

## CASE STUDY

# Global Low-Code Pioneer Improves Resilience and Cuts Management Complexity Both On-Premises and in the Cloud

Founded in 2001 with the vision to transform how enterprise software is delivered, OutSystems pioneered the low-code market in Europe and is today recognized as a global leader in high-performance application development. With headquarters in Lisbon, Portugal; and Boston, MA, the company employs more than 1,700 employees globally. It has more than 600,000 community members, 400 partners and active customers in 87 countries across 22 industries.

As the company has grown, so too has the complexity of managing its network infrastructure and the systems that staff use on a daily basis. A couple of years ago, it was time for a networking and security change.

## Complexity Makes for Burdensome Firewall Management

The first challenge that OutSystems tackled was inefficient security within the company's wide area network (WAN). The OutSystems network and security team manages the company's WAN infrastructure for locations across Europe, Asia, and North America. Each remote office uses at least two separate internet service providers (ISPs) to ensure business continuity, while the Lisbon headquarters uses three for maximum resilience.

For several years, OutSystems had relied on FortiGate Next-Generation Firewalls (NGFWs) to protect its data centers and office locations. "Each time our services evolved, security was updated through the addition of new firewall rules," explains Óscar Rodrigues, TechOps Network and Security Lead for OutSystems. "Although this kept us safe, we had a significant number of rules, which was becoming unmanageable. What we needed was a solution that could help us reduce that burden and simplify ongoing administration."

Rodrigues saw an opportunity to simultaneously improve WAN performance and resilience and reduce the complexity of network administration. He and the team upgraded the legacy firewalls for OutSystems to a new FortiGate cluster and leveraged the integrated software-defined WAN, or SD-WAN, feature to optimize traffic and automate failover for its offices.

The team designed a new topology for the OutSystems WAN. They rationalized the many security rules, developed a new nomenclature, and adopted only the rules that were necessary. The new topology implementation started with remote offices. It permitted the company to change the process of firewall rule configuration and it decreased firewall policy rule number and management.



*"Each time our services evolved, security was updated through the addition of new firewall rules. Although this kept us safe, it was becoming unmanageable. What we needed was a solution that could help us reduce that burden and simplify ongoing administration."*

**Óscar Rodrigues**  
TechOps Network and Security  
Lead for OutSystems

## Details:

**Customer:** OutSystems

**Industry:** Technology

**Location:** Portugal and the United States

**Number of Secure SD-WAN Locations:** 8

## Business Impact

- Reduced operations overhead through simplified infrastructure management
- 85% reduction in number of firewall security rules, easing management complexity

## Simplification through SD-WAN

Now, Fortinet Secure SD-WAN protects traffic between OutSystems locations, while also optimizing performance by routing traffic to whichever ISP connection works best for that particular communication. In addition, the SD-WAN solution provides automatic failover, without the need for manual intervention, in the event that one of the ISP connections fails.

“Before the migration, network connectivity issues could be quite time-consuming to resolve,” explains Rodrigues. “But with Fortinet’s integrated SD-WAN capabilities, we can now pinpoint their cause really quickly—even subtle problems, such as intermittent packet loss from one of the multiple ISPs, are easily identified through the central management console.”

The new FortiGate cluster made the WAN much easier to manage. “Previously, we were using approximately 35 public IP addresses,” recounts Rodrigues. “With the new Fortinet infrastructure, we have been able to reduce this to just five IP addresses. During the migration, all firewall rules were reviewed and multiple interface policies implemented. SD-WAN, together with the multiple interface policy and policy review, permits us to decrease rules by nearly 85%.”

## Internal Workloads Migrate to Cloud

After the SD-WAN infrastructure was functional, Rodrigues and the team set their sights on streamlining management of the company’s crucial internal workloads. As a software innovator, OutSystems relies heavily on its own internally developed applications. Managers and employees needed to access these servers from remote locations all around the world.

