SOPHOS

CUSTOMER CASE STUDY

A Trio of Sophos Security Solutions Protect Healthcare Organization Galeno from Ransomware Attacks and Advanced Cyber Threats

GALENO

Customer-at-a-Glance

Galeno Argentina S.A.

Industry
Healthcare

Number of Users
2500

Sophos Solutions
Sophos Endpoint Protection Advanced
Sophos Sandstorm for Email Protection
Sophos UTM Web Protection

'We've saved a tremendous amount of time and money because of Sophos, something that we never thought possible.'

Carlos Farias
IT Director
Galeno Argentina S.A.

With more than 30 years of experience, and a presence across Argentina, Galeno S.A. is a Health Maintenance Organization (HMO) that provides a form of health insurance coverage, health maintenance services, worker's compensation, and other health related services. With these kind of services, Galeno is a data rich organization responsible for sensitive patient information, personal data, and payment details. The vast amount of personal customer data that is collected daily means that Galeno needs a strong IT security posture primarily focusing on endpoint security, defenses against advanced malware, and comprehensive email and web protection. One of Galeno's goals is to ensure that critical and sensitive patient information does not fall into the wrong hands because of any targeted attack. After utilizing other security products, Galeno identified Sophos as the security vendor best placed to address its data security concerns.

Challenges

- Protection of users and their devices on the go
- Eliminate ransomware in order to decrease risks to organizational processes and to diminish the threat to employee productivity
- Help to protect against advanced malware threats and ransomware attacks, which could interfer with patient care
- Extend the highest level of security across a distributed environment of branches and clinics
- Simplify security deployment and management in order to remove delays, configuration errors, and inefficiencies

Carlos Farias is the IT Director at Galeno Argentina. Farias and his team are solely responsible for strengthening the company's IT security infrastructure. As a result, Farias and his IT organization were looking to improve the company's cyberattack preparedness especially in the wake of experiencing various ransomware attacks. These attacks disabled endpoints and encrypted critical files which included sensitive patient data. This caused a tremendous disruption in the company's processes and the IT security infrastructure became unnecessarily complex for Farias and his team. "When we experienced a ransomware attack, the output was catastrophic. My team had to work on cleaning up the systems to ensure the

organization was operating as it should. When we had an attack like this, patients were not able to be seen by doctors because our files were encrypted. Everyone from staff to patients felt the effects," clarifies Farias.

These ransomware attacks impacted the operation of more than 50 branches and 150 clinics, affecting how medical staff could provide care and subsequently how patients were treated across the organization. The attacks also caused potential harm to the hard-earned and impressive reputation of the organization, resulting in the loss of trust from the community who saw Galeno as a reliable provider. "What kept me up at night was the ever-increasing concern that we would experience additional attacks to our systems. With the sensitive data we manage and the compliance regulations we must keep, ensuring our systems are safe from threats is paramount. But most importantly, we wanted patients to know we had their best interests at heart. It wasn't just about keeping their personal information safe. It was also about providing the proper care to the community," explains Farias.

How do ransomware attacks affect a healthcare organization?

Because of the attacks, which weren't stopped by the previous security products, the Galeno IT department unfortunately lost 2-3 full days spent on fixing issues resulting from the multiple ransomware attacks. This included gaining back control of files and ensuring that the security system had been completely updated. This entire process led to a backlog of other IT issues which resulted in loss of productivity across the organization. "Because our team spent most of their time cleaning up after the ransomware attacks, they didn't have enough time in their day to spend on other important IT projects. This wasn't efficient for us as a team and I knew we needed better protection," describes Farias.

The fallout of the work managed by the IT department had a greater effect to the patients under Galeno's care. The medical staff spent much of their time ensuring they had the proper files and correct information on each patient, adding more steps to the process of medical care. "Although it is important to note that while some patients were not directly affected by these attacks, the branch offices found it difficult to keep up with the appointments and work load of validating information," expresses Farias.

How do you protect your organization against zero day threats?

Initially, Farias and his team had found Symantec and TMG to be adequate security products. But as ransomware attacks became more common and consistent, Farias realized these security products were unable to cope with advanced malware attacks and zero-day threats. "I was concerned about the number of the attacks we were seeing consistently and the level of sophistication of those attacks," declares Farias. The features from the Symantec and TMG products proved to not be adequate to protect against the rapidly evolving cyberattack methods and the growing complexity of daily threats.

In addition to managing the unfortunate outcome of the multiple ransomware attacks, Farias and his team required additional support from both TMG and Symantec. "My team is a group of experts who managed the effects of the attacks professionally. Although we have the right level of skill in-house, we looked to Symantec and TMG to provide us the right level of customer support when we needed it. After the challenges we faced from the ransomware attacks, I was disappointed with the lack of customer support from such established security vendors. Their customer support mechanism wasn't at the level it needed to be for us and I felt we did not get the support we needed at such a challenging time. It was then that I decided we should look elsewhere. We required the right security solution to stop attacks and a level of engagement from a security company who could properly support us as a healthcare organization," articulates Farias.

How did Sophos solutions play a role in providing the right healthcare in Argentina?

