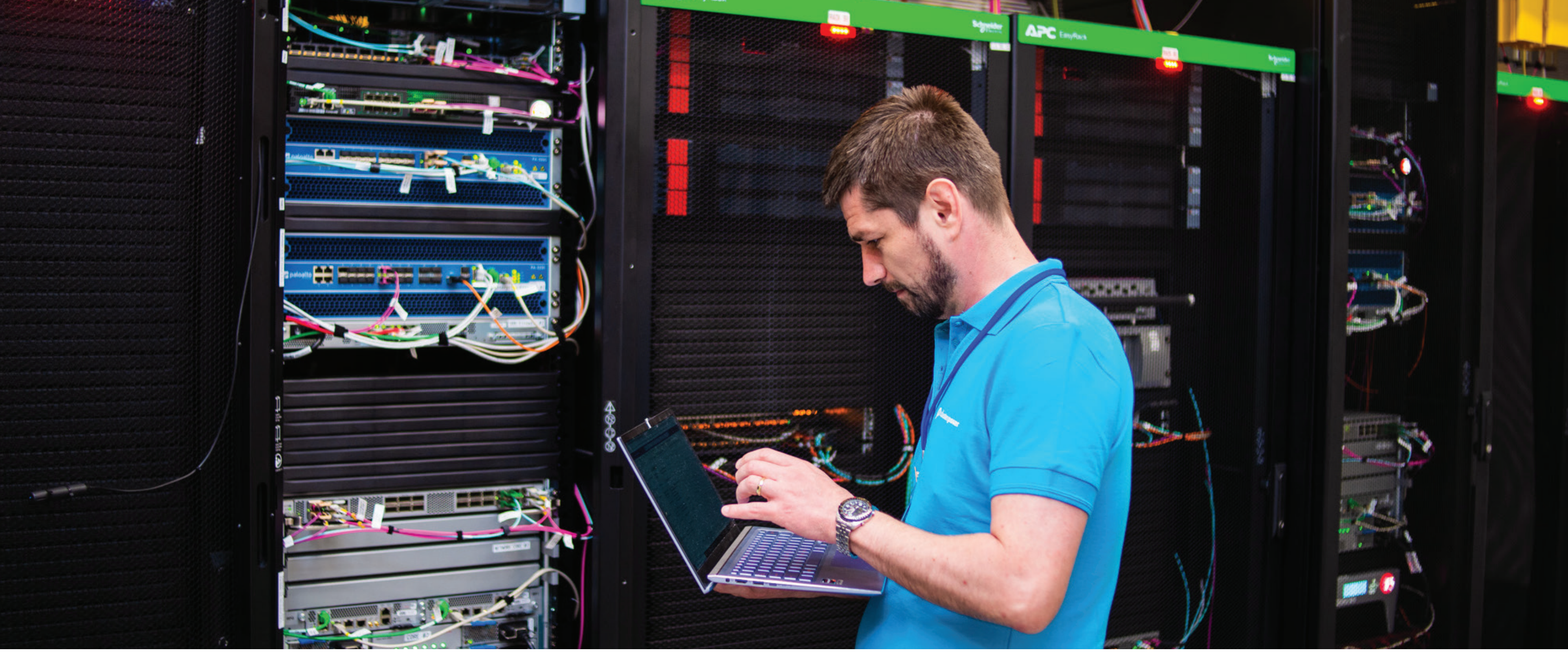

CASE STUDY

ClusterPower manages risk and maximises opportunities with Palo Alto Networks

Cloud service provider (CSP) ClusterPower is fast-forwarding Romania's digital transformation. By standardising on a scalable and adaptive Palo Alto Networks network security strategy, the organisation is safeguarding customer infrastructures, based on a prevention-focused architecture. Customers can now launch innovative new services more quickly, safe in the knowledge their underlying data is secure, fast, and reliable.

IN BRIEF

Customer
ClusterPower

Organisation Size
200-megawatt technology campus

Industry
Technology

Featured Products and Services
CSP services, including infrastructure as a service, application optimisation, and cloud gaming

Location
Bucharest, Romania

Challenges

Starting from a greenfield data centre infrastructure, this Romanian CSP required a trusted and scalable security model to protect customer data. For added security, ClusterPower wanted to use network segmentation to prevent attackers moving through the network.

Requirements

+ Collaborative partner to share security innovations and support growth.
+ Powerful, simple, and versatile network security platform.
+ Capability to divide network into multiple segments.
+ Scalable, high-performance network security, proven to deliver in data centre.

Solution

Palo Alto Networks ML-Powered Next-Generation Firewalls, with Cloud-Delivered Security Services, including Threat Prevention, Advanced URL Filtering, and GlobalProtect

CHALLENGES

High-performance computing in the heart of Europe

ClusterPower is spearheading digital transformation in Romania and neighbouring countries. Founded in 2019, this leading CSP offers customers a scalable high-performance computing infrastructure in the heart of Europe.

