ERICOM
Be Connected, Be Secure

Ericom Global Cloud

The Ideal Platform for Our Cloud-Native SASE

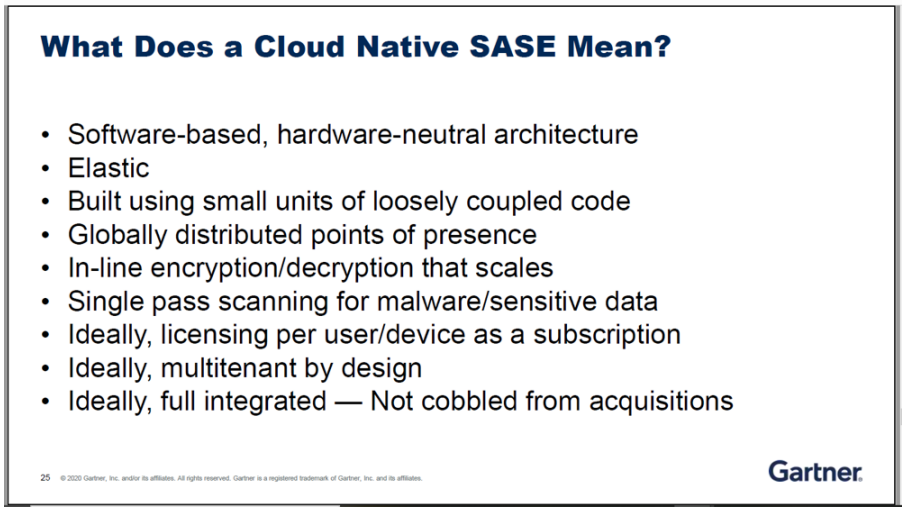
Ericom Global Cloud: The Ideal Platform for Our Cloud-Native SASE

Table of Contents

Ericom Global Cloud: The Ideal Platform for Our Cloud-Native SASE

What Makes a Cloud Suitable for Cloud-Native SASE?

In a session entitled, “The Future of Network Security is in the Cloud”, Gartner enumerated nine criteria for cloud-native secure access service edge (SASE) solutions. Six of these criteria were deemed essential, with the final three presented as ideals.



Ericom solution architects were gratified to see that Gartner could have (but *definitely* didn’t) based their criteria on our very own Ericom Global Cloud.

The criteria that Gartner considers essential are:

1. Software-based, hardware-neutral architecture
2. Elastic
3. Built-using small units of loosely coupled code
4. Globally distributed points of presence
5. In-line encryption/decryption that scales
6. Single pass scanning for malware/sensitive data

Criteria that are recommended include:

7. Licensing per user/device as a subscription
8. Multitenant by design
9. Fully integrated – not cobbled from acquisitions

In this technical brief, we review each feature or capability and discuss its significance for cloud-native SASE solutions.

Ericom Global Cloud: Checking the Boxes for Essential SASE Cloud Criteria

Software-Based, Hardware-Neutral Architecture

Ericom Global Cloud services utilize microservice architecture that's managed by Kubernetes. A Kubernetes abstraction layer runs on all hosts, including major cloud platforms and on-premises, making the Ericom Cloud to hardware-neutral and cloud-agnostic.

Why is software-based, hardware-neutral architecture important?

"Neutrality" and "agnosticism" are terms that sound, well, fairly neutral. So, what makes them important for a SASE cloud?

The answer, in just a few words, is freedom, efficiency and cost savings: Workloads can be moved freely between platforms and vendors. Once you've designed your applications and standardized them on the platform, you never need to rethink infrastructure or worry about being locked in to a specific vendor.

Elasticity

Ericom Global Cloud is elastic in its ability to rapidly scale geographically and for load handling, computing capacity and fail-over.

Elasticity is built in to the Ericom Global Cloud, which leverages Kubernetes node pools to enable rapid instantiation to meet demand. Each functional cluster within the cloud comprises multiple pools of identically configured nodes, with the quantity of pools standing by optimized via AI logic for cost/performance. This ensures high availability, with new nodes automatically created and/or existing nodes immediately ready to accept loads in the event that of node failure due to infrastructure problems, power outages, hardware failure, network issues or any other reason.

