



2023



Fundação CASA elevates cybersecurity maturity with expansion beyond the endpoint

The institution, part of the State Secretariat of Justice and Citizenship, uses Kaspersky's Managed Detection and Response services to increase security in an automated and preventive way, amid the changing digital landscape, with 24/7 monitoring

Fundação CASA

Fundação Centro de Atendimento Socioeducativo ao Adolescente (CASA) is an institution that is part of the State Secretariat of Justice and Citizenship, aimed at increasing socio-educational measures following directives and regulations from the Child and Adolescent Statute (ECA) and the National System of Socio-Educational Assistance (SINASE).

Fundação CASA assists young people aged 12 to 21 all across the state of São Paulo. In 2015, Fundação CASA/SP had 149 socio-educational centers in the state: 108 for interns, 53 for temporary interns, 10 for initial assistance, and 27 for semi-detention.

The organization also manages the São Paulo socio-educational system, following the Decennial Plan for Socio-educational Assistance in the State of São Paulo from 2014. The foundation offers studies and solutions to assist teenagers who have committed crime. In São Paulo, since 2010, socio-educational practices – such as detention or community services – are the responsibility of each municipality.

The Covid-19 pandemic has presented new scenarios and challenges on organizations and strongly accelerated digital transformation. With part of the employees working remotely and the inclusion of virtual visits and tele audiences for teenagers complying with a socio-educational measure, Fundação Casa took advantage of a partnership that had existed since 2016 with Kaspersky to upgrade the solutions and increase their cybersecurity.

In mid-2022, Fundação Casa switched from Kaspersky Endpoint Security for Business Advanced to a more holistic solution: Kaspersky Optimum Security, which includes Kaspersky EDR Optimum, with its easy-to-use basic EDR and robust EPP functionalities and Kaspersky MDR Optimum. MDR is an advanced managed security service that provides attack intelligence, threat hunting and 24x7 security monitoring to continuously research, detect and eliminate threats targeting your organization.

The upgrade increased the institution's cybersecurity level, considerably improving device management and institutional data protection, as Fundação CASA/SP CIO Julio Signorini explains: "We now have visibility of micro incidents, get feedback from possible threats and know which park vulnerabilities we need to look at more closely. It's something we didn't have in the past".

By increasing the scope with Kaspersky, Fundação CASA's information technology (IT) team gained more time to perform other functions within the department that serves the institution as a whole, providing service desk, contact center, DevOps, among others. The cybersecurity team has six professionals. "Today, thanks to the MDR, we are able to have a macro view of the institution, of the entire computing environment, and we are able to act on the micro even with a lean team", explained the CIO.

There is constant communication with Kaspersky's specialized team, with daily reports. "When there is something to be treated, we are very agile to mitigate any possibility of infection. We are informed immediately when there's an incident", said Signorini.

A step ahead

Fundação CASA adopted Kaspersky's solutions in 2016, when it decided to change suppliers following a ransomware attack. Since then, the institution has never again faced problems. After the successful case, the autarchy, which provides assistance of young people between 12 and 21 years of age inserted in socio-educational measures of deprivation of liberty (internment) and semi-liberty, decided that it was time to rely on more efficient solutions. Thus, it took advantage of the renewal of licenses to raise the level of cybersecurity, contracting MDR services and starting to rely on Kaspersky SOC professionals in mid-2022.

The foundation initially had 4,500 licenses of Kaspersky Endpoint Security for Business Advanced, a tool that includes a series of endpoint protection modules, such as finding and fixing vulnerabilities through patch management, software and hardware inventory, and encryption. The upgrade with the latest generation MDR represented a level beyond, now having continuous protection in a service that combines detection technologies, including machine learning techniques. "We were facing difficulties due to the small team and the size of the institution. We saw a favorable situation to upgrade to MDR and have Kaspersky's SOC service working with us", said Julio Signorini.