Because of his expertise in the security industry, Farias knew he now wanted to deploy an integrated security systems that offered comprehensive protection for Galeno's network and endpoints. Most importantly the solutions needed to be easy to deploy and manage, especially when battling sophisticated threats and attacks. As a result, Farias began looking for a security vendor who offered a portfolio of powerful and effective security products which are easy to manage after initial deployment. These products needed to address the increasingly complex and sophisticated threats

'With Sandstorm, we were up and running in minutes, using this strategic technology in the cloud, along with minimum investment in on-premise hardware. We now have an extended level of intelligence complete with deep learning analysis, which we didn't have before.'

Carlos Farias
IT Director
Galeno Argentina S.A.

and the rise of new attacks such as ransomware. "My overall goal was to deploy security solutions that tied in with our larger vision of IT security that focuses on protecting information and ensuring nothing interrupts patient care nor impacts productivity," states Farias

During the evaluation phase, Sophos' large installed based gave Farias and his team confidence that the Sophos solutions provided the proper security foundation Galeno needed. "We worked with a channel partner we knew well and who was a trusted resource. The channel partner had a track record of effective implementations in the region and we valued their recommendation to look at Sophos. While we evaluated other security vendors as well, it was Sophos Endpoint Protection, Sandstorm for Email, and UTM Web Protection that met all our requirements, especially those pertaining to ransomware. "The comprehensive security Sophos offers is exactly what we were looking for," declares Farias. For his team, the real benefit lay in Sophos' ability to make the complex simple. While Sophos solutions offer sophisticated, next-generation capability, they are extremely easy to configure, manage, and use.

Farias and his team identified Sophos as their security vendor of choice after thoroughly evaluating several vendors on the market, including an examination of their experience with Symantec and TMG. For Farias and his team, there were key advantages which separated Sophos from the rest of the competition. "Moving to Sophos made sense for us as a company because we are always looking for innovative solutions which match up with specific emerging technology trends. When comparing Sophos to the previous security products we had, I would say that Sophos is far more prepared to prevent the latest threats. What we loved about Sophos was the easy and straightforward migration process, the next-generation protection of its offerings, simplified management and, last but certainly not least, its expert and diligent support staff who are always willing to assist us," reveals Farias.

One of the key factors in selecting Sophos was to maximize the efficiency of the IT team and overall infrastructure, allowing for proper healthcare to be administered to patients consistently. "I wanted to ensure our employees could diligently care for patients in a timely manner. Additionally, it was important we keep medical records and sensitive data safe. Consistent care and safety was something we didn't want to compromise. Lucky for us, Sophos helps us do just that," pronounces Farias.

What benefits do email, web, and endpoint protection bring to a healthcare provider?

Farias knew that selecting Sophos Endpoint Protection for their systems was the fitting choice. Sophos Endpoint blocks malware and infections by identifying and preventing the handful of techniques and behaviors used in virtually every exploit. Sophos Endpoint does not rely on signatures alone to catch malware. For Farias and Galeno this meant Sophos Endpoint catches zero-day threats without adversely affecting the performance of the organization's devices. "Before we never had any insight into an exploit until it hit our systems, which meant we had to react to fix the problem. Now with Sophos Endpoint deployed we are completely protected from new threats and we have extensive visibility to what's happening with our endpoints," affirms Farias.

Ensuring network security across the multitude of clinics and branches was the initiative Farias worked toward in tandem with their improved endpoint security. Through his thorough evaluation process and after completing in-depth research, Farias selected Sophos UTM and Sophos Sandstorm for network and email protection. Sophos Sandstorm uses next-gen, cloud-sandbox technology to give organizations an extra layer of security against ransomware and targeted attacks. Sandstorm extends conventional security to enhance ransomware and targeted attack protection, visibility, and analysis, which was exactly what Farias knew Galeno was searching for. As the only network sandbox to use deep learning analysis for more effective detection, Sophos Sandstorm integrates with other Sophos solutions seamlessly with no additional hardware required. "With Sandstorm, we were up and running in minutes, using this strategic technology in the cloud, along with minimum investment in on-premise hardware. We now have an extended level of intelligence complete with deep learning analysis, which we didn't have before. Moreover, I'm beyond impressed by Sandstorm's protection from advanced persistent threats and targeted attacks," adds Farias.

Sophos UTM is unmatched in its deployment flexibility providing Farias simple options for high-availability, clustering, branch office connectivity, wireless, and centralized management, and reporting. And unlike competitive products, Sophos UTM doesn't compromise on features or performance, which means that every feature is available to Farias and the Galeno branches. Galeno utilizes Sophos UTM alongside Sophos Sandstorm technology for targeted attack and ransomware protection, along with transparent visibility and full analysis with what is happening on their network.

"With Sophos we've been able to save hundreds of non-service hours from our day-to-day operations. Saving this amount of time has had positive effects for our IT team, who previously had to spend much of their time fixing issues which resulted from the various attacks. We have also found the centralized console and ease of management from Sophos is truly unsurpassed. And now with Sophos, we are elevating the vision of IT security in Argentina's healthcare industry," asserts Farias.

With the proper security solutions covering Galeno's endpoints, email, web, and their all-encompassing network, concerns about zero-day threats and ransomware attacks are a thing of the past. Galeno is now realizing the benefit of maximum productivity and resources saved. "We've saved a tremendous amount of time and money because of Sophos, something that we never thought possible. Sophos is exactly what we need, when we needed it. Thankfully, Sophos has restored our faith and trust in cybersecurity counter-measures," concludes Farias.

Start your free trial of Sophos Sandstorm today to get started with Advanced Web Protection.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2018-03-8 CS-NA (RP)