In addition, Ericom Global Cloud leverages availability zones within each datacenter, distributing workloads between them to ensure high availability and provide automatic recovery in case of zone failure.

On the application level as well, Kubernetes enables elasticity. For instance, Ericom Shield is comprised of several services, each of which has a dynamic number of instances, with the number scaling up and down based on load. The service acts as a load balancer, so every communication into Shield and within Shield is via load balancers. This enables elasticity and high availability at every level, with pod availability for each service scaling based on anticipated demand. For Ericom Shield services, pod availability scales based on observed memory and CPU utilization.

Why is elasticity important?

In any system, workflows and processes vary considerably based on user activity. Provisioning a system to handle maximum loads can keep response times low and ensure peak performance. But it is also costly and wasteful, since many resources will be idle at most times. Under-provisioning a system, on the other hand, can result in poor service and system failure as capacity gets stretched to the breaking point.

Systems that are elastic efficiently match resources allocation with resource needs at any given time. They detect changes in workflows and processes and dynamically deploy additional resources – or collapse them – as needed.

Built Using Small Units of Loosely Coupled Code

The Ericom Global Cloud leverages Kubernetes orchestration capabilities to enable applications comprising many very small containers, each generally containing code for a single process or action. For instance, Shield services comprise 20 to 30 different types of containers, each performing a specific action, such as the admin console, authorization, system backup, system monitoring, and so on.

These very small units are loosely coupled, "finding" each other via Kubernetes service discovery. Communication is primarily via REST APIs, allowing easy component replacement as long as the API is maintained.

Why is it important for the cloud to use small units of loosely coupled code?

Small containers with only a single process are preferable because all containers in a pod scale together, even if only one needs to scale up. Keeping units small minimizes the extent of scaling required and therefore reduces resource – and cost! – wastage.

In addition, the combination of tight process focus and loose coupling makes diagnosing issues and deploying updates quicker and easier.

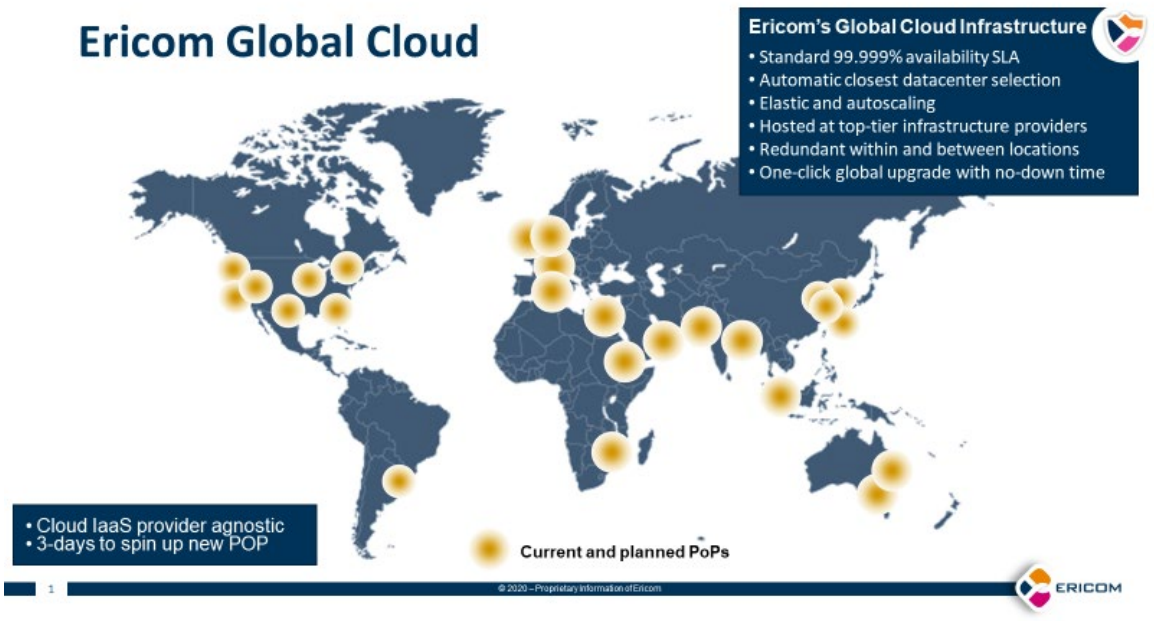
Finally, capabilities required for specific processes can be provided as narrowly as possible. For instance, for security solutions, Kubernetes provides a "secret management" capability that supports storage and management of sensitive information, such as passwords, OAuth tokens, and SSH keys, and is responsible for distributing and protecting the information. By placing security processes in their own containers, secret management need only be provided for those containers.

