CNR fortifies its IT security with Kaspersky

CNR
Ministerio de Agricultura
Gobierno de Chile

CNR

kaspersky BRING ON THE FUTURE

Chile's National Irrigation Commission (CNR) has partnered with Kaspersky to improve the visibility of the state of its ICT equipment and bolster its internal cybersecurity.

The CNR promotes the agricultural development of Chile's farmers, growers, and producers through funding, development, and transformation.

Public Service – Government

- Chile, South America
- Using Kaspersky Endpoint Security Cloud Pro
- Addressing a major vulnerability gap that threatened both the service and the State

220
users across Chile

110,000m
pesos funding delivered annually

48
years of experience in the industry

- **Ease of use,** excellent asset management, and vendor support
- **Cloud-managed,** so directive-focused and simple to implement
- Expected **protection was fulfilled 100%** across all platforms
- **Competitively priced** and all cyberat-tacks/incidents blocked

"We trust in Kaspersky as a direct partner for all the protection and visibility it has given us. We can track attacks, incidents, patching, and manual blocking."

Sebastian Casabonne Vilches
Technology and Digital Transformation Unit Coordinator

About the customer

The CNR has been contributing to Chile's national irrigation policy and improving the efficiency of its irrigation systems since 1986, with a particular focus on producers in vulnerable situations and the ongoing development of extreme regions of the country. It does this through development projects and productive transformation, as well as the promotion of private investment in irrigation and drainage works.

Challenges

The CNR had identified a vulnerability gap in its systems which it felt needed addressing as a matter of urgency.

The gap in question was between its ICT assets and the education of its employees, which meant that daily reports, notifications, and the execution of update activities were being patched to protect against attacks.

Before approaching Kaspersky, the CNR was using another solution. The renewal proposal for this was extremely high and was going to require the acquisition of separate security modules. The team opted to carry out a proof of concept exercise with Kaspersky, to gain visibility and highlight the number of attacks against the organization.

The CNR also wanted visibility of the state of its ICT equipment, as well as for its internal security to be bolstered by awareness, supported by policies, decrees, instructions, and good cybersecurity practices.

It specifically wanted this to include access control, data protection, incident response, and early monitoring detection. It needed the whole thing to be easy to understand for both the ICT operator and the end user, all with a high level of partner support in case any queries should arise, and all at a reasonable cost. The solution needed to be effective and easy to understand, with supplementary support on offer both throughout the set-up and familiarization phases and moving forward thereafter.

Ultimately, the CNR wanted to enhance its threat intelligence capabilities and, through the enrollment of a trusted cybersecurity partner, have complete faith in both its system and its employees' response to current and emerging cyber threats.

99% uptime
of the platform

24%
cost saving

0% materialized events
in cybersecurity through EDR and zero trust

"With Kaspersky Endpoint Security Cloud, we can now manage security and vulnerabilities promptly and give it more focus throughout the organization. This has allowed us to maintain full control of operations within CNR."

Nicolás Ignacio Cares Toro,
Infrastructure and Operations Manager, Technology and Digital Transformation Unit, CNR

The Kaspersky solution

Kaspersky provided the CNR with an end-to-end integrated cybersecurity solution. It implemented the Kaspersky Endpoint Security Cloud Pro enterprise-grade solution across workstations, servers, and mobile devices, covering approximately 300 licenses in total.

Kaspersky Endpoint Security Cloud Pro was chosen for its ease of use and excellent asset management capabilities, which made for a straightforward user experience. It also meant that the CNR could have access to 24/7 technical support, manage everything from the cloud, and operate within its budget.

- The CNR was able to lay a strong foundation for the future with a seamless upgrade path to EDR, gateway protection, and cloud security.
- By bringing different security tools under a single solution, the CNR was able to maximize both efficiency and convenience.
- Kaspersky Endpoint Security meant the CNR could leverage a multi-layered protection approach based on Machine Learning technology and outstanding Threat Intelligence that covered fileless threats, exploits, rootkits, to name just three.

Protection
The CNR can now stop threats including (but not limited to) ransomware, fileless attacks, exploits, rootkits, viruses, and trojans.

Efficiency
Work is now optimized on a single platform, using automated tools.

Flexibility
The CNR now has end-to-end security capabilities that are quick to deploy, and can be used on any platform, with all its existing infrastructure.

Transparency
The visibility that the CNR wanted as a priority is now a reality. It can access reviews of product code, updates, and threat detection rules, and monitor threats in real-time.

The implementation of Kaspersky's Endpoint Security gave the CNR a safe foundation to enable and support its digital transformation in a robust, simple way.

Having implemented Kaspersky's removable drive blocking, zero trust, panel recommendations, notifications, EDR, safe browsing for Windows, MAC and mobile devices, the protection it required has been 100% fulfilled. The ongoing partnership between Chile's National Irrigation Commission and Kaspersky is one of absolute trust.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

kaspersky BRING ON THE FUTURE