



AL SERVIZIO DELLA RISTORAZIONE

PREGIS[®]



CASE STUDY

Improving Business Continuity While Boosting Security for Pregis SpA

Italian food services leader Pregis SpA relies on Palo Alto Networks Next-Generation Firewalls (NGFWs), DNS Security, and Cortex[®] XDR[™] to protect its infrastructure, avoid downtime, and support its time-sensitive business.



IN BRIEF

Customer

Pregis SpA

Industry

Food services

Country

Italy

Products and Services

Food distribution

Organization Size

200 employees and 300 sales consultants

Challenge

Pregis SpA needed to protect its endpoints, network, and perimeter by proactively facing cyberthreats.

Requirements

- + Activate innovative and effective security technologies
- + Gain greater control and centralized management
- + Deploy rapidly while maintaining business continuity

Solution

With Palo Alto Networks NGFWs, DNS Security, and Cortex XDR, Pregis SpA was able to save time, increase traffic visibility, and realize proactive protection across its infrastructure.

Maintain Security and Business Continuity

Advanced security technologies allow Pregis SpA to protect its data centers and securely connect with its branch offices, guaranteeing operational continuity. Continuity is a paramount element for the company, which must deliver food in a timely manner to private and public organizations with the highest levels of accuracy and reliability.

That's why Moreno Gisaldi, IT director of Pregis SpA, has explored ongoing security improvements to achieve the company's mission every day, avoiding any disruption due to obsolete technologies or advanced cyberthreats that could affect Pregis SpA systems.



Challenge

PROTECT INFRASTRUCTURE TO PROTECT CUSTOMERS

Pregis SpA' mission is to guarantee customers a safe, punctual, quality service as well as reliable and competent advice. Among its customers, Pregis SpA includes hotels, restaurants, and public organizations such as schools and hospitals. Reliability and continuity of services are essential elements.

An Italian company specializing in food distribution in the Food Services industry, Pregis SpA ranks third nationwide in terms of revenue, reaching 240 million euros in 2019. Founded in Riva del Garda in 1960, today it has nine branches in Italy, about 18,000 customers, 200 employees, and 300 sales consultants, processing 6,000 orders every day. Pregis SpA' offering portfolio includes more than 15,000 references made available in real time, with an average order processing time of four hours. In terms of distributed technology, the company manages 1,000 warehouse terminals and approximately 900 corporate devices.

“Providing timely services and relying on a secure IT infrastructure is mandatory for us,” Gisaldi says. “We can't allow any risk of disrupting our food delivery service due to a vulnerability or malware, as the satisfaction of our customers represents our core business.”

Requirements

CUTTING-EDGE PROTECTION ENSURES BUSINESS CONTINUITY

Security plays a fundamental role in the company, not only to comply with all regulations related to data management and storage. Protecting infrastructure, endpoints, network traffic, and the perimeter to detect and mitigate any cybercriminal activities—including malware attacks, ransomware, and credential theft—is critical for Pregis SpA.

“Cyberattacks are becoming ever more sophisticated, with social engineering techniques that are more difficult to detect,” Gisaldi says. “We needed to boost our security level to enable secure operations, avoiding any risk of compromise. With ransomware also becoming increasingly aggressive, the impact of a cyberattack would be critical for our business; a risk we can't afford to take.”

In 2017, Pregis SpA decided to initially renew its firewall architecture to achieve more effective and performant protection. Gisaldi and his team started looking at new and enhanced solutions to achieve greater control and centralized management that would optimize their business operations.

““We needed to be sure we have the highest protection measures in place to avoid any possible disruption of our productivity and core business.””

— **Moreno Gisaldi, IT Director at Pregis SpA**

Solution

NEXT-GENERATION FIREWALLS DELIVER PERIMETER PROTECTION

Gisaldi and his team considered different solutions from leading security vendors. Thanks to the valuable support of Infonet Solutions—a company with 30 years’ experience in the IT sector and a member of the Palo Alto Networks NextWave Partner Program—after analyzing and evaluating the policies and internal components to be monitored, Pregis SpA chose Palo Alto Networks to protect its infrastructure.

Specifically, the company decided to renew its perimeter protection system, deploying 18 Palo Alto Networks PA-Series NGFWs to protect applications and prevent vulnerabilities while data is in transit on the network. A VM-Series Virtual NGFW was also deployed to extend the levels of visibility and application protection against vulnerabilities to the cloud environments, where deploying a hardware firewall would be impossible. Both hardware and virtual firewalls are managed by Panorama™ network security management, which allows the IT team to control all application, user, and content data across firewalls from a single pane of glass.

