cradlepoint PART OF ERICSSON

Data Sheet

NetCloud SASE

2024 - 04 - 25

Simple, agile SD-WAN and security for dynamic, highly distributed wireless and hybrid WANs

The Challenge

The adoption of 5G Wireless WANs is enabling fast-moving organizations to extend their reach and move their services closer to their customers. But while every new 5G connection means growth and scale, it also means organizations are increasing their network attack surface. Even though 5G as a WAN technology is inherently secure, the devices connecting to the 5G network could be vulnerable. An example is the influx of inherently insecure IoT devices that could be an attack vector into the network.

Another key challenge is LTE/5G WANs are far more dynamic than traditional wired networks. Temporary sites are moving locations, vehicles are moving between coverage areas, IoT devices are multiplying, and employees are working from anywhere. Traditional security can be complex in these changing, highly distributed environments.

What's Required?

As the network changes and becomes more dynamic and more distributed, security needs to change along with it. NetCloud SASE provides the simple and agile security that is required for organizations managing thousands of fixed and temporary sites, vehicles, IoT devices, and remote workers.

Key attributes of the NetCloud SASE solution:

- Optimized to support dynamic **wireless and hybrid WAN use cases** that include mobility and roaming
- Designed with a **zero trust foundation** that hides the network attack surface even while the network is scaling
- Offers a **consistent, unified policy** that follows users as they work from anywhere
- Offers robust **security for managed and unmanaged devices**
- Goes beyond just signature-based detection of web and email threats to a completely air-gapped approach based on **Remote Browser Isolation**
- **Simple to deploy, manage, and troubleshoot** for lean IT managing thousands of microsites

Enabling Organizations

NetCloud SASE gives networking/IT teams the **confidence** to connect anything from anywhere. Specifically, organizations can:

- Create highly secure **zero trust networks, at scale, in as little as six minutes**.
- Enable a **zero loss WAN** through intelligent bonding suitable for mission-critical communications from a site or a vehicle.
- **Block zero-day exploits and sophisticated phishing attacks** using powerful isolation technology – transparently to the end user.

- **Protect corporate applications from risky unmanaged devices** using Web Application Isolation.†
- **Retain an organization's intellectual property and sensitive data**, even in the era of Gen AI.†

†Requires Ericom Security Platform. Will be integrated into NetCloud SASE in the future.

Three Main NetCloud SASE Capabilities

Zero Trust SD-WAN

A simpler, more secure SD-WAN, optimized for cellular networks. It allows organizations to provide an outstanding digital experience in environments where applications reside anywhere and require secure access from anywhere. The zero trust foundation ensures that security is built into the service as opposed to bolted on, which increases simplicity, security, and cost-effectiveness. Application-based traffic steering, intelligent bonding, and forward error correction ensure that a high level of resiliency and quality of experience is achieved for every user and every location.

Zero Trust Private Access

Provides controlled, secure access to private applications or assets on the WAN for both managed and unmanaged devices (IoT, contractor devices, BYOD). "Connect and Go" zero trust networks can be deployed in a few clicks, allowing networking IT teams to deploy high volumes of IoT devices without compromising security. For users, universal ZTNA capabilities allow for a single policy to follow them as they work from anywhere and provide secure remote access to only authorized resources. Finally, for organizations that have contractor and BYOD devices accessing corporate web applications, NetCloud SASE offers robust isolation-based security to protect applications from risky devices that could contain malware or viruses.†

Zero Trust Internet Access

This suite of services, consisting of Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Remote Browser Isolation (RBI), Data Loss Prevention (DLP), and Content Disarm and Reconstruct (CDR), offers protection from sophisticated malware (including zero-day exploits), phishing attacks (even when the user clicks on a link), unauthorized SaaS usage, and data leaks from both collaboration and Gen AI platforms.†

†CASB and DLP are available through the Ericom Security Platform. Will be integrated into NetCloud SASE in the future.

Why NetCloud SASE Is Different

Designed for cellular-centric use cases that include roaming and mobility, with key Wireless WAN optimizations that preserve bandwidth, enhance performance, and deliver a slicing-ready solution as 5G networks evolve to 5G standalone.

