ericsson.com/
service-orchestration

Enterprise service orchestration

Enterprise security use case

November 2020

The need for enterprise security services

The global enterprise services market was worth USD 1.7 trillion in 2020, with a compound annual growth rate (CAGR) of 9.4 percent[1].

However, the enterprise connectivity market share is expected to decrease from 48 percent to 19 percent by 2026.

As an adjacent market to connectivity which requires close integration to the network, the enterprise security market is an obvious target segment for communication service providers. The enterprise security market is estimated to be worth USD 52 billion in 2020, with a CAGR of 11 percent and a market share similar to network infrastructure, workspace and IT applications of around 11 percent making it an attractive segment for services beyond communications.

And, because enterprise security is so closely linked to enterprise connectivity, they are often bundled together, with the majority of enterprises seeing security services as critical for business.

What are enterprise security services?

Enterprise security services cover a series of virtual network function (VNF) powered services or service chains that provide network security either on premise using universal CPE (uCPE), or in the cloud using virtual CPE (vCPE) to host the virtual functions.

Enterprise security services include VPN, deep packet inspection (DPI), firewalls and distributed denial of service (DDoS) which are all orchestrated services.

Firewalls are the most common type of enterprise security solution deployed. Their role is to monitor incoming and outgoing traffic based on predetermined security rules. They are used to separate trusted networks, such as corporate VPNs, from untrusted networks, such as the internet.

Understanding the business problem

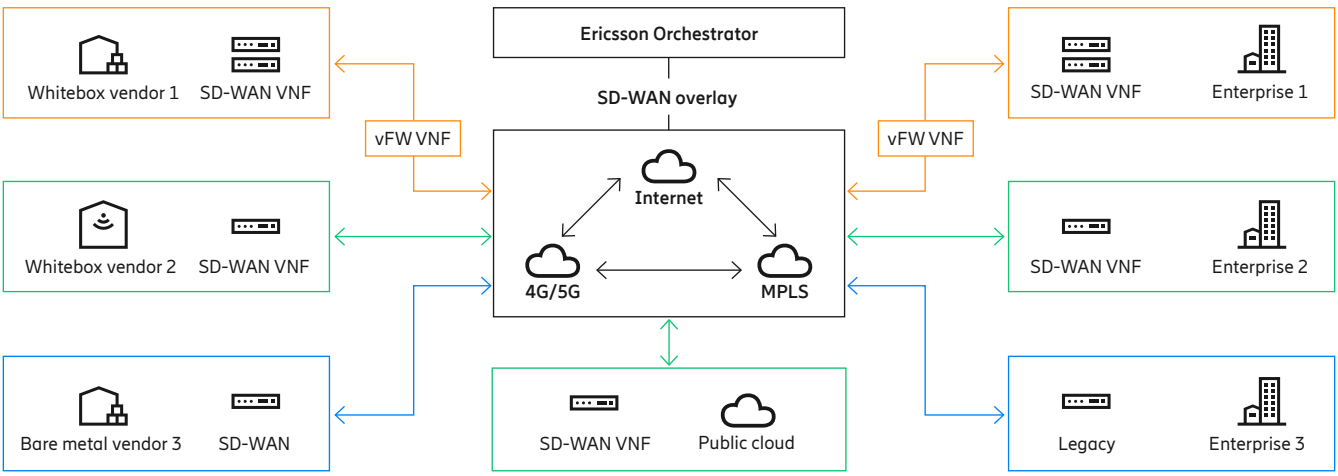
Cyber-security breaches can have a huge impact on enterprises. Organized ransomware attacks can paralyze businesses for weeks, as well as costing millions to release the systems.

In 2020, the National Cybersecurity Centre, part of British Intelligence organization GCHQ, stated that there had been a 10 percent increase in cyber-attacks since the previous year. In April 2020, for example, travel money firm, Travelex, was hit by a ransomware attack and had to pay USD 2.3 million in bitcoin to regain control of its systems.

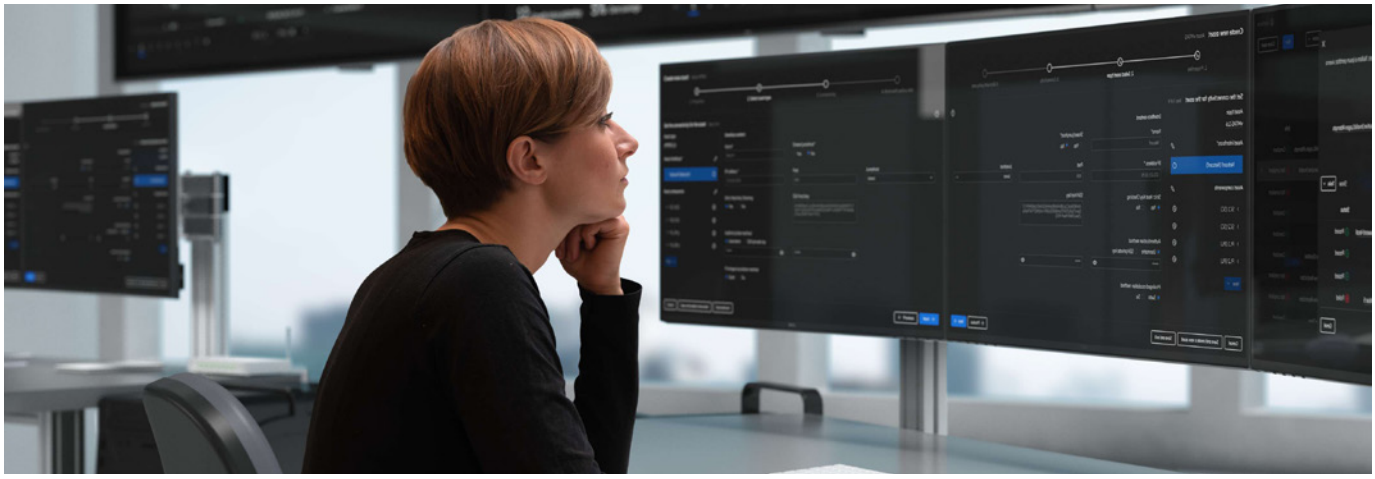
In 2020, a number of companies and universities involved in COVID-19 vaccine research reported a large number of targeted attacks believed to be attempts to steal research data which is potentially worth billions of dollars. Successful cyber-attacks can lead to significant financial losses and can potentially affect share prices.

