Spanish Law Firm Thwarts Ransomware, Simplifies Endpoint Security Management

Pérez-Llorca

"Having Palo Alto Networks Traps advanced endpoint protection makes us confident that we can protect our endpoints and prevent data leakage from any device. Pérez-Llorca considers Traps to be a giant step forward in endpoint security."

Aitor Lasala | Chief Technology Officer | *Pérez-Llorca*

Organization

One of the premier law firms in Spain, Pérez-Llorca employs more than 150 lawyers and 70 support staff. The firm's expertise spans a wide range of legal subjects, including corporate mergers and acquisitions, capital markets, banking and restructuring, litigation and arbitration, real estate, tax law, and labor law. Pérez-Llorca has its primary offices in Madrid and Barcelona and has recently established branch offices in New York and London.

Industry

Legal

Challenge

Prevent the loss of sensitive client information, block ransomware and other cyberthreats, and avoid costs associated with remediating successful attacks.

Solution

Palo Alto Networks® Traps™ advanced endpoint protection protects endpoints from ransomware, botnets and other cyberthreats while centralizing endpoint security management.

Results

- Eliminated successful attacks by ransomware
- Avoided 10–15 hours of lost lawyer productivity per month
- Saved 30–40 hours of IT time per month
- Cut troubleshooting time by 15–20 percent
- Reduced support calls significantly
- Centralized control of all applications, including some previously unknown

Story Summary

Spanish law is a civil law system based on Roman law, making it quite different from the common law system used in England and the United States, among others. As a result, enterprises doing business in the Spanish market often require top-notch legal help to navigate the complexities of the nation's legal code. For more than three decades, Pérez-Llorca has filled that need, offering expert advice to help national and international companies succeed in Spain.

On several occasions, ransomware had penetrated Pérez-Llorca's endpoint defenses and infected computers used by the firm's lawyers. In addition to lost productivity for the affected users, mitigating these successful attacks drained valuable IT time that was needed for more strategic tasks.

All of that changed when Pérez-Llorca deployed Traps to protect about 200 endpoints. Now successful ransomware attacks have been eliminated, resulting in monthly savings of 30–40 hours of IT time and 10–15 hours of lawyer time. In addition, the firm's IT staff can better control the entire application environment, a true confidence builder. Traps is a key part of the security infrastructure that protects Pérez-Llorca's confidential information, its most valuable asset.

The International Language of Cybercrime

When it comes to security, the harsh reality is that cybercrime is not sensitive to cultural and linguistic differences: It can happen to anyone with valuable information to steal. In that sense, Pérez-Llorca faces the same challenges as any large law firm. Protecting clients is paramount: Any accidental or deliberate disclosure of confidential information could be devastating for the client, the Pérez-Llorca brand and, ultimately, revenues. At the same time, highly sensitive legal documents must flow easily between lawyer and client; therefore, the security infrastructure must facilitate and secure these communications even as it blocks unwanted traffic.

Recently, the firm suffered several successful attacks by ransomware, which encrypts the data on the user's hard drive and demands a payment to provide the decryption key. Aitor Lasala, the chief technology officer for Pérez-Llorca, describes the sequence of events. "Most lawyers are not highly skilled in technology, so when an email arrives in their inbox, they open the attachment," he says. "Unfortunately, sometimes that attachment infects the endpoint with ransomware, rendering the machine unusable by the lawyer until it can be remediated."

"Traps give us better control of our entire application environment. The dashboard is clear and easy to use, cutting the time it takes to perform routine tasks, such as upgrading the endpoint software."

Aitor Lasala | Chief Technology Officer | *Pérez-Llorca*

Small Staff, Big Responsibilities

The good news is that Pérez-Llorca has a robust backup system in place, which allows the IT staff to rebuild the machine without paying the ransom. The bad news is that mitigating attacks is costly. "When an endpoint is infected, we don't lose any information," says Lasala. "However, the lawyer is less productive during the time it takes the IT staff to rebuild the system from backups."

That IT time comes from a relatively small resource pool: Like most firms its size, Pérez-Llorca keeps its support staff lean. Every hour spent on remediation is an hour taken away from higher-value tasks. In light of these costly incidents, Lasala decided that the antivirus solution currently deployed on the firm's endpoints was no longer adequate. He immediately began a search for an endpoint security solution that would eliminate the ransomware problem in particular and improve endpoint security in general.