Truly unified for unparalleled simplicity. Although many SASE solutions provide unified management, underneath there are still multiple disjointed products, multiple policy engines, and an inconsistent provisioning experience across the various services. NetCloud SASE is unified from a management, control, and data plane perspective, offering one true policy engine and one consistent provisioning experience across all networking and security services.

Zero trust built in rather than bolted on. Combines security with the network creation process to construct a zero trust foundation that is deny-all by default. This provides the secure foundation to build additional policies from. The NetCloud SASE solution obscures all public IP addresses (even for applications and assets that connect to the zero trust network), ensures assets and applications connecting to the network remain "dark" until explicitly defined, and restricts all access unless explicitly defined by policy.

Isolation at the core. NetCloud SASE goes beyond just relying on threat detection for web and email threats and leverages Remote Browser Isolation to completely airgap users and their devices from web and email borne threats, including destructive zero-day exploits. Without impacting the browsing experience, the solution protects organizations against phishing attacks (even when a user clicks on the link), retains intellectual property from potential leaks, and disarms embedded malware in attachments.

Robust security for unmanaged devices. While most SASE solutions provide security for managed devices, unmanaged devices can still put organizations at risk. NetCloud SASE goes beyond clientless browser-based access for third-party devices and leverages Web Application Isolation to completely airgap corporate web applications from risky third-party devices – mitigating the risk of malware infection.†

†Requires Ericom Security Platform. Will be integrated into NetCloud SASE in the future.

NetCloud SASE Management and Operations

NetCloud SASE is fully deployed and managed through Cradlepoint's powerful cloud management and orchestration platform, NetCloud Manager. With features that include zero-touch deployment, bulk provisioning, multilayered dashboards, centralized flow-level visibility, and intuitive troubleshooting tools, NetCloud Manager is a valuable assist to lean IT organizations. With the addition of a premium license, NetCloud Manager also offers valuable AI-driven insights.

Features List

Zero Trust SD-WAN

- **Zero trust foundation for SD-WAN**: While traditional SD-WAN technology leverages encryption and site-based VPN technology to secure traffic over multiple WAN connections, NetCloud SASE leverages a true zero trust foundation that minimizes the attack surface, limits the blast radius, and is deny-all by default.
- **Classification of traffic into predefined classes**: Through deep packet inspection, administrators can classify their traffic into business critical, real-time, interactive, or best effort.
- **Application-based traffic steering**: After traffic is classified, policies can be created to ensure business critical and real-time applications are prioritized across the WAN and are always traversing the highest performing WAN connection.
- **Traffic steering based on real-time WAN performance**: Using in-line traffic, NetCloud SASE measures latency, loss, and available bandwidth across all available WAN connections. If performance degrades beyond the predefined thresholds, traffic is dynamically steered to a better performing connection.
- **Direct Internet Access**: To enhance performance and reduce the costs of backhauling, NetCloud SASE enables Direct Internet Access capabilities from sites and vehicles.
- **Traffic steering across 5G network slices**: Select Cradlepoint modems can support up to eight 5G SA network slices. Leveraging NetCloud SASE, when a 5G SA network is in place, the ability to steer applications into the most suitable network slide is available. (For example, business-critical traffic can be steered into an ultra-reliable low latency slice.)
- **Flow duplication across bonded WAN connections**: Creates a zero-loss WAN connection for mission-critical applications by duplicating traffic flows across two diverse connections to increase availability.
- **Weighted flow balancing across bonded WAN connections**: Distributes application traffic flows across diverse WAN links according to user-defined weights for improved efficiency and cost savings.
- **Bandwidth aggregation across bonded WAN connections**: Aggregates two or more WAN links into one logical link to gain access to higher aggregate bandwidth.
- **Forward Error Correction**: Most effective for chatty TCP-based applications, FEC mitigates against lossy connections by adding parity bits to an application flow to prevent application retries, thereby improving application quality of experience.
- **Networkwide application-based policies**: With NetCloud SASE, just a single SD-WAN policy can be applied across the entire network, including across heterogenous product types.