The obvious solution was to shift to a distributed, cloud-based architecture. By moving from on-premises data centers to the cloud, internal applications would be able to leverage many of the same economies of scale, flexibility, and performance advantages that OutSystems’ low-code applications and services provide to the company’s customers. OutSystems decided to transition away from its existing, on-premises approach to delivering internal services and instead to utilize a cloud-based architecture with three interconnected virtual data centers.

Properly safeguarding the company’s reputation and assets, while maximizing the cyber resilience of operations and services—both on-premises and in the cloud—would require a leading-edge, agile security infrastructure.

## Better Control through Integrated Security

Rodrigues and the team evaluated a shortlist of cybersecurity solution vendors, looking at their ability to provide the protection and visibility that OutSystems requires. The due diligence process led them to expand their Fortinet footprint to include cloud-based security as well as on-premises.

“Fortinet had solutions to all our cloud-security needs,” adds Rodrigues, “but it was the seamless integration with the cloud and the ease of management that really stood out.”

This integration enabled OutSystems to rapidly apply all the necessary security controls at all critical points throughout its cloud environments, including on all traffic from each of its virtual WAN hubs. And as OutSystems was using the same FortiGate NGFWs in the cloud as it had been using on-premises, it was able to leverage all the work already done to optimize the security rules and ensure that the security infrastructure for its cloud environments would be streamlined.

## Business Impact (cont.)

- 86% reduction in public IP addresses, significantly reducing management time and costs
- Strengthened protection of company reputation and assets through enhanced application security, reporting, and analysis
- Increased business continuity through automated network performance, flexibility, scalability, and resilience

## Solutions

- FortiGate Next-Generation Firewalls
- FortiGate VM
- Fortinet Secure SD-WAN
- FortiWeb
- FortiView
- FortiAnalyzer

*“Fortinet had solutions to all our cloud-security needs, but it was the seamless integration with the cloud and the ease of management that really stood out.”*

### Óscar Rodrigues

TechOps Network and Security Lead for OutSystems



OutSystems also deployed the FortiWeb web application and application programming interface (API) protection (WAAP) solution for advanced protection of the company's multiple web portals and back-end APIs. Using machine learning to automatically model each application, FortiWeb protects OutSystems web services from known vulnerability exploits as well as unknown threats, all while minimizing friction for the development and the security teams. Advanced bot mitigation accurately differentiates between good and malicious bot traffic, providing Rodrigues and the team with the visibility and control they need, without slowing down legitimate users with unnecessary CAPTCHA security tests or challenges.

## Single-Pane-of-Glass Management for All Security On-Premises and in the Cloud

Through an integrated suite of graphical analysis tools called FortiView that integrates with FortiWeb, OutSystems staff can get an actionable picture of their entire web traffic. They can pinpoint potential weak spots by drilling down into key metrics such as server/IP configurations, attack and traffic logs, attack maps, and OWASP Top 10 attack categorization, as well as user activity.

To increase accountability and enable its security posture to adapt to the evolving

threat landscape, OutSystems also deployed FortiAnalyzer. With centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining, and vulnerability assessment, FortiAnalyzer allows Rodrigues and the team to see and precisely measure the impact of their security interventions.

## A Solid Foundation for Future Growth

Moving internal workloads from physical, on-site data centers to a distributed cloud infrastructure has enabled OutSystems to raise security levels while dramatically reducing management complexity, freeing Rodrigues and the team to focus on supporting the needs of their growing business.

"With Fortinet, we now have visibility and control over everything. We can even spot potential problems before they start to have an impact on our users," Rodrigues says.

*"Before the migration, network connectivity issues could be quite time-consuming to resolve. But with Fortinet's integrated SD-WAN capabilities, we can now pinpoint their cause really quickly—even subtle problems, such as intermittent packet loss from one of the multiple ISPs, are easily identified."*

**Óscar Rodrigues**  
TechOps Network and Security  
Lead for OutSystems



[www.fortinet.com](http://www.fortinet.com)