Finally, the COVID-19 pandemic has driven many enterprises to distribute their organizations with vast numbers of new home-based workers, potentially creating a much larger number of potential attack entry points for a distributed enterprise, and so they need to extend these capabilities, which are usually deployed in offices, out to the home environment to ensure security.

Figure 1. Enterprise security



[1]Source for market data: Frost and Sullivan: Frost Radar™ North American managed services SD-WAN market 2020



Enterprise security services represent a significant opportunity to grow enterprise revenue for CSPs.

Ericsson's solution

Ericsson's solution for enterprise security is to deploy Ericsson Orchestrator, including the Cloud Manager and Evolved VNF Manager components, to orchestrate third-party security applications. These security solutions, typically firewalls, are deployed as VNFs which can be deployed at uCPE, vCPE or on public cloud to provide end-to-end security.

In addition, Ericsson have pre-integrated the Ericsson Orchestrator with several leading enterprise security vendors including Palo Alto, Checkpoint and Fortinet. This pre-integration accelerates the implementation of enterprise security with these vendors.

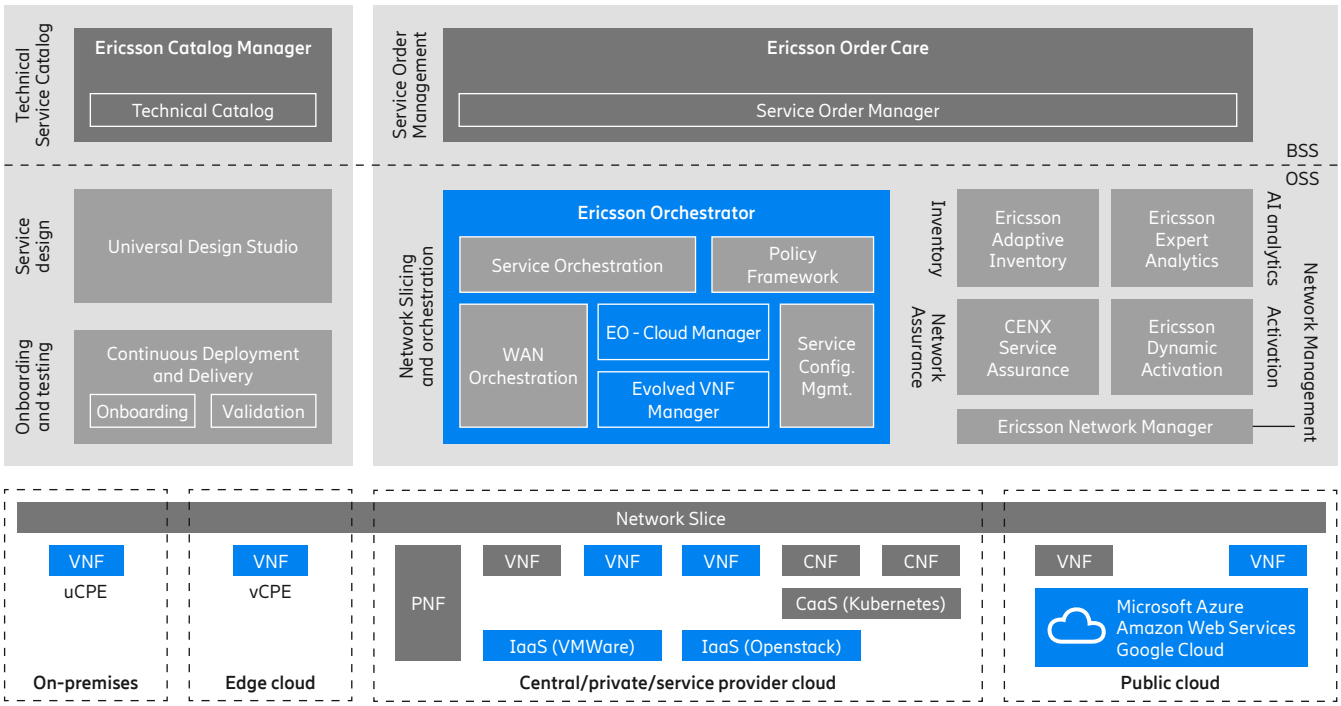
The impact of enterprise security

Enterprise cyber-security is essential for modern enterprise businesses, and because it is tightly linked to network connectivity, it makes sense for connectivity providers, usually service providers, to deliver enterprise security as a bundle with connectivity.

Combined enterprise offers such as SD-WAN plus WAN optimization and enterprise security are compelling, taking the service provider beyond traditional communications services. In recent years, there have been a number of acquisitions of security vendors and professional services companies by both service providers and network equipment vendors (NEPs) as they aim to strengthen their security portfolios.

The potential financial and commercial impact of a successful cyber-attack means that there is a willingness to invest and a tendency not to be price sensitive. Service providers able to offer standalone and bundled enterprise security services have a significant opportunity to grow their enterprise revenues for services beyond communication.

Figure 2. Ericsson Dynamic Orchestration – Portfolio – security highlighted



Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

www.ericsson.com

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

7/0341 FGB 101 0800 Uen