data leakage and excessive data exposure anywhere regulated data moves and resides, and in accordance with compliance requirements. Supports structured and unstructured data, data classification, Exact Data Match (EDM), Optical Character Recognition (OCR).
Zero Trust Network Access	Secure access to corporate and cloud resources, providing reliable connectivity and consistent security anywhere. Reduce risk by extending visibility and enforcement to users wherever they are.
User identity	Integrates with identity services, such as Azure AD and Okta, that help Secure Edge define policies and application use based on individual users or user groups. Provides visibility into application usage at the user level rather than IP address, providing powerful insights into application traffic traversing the network, on-premises and in the cloud.
Dynamic user segmentation	Helps to limit third-party access as an attack vector with follow-the-user policies. Policies can be created to apply to users wherever they go, on or off the corporate network, providing automated access control to employees and third-party contractors.
Intrusion detection and prevention services (IDS/IPS)	Mitigates network and application exploits and protects against a range of attacks with signatures proven effective by multiple third-party tests. Juniper intrusion detection and prevention (IDP) constantly monitors new exploits against recently discovered vulnerabilities, keeping network protection up to date against the latest cyberattacks and stopping them at the exploit stage before they gain a foothold inside the network.
Anti-malware	Uses a constantly updated global threat database augmented by research from threat-sharing communities such as Cyber Threat Alliance, to protect the edge. Through in-line inspection and blocking, Secure Edge prevents known malware from installing on endpoints and blocks malicious outbound (C2) communications resulting from malware infections.
Domain Name System (DNS) filtering	Identifies domains with high-risk reputations, typically those associated with attack campaigns or containing unwanted content, and blocks communications to and from both the domain and associated IP address.
DNS security	Analyzes DNS queries for threat activity, such as tunneling, C2 communications, and domain generation algorithms, identifying compromise attempts and preventing additional infection. Identifies signs of DNS misuse that attackers employ to circumvent security controls.
Advanced threat protection	Leverages Juniper ATP Cloud, Juniper's global threat intelligence hub, for advanced threat protection to uncover and mitigate zero-day malware quickly and improve threat response times by taking real-time threat information and pushing it out to all points across the network. Juniper ATP Cloud has been proven effective against new and commodity malware by multiple third-party tests.
Encrypted Traffic Insights	Restores threat visibility lost due to encryption, without the heavy burden of full TLS/SSL decryption. Secure Edge collects relevant SSL/TLS connection data, including certificates used, cipher suites negotiated, and connection behavior. This information is processed using network behavioral analysis and machine learning to determine whether the connection is benign or malicious. Malicious traffic can then be dropped, stopping threats such as botnets in their tracks.
Adaptive threat profiling	Leverages existing infrastructure to create security intelligence feeds based on real-time events occurring on the network. These feeds, unique to each organization, can be configured based on security policies and utilized by other enforcement points on the network to detect threats and update their infrastructure in real time, blocking potential attacks.
Compromised host isolation	Identifies compromised devices, which can be added to a quarantine list either manually or automatically, stopping those devices from accessing sensitive data and preventing the malware from spreading laterally.
Agentless on-ramp	Protects users with security policies through agentless functionality. Users log in through single sign-on (SSO) to securely access the applications and data they need.
SaaS Security Posture Management	Performs an automated assessment of your SaaS landscape against well-defined security guidelines, reducing the operational complexity in managing multiple apps, preventing data loss from misconfigurations, and ensuring compliance in a multi-cloud environment. Uses a prebuilt compliance libraries of common standards or best practices such as CIS Foundations Benchmarks, SOC 2, PCI, NIST 800-53, or HIPAA. Provides visibility and insights into third-party applications connecting to your SaaS applications.
Cloud Data Discovery	Performs periodic or ad-hoc deep assessments of data in cloud apps using DLP templates to identify security blind spots, detect open shares and address many global regulations — PCI, HIPAA, GDPR, GLBA, etc.

Product Options

Secure Edge can be purchased as a subscription license based on the number of users. Licensing for 1-and 3-year terms are available for both standard and advanced tiers.

Licensing also entitles the customer to a free fixed allotment of cloud data consumption, which is calculated based on the product of the number of users and the per-user allotment amount per period. If overages are applicable, Juniper will issue a quote, the customer will issue a purchase order, and Juniper will issue an order of acknowledgment.

For more details regarding such overage charges, please contact your Juniper Sales Representative or Partner.

Feature	Standard	Advanced
TLS/SSL inspection	Yes	Yes
Secure Web Gateway	Yes	Yes
URL filtering	Yes	Yes
Content filtering	Yes	Yes
Application visibility	Yes	Yes
User awareness and segmentation	Yes	Yes
Standard threat prevention (threat intelligence feeds, DNS filtering, anti-malware, compromised host isolation)	Yes	Yes
In-band CASB	Yes	Yes
Advanced Threat Prevention (DNS security, zero-day malware prevention, Encrypted Traffic Insights, adaptive threat profiling)	No	Yes
Intrusion detection and prevention services (IDS/IPS)	No	Yes
Out-of-band CASB-DLP-SSPM	Add-On	Add-On
Secure Remote Access	Add-On	Add-On

Add-Ons to WAN Assurance

Customers can add out-of-band CASB-DLP to their active WAN Assurance (SD-WAN) or Secure Edge licenses.

Out-of-band CASB-DLP*	Standard	Advanced
CASB	Yes	Yes
DLP	Yes	Yes
SaaS Security Posture Management	No	Yes
Additional Cloud Data Discovery (per TB)	Add-On	Add-On

*Out-of-band CASB-DLP licenses must be tied to an active base license for Juniper Secure Edge or Juniper WAN Assurance/SD-WAN.

Specifications

	Standard	Advanced
Traffic forwarding	Proxy autoconfiguration (PAC), GRE, IPsec	PAC, GRE, IPsec
Authentication	Security Assertion Markup Language (SAML), Lightweight Directory Access Protocol (LDAP), Juniper Identity Management Service (JIMS)	SAML, LDAP, JIMS

Juniper Security Director Cloud

As Juniper's simple and seamless management experience, Security Director Cloud is delivered in a single UI to connect customers' current deployments with their future architectural rollouts. Management is at the center of the Juniper Connected Security strategy and helps organizations secure every point of connection on their network to safeguard users, data, and infrastructure.

Security Director Cloud enables organizations to secure their architecture with consistent security policies across any environment—on-premises, cloud-based, cloud-delivered, and hybrid—and expands zero trust to all parts of the network from the edge into the data center and to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Juniper meets customers where they are on their journey, helps them leverage their existing investments, and empowers them to transition to their preferred architecture at the best pace for business by automating their transition with Security Director Cloud.

Ordering Information

To order Juniper Secure Edge and access software licensing information, please visit the How to Buy page at https://www.juniper.net/us/en/how-to-buy/form.html.

Files uploaded to the cloud for processing are destroyed afterward to ensure privacy. The Juniper Networks privacy policy can be found on the product Web portal at https://www.juniper.net/us/en/privacy-policy.html.

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit https://www.juniper.net/us/en/products.html.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security, and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability, and equality.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240 1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.207.125.700

Juniper Networks | Driven by Experience™