Zero Trust Private Access

NetCloud SASE Secure Connect

- **Domain name-based routing**: Translates complex IP addresses to more intuitive names to hide the network attack surface, simplifies provisioning, and creates more intuitive policies.
- **Support for overlapping IP addresses at sites**: With domain-based routing in place, overlapping IP addresses can easily be accommodated.
- **Resource-definition**: Applications and assets connecting to the network are "dark" until explicitly defined and an access policy is created.
- **Deny-all by default**: Rather than broad network access, zero trust starts with a secure foundation where access is restricted until explicitly defined by policy.
- **Blocks east/west traffic by default**: Contains breaches to where they occurred by blocking east/west and all incoming traffic to a site, unless enabled by policy.
- **Split routing from sites**: Enables Direct Internet Access from the edge router. Administrators define all the IP subnets that need to go through the SASE service; all other traffic goes direct to the internet.

NetCloud SASE ZTNA

- **Identity verification**: Offers integration to any SAML 2.0 compliant Identity Management Platform, preventing identity sprawl.
- **Isolated user-to-resource access**: Users are directly authenticated to their authorized resources per session.
- **Least privilege access**: Different levels of access, ranging from visibility only to full configuration, can be granted based on the user's job function or identity.
- **Continuous monitoring for changes in context**: Changes in context are monitored, resulting in changes in access privileges if warranted.
- **Device posture visibility**: Administrators can view details on the device posture (for example, anti-virus installed and running, OS version, and device type) for any device that has the client installed.
- **Flexible user authentication**: In addition to being able to authenticate users through a Cradlepoint router, a wide range of Windows, Mac, and Linux clients are supported to enable safe remote connectivity from anywhere.
- **Microtunnel architecture for client access**: Ensures minimal bandwidth utilization and improved application performance.

Zero Trust Internet Access

- **Secure Web Gateway**: Ensures that user-initiated web requests align with the established policies of an organization. If the request raises any red flags or appears linked to suspicious or malicious websites and applications, the gateway promptly intervenes by returning a warning or outright blocking user access.
- **Remote Browser Isolation**: Separates users' devices from the act of internet browsing by hosting and running all browsing activity in a remote, isolated cloud-based container. Only a safe rendering is delivered to the end user.
- **Content Disarm and Reconstruct**: Protects against known and unknown threats contained in documents by removing executable content before the file is downloaded to the user's device.

Premium License Only Features

Hybrid Mesh Firewall

- **Application visibility and enforcement**: Uses policies and deep packet inspection to determine whether to block or allow traffic, including communications to or from an application.
- **IDS/IPS**: Provides continuous monitoring of all north/south and east/west traffic flows to detect and prevent malicious activity.

- **Web filtering**: Blocks access to inappropriate web content including high-risk domains that may contain malware.
- **Firewall-as-a-Service**: Simplifies firewall deployment by using cloud firewall capabilities instead of requiring local firewalls in all locations.

AI-Driven Insights

- **AI-driven insights**: An integrated AIOps dashboard simplifies the ongoing operations of the SASE network by quickly identifying faults, determining the root cause, and pinpointing all the affected sites, users, and applications.
- **Virtual Expert capabilities**: While Cradlepoint's AI-based NetCloud Assistant (ANA) is to be available across all NetCloud Manager dashboards, more specialized troubleshooting functionality is only available with a NetCloud SASE Premium license.

Ordering Guide

This section provides an overview of ordering NetCloud SASE. Contact your authorized sales representative to obtain a quote.

For ordering details, see the following:

- **Step 1**: Select the **NetCloud Service plan(s)** and NetCloud SASE compatible router.
- **Step 2**: Select NetCloud SASE Secure Connect or NetCloud SASE SD-WAN **site license(s)** for supported routers. Select Standard or Premium. Each license includes 500 GB for a shared data pool.
- **Step 3**: Select NetCloud SASE ZTNA license and/or Advanced Web Security license per user. Select Standard or Premium, matching the Step 2 selection.
- **Step 4**: Select NetCloud SASE Virtual Edge per each Amazon VPC. Select Standard or Premium, matching the Step 2 selection. Each license includes 500 GB for a shared data pool.
- **Step 5**: Select additional 500 GB data credits to add to the shared data pool.