“The excellent capabilities and performance provided by Palo Alto Networks firewalls have allowed us to enhance the level of protection of our infrastructure, increasing visibility on traffic and any possible threat that could slow down or disrupt our activities,” says Gisaldi. “For the type of services we provide, we can’t afford any kind of interruption or slowdown; a ransomware attack stopping our activities for days would mean a real disaster for our activities.”

Palo Alto Networks NGFWs enable Pregis SpA to process data flows in a single pass, extracting all the necessary data to operate security functions based on the identification of applications, data, and users, with relevant benefits in terms of performance and predictable scalability under heavy workloads, such as those on the application level for a firewall.

In November 2020, the company decided to turn on the DNS Security service across all NGFWs, which allows predictive analysis to stop any attack using DNS and automate protection. With the DNS Security service, Pregis SpA was able to eliminate the need for additional point products.

Phishing Attack Lifecycle

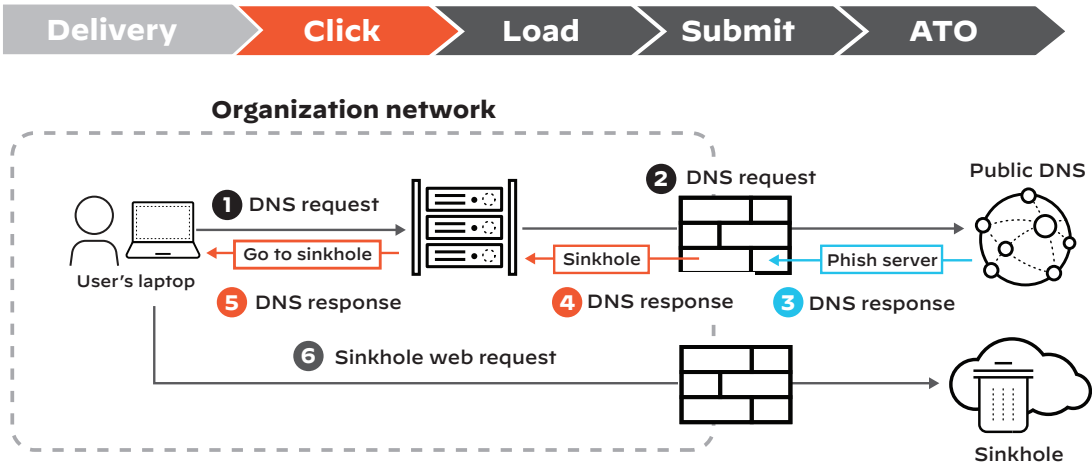


Figure 1: Automated policies triggered by DNS sinkholes

CORTEX XDR PROVIDES AI-POWERED DETECTION AND RESPONSE

As an addition to corporate security, Pregis SpA also decided to deploy Cortex XDR on company endpoints to enable a proactive approach to threat detection and response, with higher visibility into data across networks, clouds, and devices, applying analytics and automation to protect against increasingly sophisticated threats.



“Our security team is now able to significantly reduce the lifetime of attacks down to a few minutes. Day-to-day security operations also now have a reduced impact on our workforce; we’ve been able to reduce repetitive manual tasks by up to 80%”

– Moreno Gisaldi, IT Director at Pregis SpA

Benefits

CENTRALIZE THREAT MONITORING AND ANALYSIS

The security infrastructure implemented by Pregis SpA allows the company to streamline monitoring and analysis of external threats, combining cutting-edge technologies with the human intelligence of its IT staff for high-level security orchestration.

ENABLE PROACTIVE DETECTION AND RESPONSE

The company has also deployed Cortex XDR to its endpoints to take a proactive approach to threat detection and response. With high visibility into data across networks, clouds, and endpoints, Pregis SpA can apply analytics and automation to protect against increasingly sophisticated threats.

ACCELERATE INVESTIGATIONS WITH AUTOMATION

Using behavioral analytics, Cortex XDR can accelerate investigation processes through automation and block attacks before they can impact any systems. “Our security team is now able to significantly reduce the lifetime of attacks down to a few minutes. Day-to-day security operations also now have a reduced impact on our workforce; we’ve been able to reduce repetitive manual tasks by up to 80%,” adds Gisaldi.

“Palo Alto Networks’ commitment to evolve and update its technologies to meet constantly changing requirements allows us to have the highest level of proactive protection. This allows Pregis SpA to focus on our core business, significantly reducing efforts previously dedicated to security, improving results of research and event identification. The reduction in time dedicated to security can be estimated around 40%, leading to a higher operational efficiency and a parallel increase in the quality of services that we can offer to our clients.”



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

© 2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. parent_cs_pregis-spa_030521