TERIDION

Teridion's Unified SASE offering:

► End to End network performance optimization

► Global Route Optimization

► Self Healing Architecture

► Traffic aware optimization

► Interoperability supporting all CPE vendors + Remote users

► Cloud-native solution: Easy to scale, agile solution.

Give your users the experience they deserve.

CORONET
Security done.

The need for SASE

Ever since introduced with MPLS, the enterprise connectivity market has rapidly evolved. The market is currently abuzz with a new highly secured, cloud-based private network solution, also known as Secure Access Service Edge (SASE). This emerging offering is combining comprehensive network security functions along with broad WAN capabilities to support organizations' dynamic secure access needs.

SASE is reshaping enterprises' Networks Security and Data methodology, as those lean towards a unified, easy to manage solution that addresses their networking requirements and challenges.

Modern Enterprise Security Challenges

Nowadays enterprises are met with a new dynamic work environments, challenging their previously perimeter assets defense abilities

► Employees connect their private devices to access cloud native applications, utilizing WiFi and cellular networks which enterprises have no visibility into.

► The new reality imbalances security intrusiveness and productivity – limiting users' public networks access due to MDM (Master Data Management) use is challenging as it can reduce usability, response time, and productivity.

Teridion as the ultimate SASE partner

Teridion's cloud based global connectivity platform radically improves Internet performance through dynamic route optimization. Our network is based on various patented technologies as well as fully redundant – with no single point of failure, delivering unlimited bandwidth.

Coronet security challenges solution

Coronet represents the next generation of security architecture as it embraces BYOD (Bring Your Own Device) framework, remote work, cloud apps and constant change, as seen in the following features:

▶ Coronet deploys a nonintrusive Client-to-Any-Device (Corporate or BYOD) which ensures the device is organization-security posture compliant.

▶ Patented technology is used to ensure user's network compliancy with the organization's policy.

▶ The client is used as an anti malware agent that can identify and block malware on the device.

▶ Deep integration with leading SaaS products, allowing any service level monitoring and mitigation.

Cloud-level security policy enforcement – verified users, devices and networks allowed into cloud services are being monitored. Various cloud threats can then be automatically blocked.

▶ User-to-cloud services connectivity remains direct and native. Coronet's ability to exist within the service eliminates the need for a gateway, as all inspections are done at the service level.

How Coronet and Teridion provide the best of breed SASE solution

Assembling the joint capabilities of Coronet and Teridion creates a Cloud-Native-Security for their customers, enabling a wide coverage of SaaS products while boosting network performance for any client, in any location.

Together we deliver a dynamic, policy based, Secured access edge service, regardless of the requesting entities and the requested networked capabilities locations.

Seamless integration between Coronet Client Software and Teridion Access network ensures easy operation and low cost of ownership for the customers.
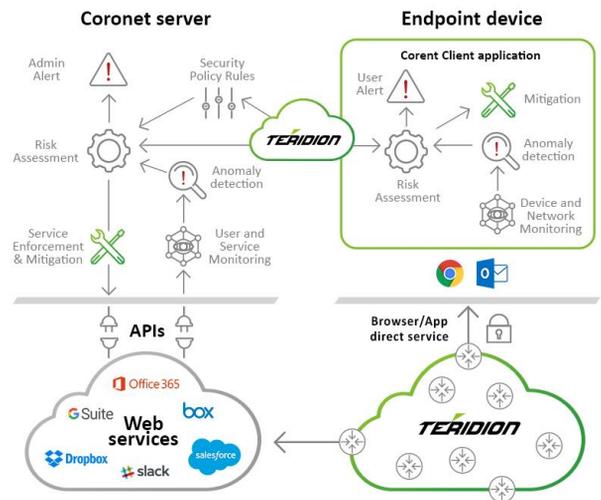
Teridion at a glance

3x-15x
Performance gain

2,000+
Virtual routers

100+ TB
Daily Traffic

Supports all
geographies