NetCloud Add-Ons

REGION	PACKAGE	DESCRIPTION	PART NUMBER
All Regions:	NetCloud SASE Secure Connect	Includes data credit and requires corresponding NetCloud Essentials plan.	NCS-0K0x-SCDC NCS-0KPx-SCDC
	NetCloud SASE Secure Connect Premium	Includes data credit, NetCloud SASE Hybrid Mesh Firewall, and AI Insights. Requires corresponding Essentials plan.	
	NetCloud SASE SD-WAN	Includes Secure Connect and data credit. Requires corresponding Essentials plan.	NCS-0L0x-SCDCSD
	NetCloud SASE SD-WAN Premium	Includes Secure Connect, data credit, SD-WAN, Hybrid Mesh Firewall, and AI Insights. Requires corresponding Essentials plan.	NCS-0LPx-SCDCSD
	NetCloud SASE ZTNA for Users	Requires NetCloud SASE Secure Connect.	NCS-0E0x-ZTNA
	NetCloud SASE ZTNA for Users Premium	Includes Hybrid Mesh Firewall and AI Insights. Requires NetCloud SASE Secure Connect.	NCS-0EPx-ZTNA

	NetCloud SASE Virtual Edge	Includes NetCloud SASE Secure Connect, data credit, and NetCloud Essentials plan.	NCS-0M0x-VESCDC
	NetCloud SASE Virtual Edge Premium	Includes NetCloud SASE Secure Connect, data credit, Hybrid Mesh Firewall, AI Insights, and NetCloud Essentials plan.	NCS-0MPx-VESCDC
	NetCloud SASE Data Credit	500 GB Add-On	NCS-0D0x-DC
All Regions Add-On:	NetCloud SASE Premium Add-On	Includes Hybrid Mesh Firewall and AI Insights. Requires corresponding NetCloud SASE Secure Connect or NetCloud SASE SD-WAN.	NCS-0NPx-HMFAI
	NetCloud SASE SD-WAN Add-On	Includes Secure Connect, data credit, SD-WAN, Hybrid Mesh Firewall, and AI Insights. Requires corresponding Essentials plan.	NCS-0B0x-SDWAN
All Regions — Renewal:	NetCloud SASE Secure Connect	Includes data credit and requires corresponding NetCloud Essentials plan.	NCS-0K0x-SCDC-R
	NetCloud SASE Secure Connect Premium	Includes data credit, NetCloud SASE Hybrid Mesh Firewall, and AI Insights. Requires corresponding Essentials plan.	NCS-0KPx-SCDC-R
	NetCloud SASE SD-WAN	Includes Secure Connect and data credit. Requires corresponding Essentials plan.	NCS-0L0x-SCDCSD-R
	NetCloud SASE SD-WAN Premium	Includes Secure Connect, data credit, SD-WAN, Hybrid Mesh Firewall, and AI Insights. Requires corresponding Essentials plan.	NCS-0LPx-SCDCSD-R
	NetCloud SASE ZTNA for Users	Requires NetCloud SASE Secure Connect.	NCS-0E0x-ZTNA-R
	NetCloud SASE ZTNA for Users Premium	Includes Hybrid Mesh Firewall and AI Insights. Requires NetCloud SASE Secure Connect.	NCS-0EPx-ZTNA-R
	NetCloud SASE Virtual Edge	Includes NetCloud SASE Secure Connect, data credit, and NetCloud Essentials plan.	NCS-0M0x-VESCDC-R
	NetCloud SASE Virtual Edge Premium	Includes NetCloud SASE Secure Connect, data credit, Hybrid Mesh Firewall, AI Insights, and NetCloud Essentials plan.	NCS-0MPx-VESCDC-R
	NetCloud SASE Data Credit	500 GB Add-On	NCS-0D0x-DC-R
All Regions — Add-On Renewal:	NetCloud SASE Premium Add-On	Includes Hybrid Mesh Firewall and AI Insights. Requires corresponding NetCloud SASE Secure Connect or NetCloud SASE SD-WAN.	NCS-0NPx-HMFAI-R
	NetCloud SASE SD-WAN Add-On	Includes Secure Connect, data credit, SD-WAN, Hybrid Mesh Firewall, and AI Insights. Requires corresponding Essentials plan.	NCS-0B0x-SDWAN-R

x = 1, 3, or 5 years