Globally Distributed Points of Presence

The Ericom cloud features multiple, geographically distributed points of presence (POPs) that cover major business centers across all five continents. It is designed to be cloud-agnostic: As such, our POPs are located on the clouds of multiple leading cloud vendors, including the Oracle, Ridge and AWS, with plans to expand to additional clouds based on demand.

At present, the cloud includes POPs in locations worldwide, including Phoenix, Ashburn, Sao Paulo, London, Frankfurt, Tel Aviv, Jeddah, Mumbai, Tokyo, Milan, Sydney and Malaysia, with additional locations available as needed.

Each user is automatically connected to the most rapid point of ingress, with geo- and latency-based routing minimizing latency. If the closest POP is unavailable for any reason, users are automatically shifted to the next best POP until service is restored.



This global coverage enables us to support customers worldwide, as well as multinational organizations, with seamless anywhere, anytime service.

Ericom Global Cloud POPs are centrally managed and instantly provisioned with all necessary operating data. Additional POPs may be rapidly added or removed from the Ericom Global Cloud as needed.

Why are globally distributed points-of-presence important?

Strategically located POPs optimize response times for all users, wherever they are located, while enabling local access, wherever "local" may be.

In-line Encryption/Decryption That Scales

All Ericom Global Cloud communications are encrypted/decrypted in-line using industry standard software, which provides load balancing to enable full scaling. Communication with all Ericom cloud entry points is fully secured: Admin consoles are accessible via HTTPs, with proxy mode support for both HTTP and HTTPs sites. Like all other system components, proxies auto-scale based on load to provide full in-line encryption/decryption even at peak capacity. HTTPs is required for redirect access.

Why is scalable in-line encryption/decryption important?

Services operate in dynamic environments, where customer usage patterns change rapidly. To ensure that all communications can be securely encrypted, the system must be 100% elastic, without “breaking” even at highest demand periods.

Single Pass Scanning for Malware/Sensitive Data

Ericom Cloud service integrates with leading DLP solutions to provide single pass protection against sensitive data leakage, External services including Google Web Risk and others provide protection against unknown/risky/malware sites and phishing.

Why is single pass scanning important?

Single pass scanning enables highest levels of security without the latency that can result from sequentially scanning for viruses, malware, vulnerability exploits and sensitive data. By eliminating redundant processes, single pass scanning enables superior throughput while applying all essential inspection, classification, detection and blocking processes.

Ericom Global Cloud: Compliance with Recommended SASE Cloud Features

Licensing Per User/Device as a Subscription

Licensing is per user/session and can be subscription-based

Multitenant by Design

Ericom Global Cloud is multi-tenant by design. Tenants share access to POPs and utilize browsers from a common pool. Each tenant is isolated, however, with its own reports, authentication settings and methods. For example, one tenant may use Ericom Shield with SAML authentication with ADFS, while another can do header authentication only from a list of allowed IPs,

Fully Integrated, Not Cobbled from Acquisitions

The Ericom Global Cloud is built in-house**,** leveraging leading open source products like Kubernetes. It integrates 3rd party services for specific functions, such as content disarm and reconstruction (CDR), phishing detection, and URL filtering.