CASE STUDY

New Integrated Security Infrastructure for Portugal's Leading Provider of Road Services

From the award of its first concession (Norte) in 1999 for the 179 km artery linking the northern Portugal coast with the mountainous inland region by the Spanish border, Ascendi has grown to become one of Portugal's leading providers of road infrastructure services and asset management. For over 20 years, Ascendi's success has been underpinned by a continuous drive to deliver service excellence through creativity, innovation, and operational efficiency. Its pioneering free-flow toll systems have become a European reference, showcasing how safe, automated toll-collection services can increase revenues through improved traffic flow and reduced congestion.

The Data Beneath the Road Network

For Ascendi, management of Portugal's road infrastructure requires careful measurement and processing of multiple inputs such as weather conditions (temperature, wind speed, precipitation), traffic speed and density, vehicle weight, and the state of the road surface—each taken at regular intervals around the entirety of the infrastructure. This real-time data is then integrated with historical data within Ascendi's innovative SustIMS maintenance management system to enable predictions of infrastructure degradation and inform the decision-making process for resource allocation and investment.

In network terms, these efforts require the interconnection of over 50,000 telematics devices such as sensors, radars, sonars, and cameras, the data from which are carried over a variety of transports including a principal fiber-optic ring, to be processed at a central data center.

In addition to this, the network delivers a wide range of web applications and services, both to the general public via its self-service web portal, and to the company's 670 staff, 320 of which work in the central operations and management centers, with the rest located at remote offices or on the road.

Similar to many organizations since the global outbreak of the COVID-19 pandemic, Ascendi has also faced a dramatic increase in the number of employees working from home.

Security Integrated by Design, Privacy by Default

For Ascendi's IT team, this unique set of requirements presented a number of challenges; one of the biggest was how to properly and efficiently protect all the myriad moving parts that comprise the critical data network underpinning the business.

Having concluded that their existing perimeter firewall was no longer sufficient, Ascendi started to look for a broader, more all-encompassing solution in which networking, security, and data privacy would be an inherent part of each infrastructure component, rather than something separate to be applied as an afterthought.

ascendi

"We compared a lot of metrics such as data throughput, resilience, feature breadth and ease of management, but the most critical of these was to have a single console with full visibility and central policy control across everything."

– Adriano Carvalho,
Head of IT, Ascendi

Details

Customer: Ascendi

Industry: Transportation

Location: Portugal

Business Impact

- Increased efficiency with streamlined operations
- Managed risks with strong security posture and data privacy
- Protected entire attack surface and kept operations running
- Reduced downtime with resilient, highly available system

The new solution would have to cover every part of the infrastructure, which would equate to protecting the entire attack surface where all possible interactions between its users, systems, and devices take place. This meant securing everything from client devices to email systems, web and application delivery servers, and the switches that interconnect them all. Most importantly, they would need a solution in which all constituent parts could act in unison in accordance with common centrally defined security policies. Instead of creating yet more separate pockets of specialized security functions, each tasked with protecting individual data flows, Ascendi wanted seamless protection that would encompass their entire infrastructure today while intelligently adapting to the needs of tomorrow.

Central Visibility and Control

With guidance from a major consulting group, Ascendi drew up a shortlist of security vendors and evaluated each according to a strict set of criteria.

"We compared a lot of metrics such as data throughput, resilience, feature breadth and ease of management," explains Adriano Carvalho, head of IT for Ascendi, "but the most critical of these was to have a single console with full visibility and central policy control across everything."

Following extensive proof-of-concept testing, the solution finally proven to best satisfy all these requirements, and above all that of centralized visibility, control, and management, was from Fortinet. By exploiting the unique and innovative cybersecurity platform known as the Fortinet Security Fabric, Ascendi could choose from an extensive range of proven security solutions to create an infrastructure greater than the sum of its parts.

With purpose-built security processors, and their ability to identify thousands of applications within the data flow for deep inspection and protection with granular policy enforcement, FortiGate next-generation firewalls (NGFWs) were deployed to interconnect the various parts of the network and to segment the combined traffic according to application, user, or device with Security-Driven Networking.

Solutions

- FortiGate
- FortiMail
- FortiWeb
- FortiAuthenticator
- FortiToken
- FortiADC
- FortiClient
- FortiManager
- FortiAnalyzer

"The Fortinet approach was the best fit for us, not just because of its strong protection across all the bases—firewall, switches, email protection, web protection, etc.—but in the way that the protection all comes together under the Fortinet Security Fabric."

– Adriano Carvalho,
Head of IT, Ascendi

To extend automated next-generation threat protection, visibility, and control to Ascendi's remote and mobile workforce, as well as to accommodate the COVID-driven surge in remote access across the organization, Ascendi deployed the FortiClient endpoint protection solution with multi-factor authentication provided by FortiToken to ensure that only trusted users can access the network.

Due to the critical role of Ascendi's public web portal as well as applications such as GIS, Exchange, and Q-Free for example, Ascendi deployed the Fortinet web application firewall solution, FortiWeb, as well as the application delivery controller, FortiADC, to ensure the strongest performance and protection against both known and unknown attacks.

To further protect Ascendi from the kinds of volume-based and targeted attacks that propagate via email, as well as to help prevent the loss of sensitive data and maintain compliance with regulations, the FortiMail solution was also deployed.

"The Fortinet approach was the best fit for us, not just because of its strong protection across all the bases—firewall, switches, email protection, web protection, etc.," adds Carvalho, "but in the way that the protection all comes together under the Fortinet Security Fabric."

With each product linked through its integration with the FortiGate firewalls and their FortiOS operating system, the Fortinet Security Fabric brings consistent configuration and policy management as well as effortless, real-time communication across the entire security infrastructure to make effective and contextual security solutions.

FortiManager and FortiAnalyzer provide the centralized window and interface through which Ascendi can now monitor, analyze, and control their critical data flows. With advanced automation and response capabilities, as well as proactive threat detection and correlation, the Fortinet Security Fabric cuts the time taken to detect and mitigate threats and reduces the security risks that might otherwise arise from configuration errors or manual data compilation.

External threat intelligence is provided by FortiGuard Labs, which collates and processes the data from millions of anonymized sensors and over 200 global partners around the world using artificial intelligence and machine learning to identify unique features for both known and unknown threats.

To maximize the overall protection and value from their solution, Ascendi also made use of the experience and technical expertise of the Fortinet Professional Services team. This helped ensure a smooth and rapid transition to the new architecture and provided peace of mind that every part of the infrastructure was correctly and optimally configured.

FORTINET®

www.fortinet.com

April 10, 2021 2:30 AM

D:\Fortinet\2021 Rebranded templates\Case Studies\March\Ascendi\cs-FA-new-integrated-security-infrastructure-462021\cs-FA-new-integrated-security-infrastructure-462021

943259-0-0-EN