Gruppo E

Gruppo E Implements Three-Phased Project To Secure Production Lines And Mobile Devices

Gruppo E is an IT leader supporting companies with sustainable digital transformation. Headquartered in Italy's Tuscany region, Gruppo E's offerings include system integration, cybersecurity, next-generation data centers, business continuity, disaster recovery, network and unified services, virtualization, and cloud-related services.

CYBERFORCE, a Palo Alto Networks technical recognition program, rewards our most elite partners for their pre- and post-sales expertise. View the value of CYBERFORCE.

Challenge

Multinational Company Requires Enhanced Security for Production Lines and Mobile Users

A multinational tissue paper company with large production facilities in Europe, North America, and Latin America experienced a cyberattack on their production environments. A Palo Alto Networks firewall foiled the hacker's attempt, but the incident highlighted an ongoing cybersecurity risk.

The interactions and transfer of information among the production system's networks and devices were not well-defined or controlled. The customer urgently needed to increase the cybersecurity of their production environments as well as secure the mobile devices used throughout the company.

CYBERFORCE Hero to Lead the Project Without Halting Production Lines

Nicola Percacciante, a CYBERFORCE Hero and Senior Solutions Engineer at Gruppo E, had become the customer's go-to expert in Palo Alto Networks technologies. For 12 years he had worked with this customer, solved critical issues, and established a trusted relationship. He also understood the customer's infrastructure and equipment – down to the individual devices and across the production processes.

The company viewed Percacciante's CYBERFORCE Hero status as an assurance of project quality, product knowledge, and deployment expertise. They looked to him to lead the efforts to better secure their production environments and mobile users.

The customer had one critical requirement: the CYBERFORCE team would have to identify and deliver a solution without bringing production at the customer's facilities to a stop. A halt in production would mean a significant loss of material, substantial economic loss, and environmental waste.

CYBERFORCE at Gruppo E:

- 4 Pre-Sales Heroes (highest level)
- 1 Defender
- 1 Strata Special Ops*
- 2 Cortex Special Ops*
- 1 Prisma Special Ops*
- 1 SASE Special Ops*
- And more to come

*Technical expertise.

"The proposed technologies provided a timely solution to the customer's problems. At the same time, we made it clear to the customer the value of Palo Alto Networks' security platform and the comprehensive, holistic, and forward-thinking approach of Palo Alto Networks to corporate security."

Nicola Percacciante,
Senior Solutions Engineer
Gruppo E

Solution

Customer Chooses Palo Alto Networks Next-Gen Firewalls, Prisma Access, and Cortex XDR

After analyzing the capabilities of Palo Alto Network solutions to integrate with the customer's infrastructure, the CYBERFORCE team recommended a three-pronged solution comprising Palo Alto Networks next-generation firewalls, Prisma Access, and Cortex XDR. The capabilities of each would address specific challenges for the customer:

- **Next-Generation Firewalls.** The Palo Alto Networks firewalls enable network segmentation in the production environment, which limits uncontrolled communications and reduces the attack surface.
- **Prisma Access.** The Prisma Access solution enables the firewalls on the production line to securely access the internet. Prisma Access also secures internet access for all the company's mobile user devices worldwide. Tablets, smartphones, PCs, and other individual corporate devices can securely access cloud applications and the internet with comprehensive traffic monitoring.
- **Cortex XDR.** Computing stations in the customer's production environment didn't receive updates as frequently as the rest of the corporate IT infrastructure. Infrequent updates to the operating systems and installed software on those stations also increased security risks for the entire production system. With Cortex XDR, the company can count on endpoint protection and security in the production environment, covering even obsolete operating systems.

Pre-Sales Engagements Include Security Vision, Roadmaps, and Ultimate Test Drive

As part of pre-sales engagements with the customers, Percacciante used several Palo Alto Networks resources including an Ultimate Test Drive virtual workshop to demonstrate the technologies.

Palo Alto's security vision and development roadmaps were key factors in the customer's decision to move forward with the Palo Alto Networks solutions. "Palo Alto Networks' vision for 360-degree security is uncommon among other vendors," says Percacciante. "Palo Alto Networks also demonstrates a significant capacity for innovating its proposed solutions, clearly outlining a development roadmap that reassures the customer."

Percacciante planned the deployment time for each of the three solutions to avoid production halts while reducing security risks in a practical timeframe.

Results

Three-phased Deployment Reduces Cybersecurity Risks with Scalable Solutions

The two-year project began with the installation of Prisma Access for mobile users, continued with the implementation of next-gen firewalls at the production sites, and concluded with the Cortex XDR deployment.

Tangible benefits for the customer include:

- Reduced risk of cyberattacks and increased control over external threats
- Simplified management and complete visibility using a single management console for the next-gen firewalls and Prisma Access
- Visibility into Cortex XDR using a dedicated console
- Scalable solutions

The firewall implementation paved the way for an IoT security proof of concept for additional production line security.

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