The institution's technology park is big. Over 10,000 devices – including laptops, tablets, and mobile devices – are used for corporate tasks and socio-educational measures

"Our relationship with Kaspersky goes back a long way and the upgrade was implemented so that we are prepared to face new threats in a preventive manner"

Julio Signorini, CIO



Adopted solutions

- Kaspersky Optimum Security (consists of Kaspersky MDR Optimum and Kaspersky EDR Optimum)
- Kaspersky Cybersecurity Assessment

during work with the young people of the foundation. Devices are also used for tele-hearings, remote communication with teenagers, and virtual visits created during the pandemic.

Furthermore, Fundação CASA manages different categories of information, such as data from teenagers under the responsibility of the state, for example. "Our security levels must be higher, precisely due to the sensitivity of the data," says Fundação CASA/SP's IT director.

Another aspect that led the foundation to migrate was the increase in the amount of information the institution had to handle. It was necessary to follow the institution's proprietary applications closely. Fundação CASA has a software factory and provides services to other government institutions.

"We added a series of functionalities to have a broader level of cybersecurity. Our relationship with Kaspersky goes back a long way and the upgrade was implemented so that we are prepared to face new threats in a preventive manner", said Julio Signorini. "We are aware of the existence of more complex threats and, many times, it is possible to detect them with an EPP solution, but it is very important to have an analytical capacity and this module to have visibility and allow the incident response cycle to work correctly", explained Milton Acevedo, who manages Kaspersky's professional services department.

Continuous threats

The threats being faced today are persistent and advanced and require skilled support professionals. Not all organizations are able to hire this kind of specialist. Kaspersky Managed Detection and Response fills this gap as it helps in the incident response cycle, working through detection and offering recommendations and actions to carry out mitigation.

While EPP (Endpoint Protection Platform) solutions detect threats, EDR (Endpoint Detection and Response) solutions give visibility into elements associated with threats, for example, registry keys, user privileges, external connections, initiating processes, etc. "We installed the solution in the customer's environment to collect information via telemetry and send it to our SOC through the MDR solution. There, our experts evaluate and give recommendations 24x7. We have artificial intelligence tools and qualified analysts inside the service center to provide full support", said Kaspersky's Milton Acevedo.



9.500
employees

4.500~5.000
teenagers currently under
socio-educational measures

120
locations in the State
of São Paulo

10.000
devices

140
software applications
published

Connectivity available
to all devices

Another essential aspect that is connected to the proactive incident response part is the Kaspersky Cybersecurity Assessment, which aims to prevent an attacker from exploiting a vulnerability and, from there, infecting the environment. For this, the Kaspersky team analyzes the risk of the environment, carrying out a long assessment with the customer in order to understand how the IT environment is managed. As a result, a report points out the risk level of the scenarios, the number of vulnerabilities, among other points.

Implementation

Fundação CASA has been a client since 2016 and decided to upgrade in mid-2022. It was a quick implementation process, completed in October 2022. Then, in November, it acquired the Kaspersky Cybersecurity Assessment service, whose report was delivered on December 27, 2022.

During the implementation work, there was a knowledge transfer process on how to use the solution and the integration of the MDR solution through Kaspersky Endpoint Detection and Response Optimum. As a result, the institution now has reports pointing to incidents in the environment to be able to work in the response cycle.

Fundação CASA/SP's IT director says that the entire automation process and setting up security rules provided tranquility to the institution and stability in their technology park. A number of best practices for data management and security were adopted.

Since the environment was adapted to Kaspersky's solution, the upgrade was quick and easy. Teams from Fundação CASA and Kaspersky worked together in the adoption of new solutions. "Our security team monitored the upgrade closely, after all, the willingness and initiative to make this move came from them – from CISO Odenilson dos Santos, and head of IT Alex Christy," says Julio Signorini.

Outcome

With this project, Fundação CASA becomes a reference in the market, raising its level of maturity in cybersecurity, by transforming a scenario of vulnerabilities into a broader and more comprehensive view through investigation, prevention, detection and response resources, automating manual processes and all without high costs or investments in new resources, with total confidence.

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

<https://usa.kaspersky.com/>

kaspersky **BRING ON
THE FUTURE**

2023 AO KASPERSKY. ALL RIGHTS RESERVED. REGISTERED TRADEMARKS AND SERVICE MARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.