

CASE STUDY

Leading Healthcare Solutions Provider Improves Business Continuity Through Secure SD-WAN Infrastructure

For over 30 years, Gruppo Servizi Italia has been meeting the evolving needs of the healthcare sector through a range of integrated solutions including the rental and sterilization of medical equipment and textiles, laundry services, and various clinical engineering services. Production takes place in 56 plants located in Italy, Brazil, Turkey, Morocco, Albania, India and Singapore. Thanks to a multi-service approach, The Servizi Italia Group is now able to provide a wide range of activities, offering a mix of tailor-made products.

The Challenge of Service Continuity in a Changing Environment

Servizi Italia's operations depend on a complex web of synchronized transactions between the company headquarters and data center in the province of Parma, Northern Italy, and its global network of processing plants and contractors. With hospitals and other critical healthcare providers depending on the timely delivery of key equipment and other provisions, service continuity has always been of mission-critical importance to Servizi Italia's information and communications technology (ICT) operations. Without sufficient network resilience or cybersecurity, even a minor network failure or security breach could potentially delay a life-saving operation due to the lack of critical sterilized equipment.

Therefore, as the ICT group began a process of digital transformation, adapting its systems to the evolving needs of its customers through the adoption of new cloud and hybrid services, the company was especially concerned with the potential performance and security implications.

Relying on existing centralized security checks could result in poor performance or even application timeouts, as all network traffic was backhauled through the data center. However, opening direct internet access at the network edge and thus bypassing such checks would expose the company to unacceptable levels of risk.

What was needed was a whole new architectural approach to networking and security.

The Transition to Secure SD-WAN

The solution to this challenge lay in the adoption of a new software-defined wide-area network (SD-WAN) infrastructure, where previous dedicated WAN connections linking the plants, contractors, HQ, and data center could be replaced with a more flexible, cost-effective network using locally available broadband connections.

"We knew that SD-WAN technology could potentially help meet our requirements in terms of performance and cost," explains Dr. Andrea Ruscitti, CTO and ICT officer manager for Servizi Italia, "but we also knew that not all solutions would provide the levels of security and network resilience that we required."

Another key concern was manageability. Without broad visibility of the whole network and its traffic, problem resolution had been a slow and resource-intensive process for Servizi Italia, in which multiple tests might need to be run just to identify the root cause of a problem. The result was that a simple link failure could sometimes take an hour or more to pinpoint and rectify.



"We knew that SD-WAN technology could potentially help meet our requirements in terms of performance and cost, but we also knew that not all solutions would provide the levels of security and network resilience that we required."

– Dr. Andrea Ruscitti, CTO and ICT Officer Manager, Servizi Italia

Details

Customer: Servizi Italia

Industry: Healthcare

Location: Italy

Business Impact

- 60% reduction in overall downtime
- Up to 100-fold reduction in typical service outage duration
- 25% reduction in the number of mobile backup links
- Significantly reduced management complexity
- Increased customer satisfaction and reduced support overhead

With a clear understanding of its requirements, Servizi Italia turned to trusted partner Mead Informatica, to assist in the selection of a suitably secure SD-WAN solution. After careful evaluation of several contenders, FortiGate Secure SD-WAN, based on FortiGate Next-Generation Firewalls (NGFWs) with FortiManager automation-driven network management, quickly emerged as a clear leader.

“The tight integration of industry-leading security and advanced SD-WAN technology within a single competitively priced platform made Fortinet a great fit for our requirements,” adds Dr. Ruscitti.

The deployment of FortiManager provided a single management console with rich SD-WAN analytics, enabling Dr. Ruscitti and the team to fine-tune the company’s business and security policies and quickly improve the overall quality of service for all users.

The advanced and adaptive self-healing WAN automation within the FortiGate Secure SD-WAN solution helps to provide an even smoother and more consistent experience for users by seamlessly switching to alternative WAN links in the event of failure. Furthermore, through more intelligent optimization of the available communications paths, Servizi Italia has been able to reduce the total number of 4G backup links by around 25%. In keeping the remaining links active, total bandwidth has been increased, maximizing the overall return on investment.

“The difference is night and day,” admits Dr. Ruscitti. “Service interruptions are far less frequent and when they do occur, their duration is now measured in minutes instead of hours—about a hundred-fold reduction.”

To further improve cloud application response times, while strengthening protection and availability, Servizi Italia also added three FortiADC application delivery controllers deployed as virtual machines.

For enhanced security and management of wired and wireless device access across the organization, the group subsequently deployed FortiSwitch secure Ethernet switches and FortiAP secure wireless access points. From a management perspective, these become logical extensions of Secure SD-WAN to SD-Branch.

With SD-Branch in place, this enables centralized management of the LAN through FortiManager and brings device access within the protective framework of the Fortinet Security Fabric, which proactively collates threat information from multiple Fortinet solutions across the network and applies artificial intelligence (AI)-driven automation to determine the most appropriate response.

The final crucial component of any Fortinet solution is the threat intelligence delivered by FortiGuard Labs. Gathering threat information from customer networks around the world, hundreds of analysts employ the latest machine learning and AI tools to process over 100 billion events per day. This collection, correlation, and delivery of real-time threat intelligence provides enterprises such as Servizi Italia with comprehensive and actionable security updates across the full range of threats encountered.

A Secure Foundation for Future Digital Innovation

Since the arrival of the COVID-19 pandemic, Servizi Italia, like most organizations around the world, has faced increased pressure to offer secure remote working solutions.

To address this need and reap the additional benefits of a mobile workforce such as reduced overhead and increased employee satisfaction, Dr. Ruscitti and the team plan to expand its use of FortiGate’s integrated virtual private network (VPN) functionality as well as the new Zero Trust Network Access capabilities now available within FortiOS, the platform’s operating system.

In addition to this, Servizi Italia plan to continue its migration of IT services to the cloud, knowing that its partnership with Fortinet and its deployment of the Fortinet Security Fabric will continue to provide the organization with the highest levels of network performance, reliability, and protection.

Solutions

- FortiGate Secure SD-WAN
- FortiSwitch
- FortiAP
- FortiADC
- FortiManager

“The tight integration of industry-leading security and advanced SD-WAN technology within a single competitively priced platform made Fortinet a great fit for our requirements.”

– Dr. Andrea Ruscitti, CTO and ICT Officer Manager, Servizi Italia



www.fortinet.com