ClusterPower has two predominant lines of business. First, wholesale co-location capacity for large enterprises or third-party data centre providers looking for additional capacity. Second, a scalable cloud infrastructure for any type of organisational cloud need.

"Customers trust ClusterPower with their most valuable asset – data – so the infrastructure must be 100% safe," says Vladimir Ester, Chief Technology Officer, ClusterPower. "We need to see and secure everything in our data centre, using a proactive, intelligent strategy to keep networks safe."

The organisation's 200-megawatt, 25,000 square metre technology campus began as a 'greenfield' project. At the outset of development, one of the primary decisions for Ester and his team was to choose a data security partner. But which one?

Ester explains: "I've been an infrastructure guy all my career, dealing with hundreds of vendors. Palo Alto Networks has always stood out as a forward-thinking global leader in infrastructure security. Their tightly integrated security portfolio was the ideal choice to safeguard our new infrastructure. The rich feature set and proven capability are real differentiators during negotiations with prospective customers."

REQUIREMENTS

A collaborative partner for the long term

Ester and his team wanted a network security partner, not a ‘sell and go’ vendor. They required:

- An innovative collaborative partner to share security innovations and support ClusterPower’s growth.
- A powerful, simple, and versatile network security platform offering comprehensive protection.
- The capability to divide their network into multiple segments.
- Best-in-class network security, proven to deliver in scalable data centre environments.

SOLUTION

Best-in-class security made easy

Following a rigorous evaluation of leading network security providers, ClusterPower has recently deployed two Palo Alto Networks ML-Powered Next-Generation Firewall (NGFW) clusters. The platform uses ML to deliver inline signatureless attack prevention for file-based attacks while simultaneously preventing unknown threats. It also natively classifies all traffic – applications, threats, and content – connecting that traffic to the user regardless of location or device type.

“As a cloud services provider, we offer customers two security options. First, firewall capacity in a public tenant, which protects customer applications and machines in the same way ClusterPower protects its own environment. The second is a segregated firewall solution,” says Vladimir.

This network segregation enables ClusterPower to create separate security policies by application, user, and content for each customer network. “Network segmentation limits the attack surface to specific groups of users. This in turn reduces the threat from vulnerabilities and ensures ClusterPower meets the guaranteed SLAs we offer to customers,” says Vladimir.

A connected suite of Cloud-Delivered Security Services (CDSS) completes the picture, providing layer upon layer of additional defence. The Advanced URL Filtering subscription, for example, can analyse live web traffic in real time and provide instant protection against the latest web-based threats like phishing. According to Vladimir, it generates a more accurate analysis of URLs than would be possible with traditional web database filtering techniques.

He says: “In time, we will offer customers a parental control application, so traffic can be filtered on children’s devices. With Advanced URL Filtering we’ll be able to block unwanted websites, applying customised protection to online data searching.”

Likewise, GlobalProtect is offered as an optional CSP service. Customers have the flexibility to extend consistent security from the ML-Powered NGFW to their remote users, wherever they are based and through any device.

BENEFITS

Driving digital change in Romania

This innovative Palo Alto Networks network security system safeguards ClusterPower data, providing the performance, availability, and scalability to help the organisation grow and extend the reach of digital transformation in Romania and beyond. The benefits include:

- **The driving of Eastern European digital transformation:** This best-practice connected network security suite enables ClusterPower to provide trusted, agile CSP services. This in turn enables customers in Romania and neighbouring countries to launch adaptive digital transformation services more quickly, supporting growth across the region.
- **Time to value:** CSP customers typically want to launch new services at short notice, to gain competitive advantage. Palo Alto Networks network security integrates rapidly and seamlessly with almost all applications and environments, allowing services to be spooled up more quickly. "The configurations are standard and automated, dramatically reducing the time to value for our customers," says Vladimir.
- **Optimised performance and stability:** The Palo Alto Networks NGFW is ideally suited to ClusterPower's high-speed data centre service-provider deployment. ML intelligence and scalability throughout ensure the Bucharest-based environment performs just the way customers expect, adhering to their SLAs. Threat Prevention uses researcher-grade signatures to safeguard the network from known threats – such as exploits and commodity malware – without compromising performance.
- **Segmented security:** By partitioning the network into manageable, secure segments, ClusterPower limits data exfiltration and reduces the attack surface. "We can use the reporting capabilities to give each ClusterPower customer a clear picture of their applications, users, and data on each segment of the network," Vladimir explains.

He concludes: "One of the great advantages of partnering with Palo Alto Networks is that 'security by design' is embedded into all of our services. We benefit from an intelligent, proactive security infrastructure – one that we can confidently deliver to our customers."

Palo Alto Networks ML-Powered Next-Generation Firewalls embed machine learning directly in the core of the firewall to provide real-time IoT device identification and inline, signatureless attack prevention. Dive into the e-book on ML-Powered NGFW. Cloud-Delivered Security Services (CDSS) reduce manual tasks and enhance security posture with a self-updating security platform that augments global threat intelligence to automatically counter attacks in near-real time.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com