Short Search Leads to Traps

That's where Palo Alto Networks partner Grupo Antea enters the picture. Pérez-Llorca often relies on Antea to assist the firm in technology matters, so it made good sense for Lasala to ask Antea's opinion. After assessing the firm's needs, Antea recommended Traps.

It didn't take long for Lasala to realize that Traps was a unique product that offered exactly the capabilities Pérez Llorca needed. "Palo Alto Networks has taken a very aggressive approach in the design of Traps," Lasala says. "Instead of simply remediating attacks, Traps stops processes from even running in the first place. No other vendor has anything like Traps."

Intercepting Threats Without Stopping Traffic

Stopping malware executables was one thing, but Lasala was concerned that Traps might interfere with the execution of legitimate applications as well. The firm's lawyers depend on a number of critical applications to track their time, communicate with clients and perform other legal tasks. Any interruption to their ability to use those applications was simply unacceptable.

With these requirements in mind, Antea and Palo Alto Networks worked with Pérez-Llorca to conduct a Proof-of-Concept (PoC) Test. "The POC test convinced us that the Palo Alto Networks solution met all of our needs," says Lasala. "Traps stopped every piece of known and unknown malware that had previously infected our endpoints. At the same time, Traps recognized our critical applications and allowed them to execute unimpeded." Based on Lasala's report, the firm's management approved the purchase of Traps.

Palo Alto Networks sent a field engineer to help Pérez-Llorca's IT team deploy and configure Traps, impressing Lasala in the process. "Palo Alto Networks made sure that we were happy," he says. "About six months after the installation, they sent another engineer to examine the log files and help tune up the system for maximum performance. Other vendors don't offer that kind of support."

Ending Ransomware Incidents

Did Traps solve the firm's problems? Lasala's answer is an emphatic "yes." "From time to time, our lawyers still open email attachments that they shouldn't open, but now Traps stops the malware from executing, preventing endpoint infection," he says. "Traps even blocks code injection attacks hidden in PDF files—something that antivirus programs simply can't do."

Because of Traps, cyberthreats that once caused havoc at Pérez-Llorca now have virtually no impact. The firm avoids between 10–15 hours of lost productivity for its lawyers every month, not to mention the frustration of trying to work for hours or days with no computer. Traps also saves 30–40 hours of IT staff time by eliminating the time-consuming task of rebuilding infected machines from backups.

Simplifying Endpoint Security Management

When Traps went into production, Lasala's team began to notice that a number of legacy applications thought to have been retired were still being used. These programs didn't pose any threat, but Lasala was glad to know about them all the same. "Traps makes us aware of our complete application landscape, which gives us better control of our entire environment," he says.

"The Palo Alto Networks Next-Generation Security Platform locates all the security information in one place, which would allow security staff to correlate threat activity and give them more tools for detecting and mitigating advanced threats."

Aitor Lasala | Chief Technology Officer | *Pérez-Llorca*

In the past, managing the antivirus software for 200 computers was complex and time-consuming. Not so with Traps. "The centralized control in Traps is quite useful," Lasala says. "The Traps dashboard is clear and easy to use, cutting the time needed to perform routine tasks, such as upgrading the endpoint software."

That ease of management frees up valuable time for the firm's small security department. "Using Traps, our team can troubleshoot and resolve a security issue 15–20 percent faster," Lasala says. "Also, support calls from users have dropped significantly because their machines are no longer getting infected."

Confident and Looking Ahead

As Lasala has gotten to know Palo Alto Networks, he has come to understand and appreciate the company's approach to security. "The security integration represented by Palo Alto Networks Next-Generation Security Platform could be valuable for us in the future," he says. "The Palo Alto Networks Next-Generation Security Platform locates all the security information in one place, which would allow security staff to correlate threat activity and give them more tools for detecting and mitigating advanced threats."

Beyond the tangible benefits, Lasala derives peace of mind just knowing that Traps is at work. "Having Traps makes us confident that we can protect our endpoints and prevent data leakage from any device," he says. Recently, Lasala received a call from his counterpart at another large Spanish law firm, asking about his experience with Palo Alto Networks. "I can tell you what I told him," Lasala says. "Pérez-Llorca considers Traps to be a giant step forward in endpoint security."