How global labs protect sensitive testing data

The customer summary

Organization
Eurofins

Headquarters
Luxembourg

Users
45,000

Industry
Life Sciences

The Challenge

Keeping sensitive data secure around the world

When you work with data, security is always top of mind. This is especially true for Eurofins, an international life sciences testing company with more than 800 labs in 47 countries. Their 45,000 employees run 400 million tests each year, on everything from food to pharmaceuticals to forensics. Eurofins laboratories around the world are helping to improve cancer treatments, fight the growing problem of antibiotic resistance, catch criminals, safeguard the health of bees, ensure our food and water is safe, determine paternity, and beat viruses like Zika, among many other things.

That's a lot of employees, in a lot of places, working on a lot of sensitive data. So keeping it all secure is a big challenge. "It's important that we prove to our customers that we can keep their data safe," said Romain Dawidski, Network Architect at Eurofins. "We also need to follow strict data privacy laws across everywhere we work, including in the United States and Europe."

Over the past 30+ years, Eurofins has worked hard to make sure their data doesn't fall into the wrong hands. But these days, as more applications and infrastructure move to the cloud, more people working off-network (and "forgetting" to turn on the VPN), and cyber attacks rising in sophistication, traditional approaches to security just can't keep up. The Eurofins team decided to improve this first line of defense, which led them straight to Cisco.

Objective

Eurofins needed a simple solution that's powerful enough to protect their complex organization, and keep their sensitive data safe.

Solution

Cisco Umbrella
Cisco AMP for Endpoints
Cisco Umbrella Investigate

Impact

- Deployed Umbrella to 90% of the users in a single day
- Bolstered security for on- and off-network users
- Blocked 220,000 malicious requests in the first month
- Discovered 6,500 apps across the business
- Helped comply with data laws like EPA and GDPR

> "Our numbers show that Umbrella is really effective at blocking requests before they reach our other lines of defense. It's cutting down on the noise and sending less traffic to our other security tools."
>
> **Romain Dawidski**
> Network Architect at Eurofins

The Solution

Adding a first line of defense

After testing out several security solutions, Eurofins soon landed on Cisco Umbrella. By delivering security at the DNS-layer, Cisco Umbrella can block many malicious attacks at the earliest point, before they ever reach the network or endpoints.

Plus, with the Umbrella Roaming Client, Eurofins can protect employee laptops 100% of the time, when they are on the road and not connected to the VPN.

"A huge benefit of Umbrella is that it works at the highest layer, the DNS layer," said Romain. "This is extremely efficient and gives us more visibility than other tools like, say, our web proxies. It means that Umbrella blocks attacks sooner, before our users ever see the effects."

Along with Umbrella, Eurofins plans to also roll out Cisco AMP for Endpoints in conjunction with Cisco Threat Response. This will let them block or contain known threats automatically—across all their endpoints, with a single click. Threat Response automates integrations across Umbrella, AMP for Endpoints, among other products and accelerates key security operations functions: detection, investigation, and remediation. "We can already see that this will give us even more control and visibility on security events, especially for our applications," said Romain. "Once we deploy AMP and start using Cisco Threat Response, it will be very useful to have one single dashboard that can correlate all security events together."

"For Eurofins, a simple yet powerful solution was key. If we'd tried to layer a complex solution over our complex organization spread around the world, it would be too difficult to manage."

Romain Dawidski
Network Architect at Eurofins

The Results

Cutting down on the noise

Given the simplicity of Umbrella, Eurofins was able to roll it out to 90% of its users in just one day. All while keeping their labs humming.

Already, they're racking up some impressive stats. In its first month, Umbrella analyzed 180 million requests and blocked 220,000 of them, spanning more than 20 types of threats.

"Our numbers show that Umbrella is really effective at blocking requests before they reach our other lines of defense," said Romain. "It's cutting down on the noise and sending less traffic to our other security tools. Which means our team is spending less time reviewing issues. And our security tools are performing better, too."

Drilling down to the details

Not only does Umbrella block malicious attacks, it also gives Eurofins new insights into what's going on, when, and where. "We're impressed with the Umbrella dashboard," said Romain. "It's very easy to understand and straightforward to manage. And by feeding Umbrella data into our other security analysis tools, we're getting a more complete picture of our network, devices, and apps."

Case in point: With Umbrella's App Discovery feature, they've found a whopping 6,500 apps used across their labs. And Umbrella assigns each one a risk score, so they know which apps to keep a close eye on. "In the past, it's been hard for us to keep track of all the apps running on our systems. Now, we can use this list from Umbrella to put together a complete list of approved apps," said Romaine. "And we can block the more risky apps."

Eurofins also leans on Umbrella Investigate to see exactly why a website was blocked and gain the security context needed to uncover and predict threats. "Investigate is powerful and lets us drill down into the details," said Romaine. "Sometimes, it's the site's registration. Or it's the location from where the DNS request was triggered. We can take a look and quickly decide if we want to add the domain to our white list. We also use the Investigate API integrated with our SIEM, to enrich our threat intelligence and correlate security events."

Leaning on a dedicated Cisco team

Through it all, Eurofins appreciated working closely with their Cisco Customer Success team. "The Umbrella customer success team has been very helpful and easy to work with," said Romain. "The Cisco engineers and support team are quick to answer all my in-depth technical questions. They've helped me create custom Investigate dashboards."

> "Umbrella is so easy to roll out and use. Yet it's also a powerful layer of defense that gives us a more complete snapshot of what's happening across our network, devices, and apps. The numbers we've seen speak for themselves."
>
> **Romain Dawidski**
> Network Architect at Eurofins