DNS4GOV CASE STUDY
PUBLIC ADMINISTRATION, EDUCATION AND RESEARCH

whalebone

Centralized protection for educational and research institutions in Luxembourg

restena

"It just works"

GUILLAUME–JEAN HERBIET,
.LU SERVICE TECHNICAL MANAGER AT RESTENA

Challenge

How to enable effective cybersecurity for 560+ educational and research institutions?

Governments and government institutions all over the world are looking for solutions to enable centralized protection for its critical infrastructure. Whalebone's technology provides a simple way to centrally deliver sophisticated DNS–based protection to institutions heavily targeted by cyber attacks.

"We saw an increase in threats to our institutions and we really wanted to provide them with additional protection. It is a way for us to be more aware about the risks, and for them not to have to worry too much and to be able to focus on their job," says Restena's .lu Service Technical Manager Guillaume–Jean Herbiet. Additionally, some of the institutions need to abide by government requirements on protection and content filtering.

The institutions to which Restena provides internet access have requested that a cybersecurity layer be added to the service. At the same time Restena has started a new wider project to build a SIEM which will monitor cyber threats and provide data which will boost the institutions' cybersecurity.

Moreover, Restena needed a solution which is relevant for Luxembourg, which is a relatively small country, as even a solution using a very large database might not catch relevant local threats if it lacks focus.

The Restena Foundation interconnects and provides network and security services to more than 560 education, research, health, culture, and public administration institutions in Luxembourg, supporting approximately 60,000 employees, students, and other users.

As a key national service provider and operator of Luxembourg's top–level domain infrastructure (.lu domain name registration), Restena needed to enhance the cybersecurity of its connected institutions without disrupting their operations.

"We needed a solution that can catch, for example, phishing campaigns mimicking a local bank or authentication service."

GUILLAUME–JEAN HERBIET,
.LU SERVICE TECHNICAL MANAGER AT RESTENA

Solution

“We know how DNS can be used for malicious activities and how efficient DNS is to combat them.”

GUILLAUME–JEAN HERBIET,
.LU SERVICE TECHNICAL MANAGER AT RESTENA

Restena was looking for a solution for enabling them to stop advanced attack techniques hackers use to compromise modern security: “Many malware types used DGAs for C&C and it is much more efficient to stop the threats through DNS than try to block their IPs with firewall or other solutions,” says Guillaume–Jean Herbiet. As Restena provides DNS resolution to the institutions in question, they can enable protection centrally to any network which chooses to opt–in.

Restena did a market comparison and survey, as finding the solution was a part of a wider EU project. They needed a solution offering both protection and content filtering, as well as high availability and scalability. Also, having an API was important so that Restena could easily extract information from the system to SIEM, and feed it from their other threat intelligence feeds.

Guillaume–Jean Herbiet further describes legal aspects of their desired solution: “We really wanted a solution which keeps as much data as possible locally, and is GDPR compliant.”

> “Of course we interviewed and studied proposals of other mostly US-based companies, but it was never really clear what kind of data they gather, store, and how they use them.”
>
> **GUILLAUME–JEAN HERBIET,**
> .LU SERVICE TECHNICAL MANAGER AT RESTENA

Concerns about net neutrality

Restena is advocating for net neutrality, which was a concern when selecting the solution. “We do not want things to be biased, so we do not think that relying on giant tech companies for DNS resolution is ideal, since it centralizes the DNS resolution within a few companies. Now our institutions can enable or disable the filtering at will, nothing is forced upon them,” Guillaume–Jean Herbiet describes.

Benefits

“We know how DNS can be used for malicious activities and how efficient DNS is to combat them.”

GUILLAUME–JEAN HERBIET,
.LU SERVICE TECHNICAL MANAGER AT RESTENA

“This was a new set–up scheme for Whalebone, since the resolvers are hidden behind DNS proxies (to make sure the institutions do not have to do any configurations themselves), and it worked instantly, exactly as we expected,” says Guillaume–Jean Herbiet.

“In two weeks we had it running for our institutions. Since then, the onboarding is ongoing and goes smoothly,” he continues. “We have run successful tests with DGAs, and the institutions that are using content filtering report that it works well, too.”

Accurate blocking rates are challenging in smaller countries like Luxembourg, as local phishing threats often go unrecognized in global databases. Whalebone addresses this by utilizing regional threat intelligence through partnerships with local telcos and European cybersecurity centers, ensuring high accuracy and low false–positive rates. Guillaume–Jean Herbiet highlights the benefits of DNS protection for public institutions: “It can be easily set up without network changes and allows instant enrollment, as they can use our resolver directly. It‘s efficient and straightforward to deploy, with tailored filtering policies available for specific institutions.”

“This is basically the easiest thing – they just tell us to enable the protection for their institution and immediately start benefiting from it.”

GUILLAUME–JEAN HERBIET,
.LU SERVICE TECHNICAL MANAGER AT RESTENA

ADDITIONAL REFERENCES

Contact our government liaison George Buhai to find a way to protect the core institutions in your country.

immunity@whalebone.io

We will be more than happy to answer any questions. Mutual satisfaction is our main goal and we will do our best to fulfill your requests.

www.whalebone.io

Learn more about our products at: **whalebone.io/immunity**

Follow us on LinkedIn for more information on DNS security.