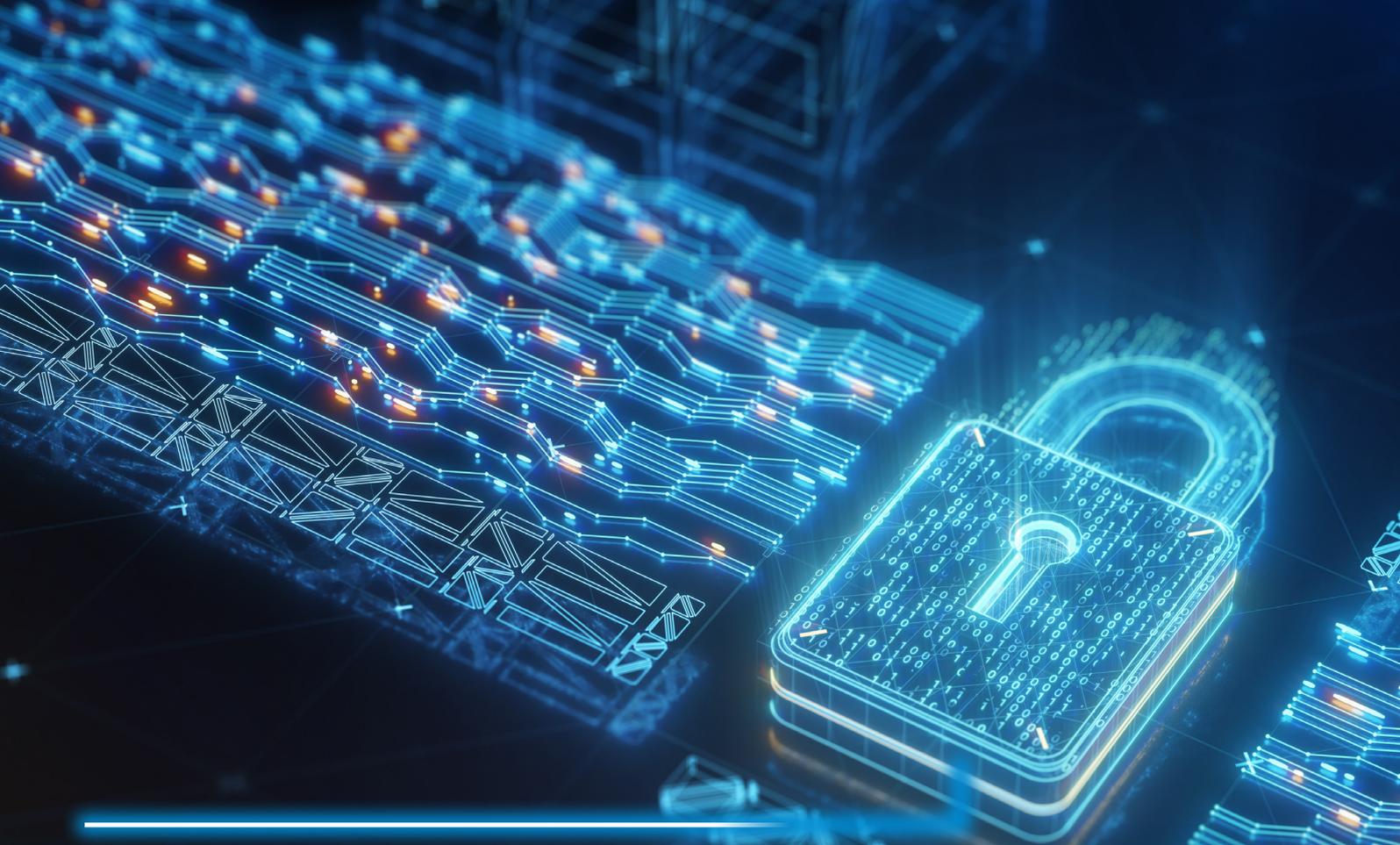




SASE CONNECT

SECURITY OVER YOUR LIMITLESS
CONNECTIVITY ECOSYSTEM

A futuristic digital landscape with glowing blue lines and a large padlock icon. The background is a dark blue with intricate patterns of light blue and orange lines, resembling a complex network or data flow. A large, glowing blue padlock icon is positioned on the right side, symbolizing security. A horizontal blue line is located below the padlock icon.

VALUE PROPOSITION

SASE Connect allows secure internet access for remote workers, IoT devices, branch offices and applications before forwarding the traffic through a multitude of destinations. This ironclad security solution will serve users wherever they are located.

If, in the past, VPNs were used to reinforce security policies by protecting end users from wiretapping, nowadays workers and devices are even more connected to cloud applications through the public internet, which requires a new approach to protect their assets from security threats. Plus, the newborn web 3.0 is spreading this need further and bringing it to an even higher scale.

The security components of SASE Connect bring together multiple layers of protection and provide a unified front against cyber threats.

In addition, a multi-function solution gives the flexibility to choose the specific security features in use at any given time. Enterprises can tailor their need-based solution choosing from a plenty of security functions included in SASE Connect range. With SASE Connect, the benefits of cloud consumption models can now be applied to security.

SASE Connect brings the cloud's scalability and simplicity to cyber protection, simplifying its deployment and consumption for enterprises of all sizes. This allows companies to customize their digital transformation strategy and meet any security needs arising along their journey.



ADOPTING THE RIGHT SECURITY STRATEGY

Growing security issues with cloud platforms force organizations to implement strict security countermeasures designed to protect their data stored in the cloud. With the increasing complexity of cloud-targeted cyber attacks, it becomes impossible for a single security product to fight them all.



The global shift to remote and hybrid workplace models has brought into play more attack surfaces, that is more potential hacker targets.

With the evolution of security measures in recent years, cyber threats have also evolved into multiple types, each targeting a specific vulnerability. Different security measures work individually to defend against different types of threats, but a single cyber attack can be comprised of multiple attack types, forming a cyber kill chain.

This highlights why a unified cyber security strategy consisting of multiple solutions like SASE is the right approach towards cloud security.



THE BENEFITS OF SPARKLE SASE CONNECT

Sparkle SASE Connect's distinctive benefits:

- **LOW LATENCY CONNECTIVITY AND PERFORMANCE**

Direct-to-cloud connectivity to eliminate backhauling and reduce latency

- **OPTIMIZATION**

Bundling with Sparkle's connectivity solutions for Enterprises, independently of any underlying transport technology (MPLS/DIA, etc.)

- **SIMPLIFICATION**

Flexible deployment to deliver a tailor-made SASE solution to customers. Tasks that were previously labor-intensive (e.g., branch site deployment, workflow template, automated security optimization, event correlation and active remediation) can now be addressed without any need for manual intervention

- **ASSURANCE**

Automated assurance is paramount to achieve the expected level of customer service experience. At Sparkle, the E2E Assurance process is internally managed, including a full monitoring of network and security components, which avoids delays in opening tickets with different service providers

WHY SPARKLE

Leading global service provider offering a full range of ICT solutions, global connectivity, services and capabilities designed to meet the ever-changing needs of enterprises, OTTs and content players, ISPs, fixed and mobile operators

State-of-the-art global network with proprietary backbones in Europe, the Mediterranean basin and the Americas and ownership in submarine cables connecting Europe to South-East Asia and the Americas

Sparkle's SOC is an organized and highly skilled team capable of monitoring and improving the security position of organizations by preventing, detecting, analyzing and responding to cyber security attacks

The strategic nature of Sparkle allows us to do business in peculiar sectors such as defense and national security leveraging on our ISO/IEC 27001 and NOSIS certifications

MEF certified solution and pioneering MEF member

