SeSa bolsters security posture with advanced cybersecurity

Large IT solutions provider blocks ransomware attacks, gains in-depth view of forensic activity and automates time-intensive security tasks

THE CHALLENGE

A couple of years ago, SeSa Group, one of Italy's largest IT solutions and services providers, was experiencing frequent ransomware attacks. This required the company's cybersecurity department to pour significant time and effort into performing checks, removing ransomware and disinfecting affected systems.

The cybersecurity team decided to evaluate different security solutions. The objective was to expand the cybersecurity perimeter without negatively impacting performance of employees' workstations. Ultimately, SeSa selected Bitdefender GravityZone Ultra.

Alberto Santini, Chief Information Security Officer, SeSa, explains, "In a pilot, Bitdefender showed it was most effective at detecting and resolving threats and very easy to use. GravityZone Ultra gives us the latest endpoint detection and response capabilities and protects our entire estate across virtual, cloud and physical environments in the data center and at endpoints."

THE SOLUTION

Bitdefender GravityZone Ultra provides SeSa with endpoint protection, detection and response (EDR) capabilities covering 2,000 of its Microsoft Windows and Apple workstations, as well as Microsoft Windows servers running across 20 company locations and in Microsoft Azure cloud.

Applications protected by Bitdefender include SeSa's custom-developed customer relationship management, Zucchetti enterprise resource planning, Microsoft Active Directory and File Server.

SeSa also uses GravityZone Patch Management to automate patching of operating systems and applications and GravityZone Full-Disk Encryption to automate management of encryption key—both administered from the same console as GravityZone Ultra.

SeSa S.p.A., with headquarters in Empoli, Italy, provides organizations with advanced IT solutions, including servers, storage, networking, enterprise software, as well as infrastructure, outsourcing, business intelligence and business management services. The company has consolidated revenues of about Euro 1,550 million, and an EBITDA of Euro 74.3 million.

Industry
IT Solutions and Services

Headquarters
Empoli, Italy

Employees
2,000 (IT staff: 5)

Results

- Complete blocking of ransomware attacks
- Visibility into full chain of forensic events and behavior enhances security posture
- Security automation-enabled time savings lead to smarter reallocation of IT staff resources
- Security-related trouble calls dropped from 10 to zero on average per month

THE RESULTS

GravityZone Ultra's combined endpoint-protection and EDR capabilities protect SeSa against advanced threats, while enabling its security analysts to conduct proactive threat hunting and root-cause analysis. SeSa takes advantage of the Endpoint Risk Management and Analytics functionality to assess, prioritize and address risk coming from endpoint misconfigurations and vulnerabilities, further strengthening its security posture.

"GravityZone Ultra provides us with powerful automation, machine learning and reporting," states Santini. "Since deploying GravityZone, we haven't seen a single successful attack. Even when zero-day attacks occur, which don't have signatures, GravityZone analyzes the behavior and blocks the malware almost immediately.

"Before, we were blind to some threats. With access to high-value forensic-analysis capabilities in GravityZone, we see the full chain of events and user behavior so we can respond more intelligently while capturing valuable learning for the future."

GravityZone also has safeguarded SeSa's virtual data center infrastructure explains Santini: "GravityZone has done an amazing job preventing malware from targeting vulnerabilities and spreading across our network of virtual servers."

Santini appreciates that GravityZone automates time-intensive tasks, freeing up the team to focus on critical priorities: "With just a few clicks in the GravityZone console, we're able to deploy the agent, set policies, etc. GravityZone takes care of much of the work we used to do manually."

In fact, Santini now assigns junior systems engineers to create policies, deploy endpoints, evaluate incidents, and extract and review reports. Senior systems engineers have more time to focus on higher-level activities aligned with their expertise.

In addition, GravityZone has improved the experience and productivity for thousands of users at SeSa.

Santini states, "Our users feel better protected and no longer experience sluggish performance when updates occur. The number of security-related trouble requests has dropped from 10 to zero on average per month. If there is an issue, Bitdefender detects and resolves it before the user even knows about it."

SeSa also places high value on the close partnership with Bitdefender.

"Bitdefender's ability to listen to our needs and their customer support have far exceeded our experience with other vendors," reflects Santini. "Their deep understanding and knowledge of our security requirements reinforces that Bitdefender is the ideal partner to help us navigate our cybersecurity journey."

"Since deploying GravityZone, we haven't seen a single successful attack…With access to high-value forensic-analysis capabilities in GravityZone, we see the full chain of events and user behavior so we can respond more intelligently while capturing valuable learning for the future."
Alberto Santini, Chief Information Security Officer, SeSa

Bitdefender Footprint
- GravityZone Ultra Security
- GravityZone Integrated Patch Management
- GravityZone Full-Disk Encryption

IT Environment
- Microsoft Active Directory
- Microsoft Azure
- Microsoft Exchange
- Microsoft SharePoint

Operating Systems
- Apple (Mac)
- Microsoft Windows
- Red Hat Enterprise Linux

15062020-Bitdefender-Business-CaseStudy-SeSa-creat4407-a4-en_EN