Archroma Case

About Archroma

Archroma is a global, diversified provider of specialty chemicals serving the branded and performance textiles, packaging and paper, and coatings, adhesives and sealants markets. Headquartered in Reinach, Switzerland, Archroma operates in over 100 countries, with 3,000 employees located in 35 countries and 26 production sites.

Archroma is passionate about delivering leading and innovative solutions, enhancing people's lives and respecting the planet. The company is committed to the principles of "The Archroma Way to a Sustainable World: Safe, Efficient, Enhanced. It's our nature!"; an approach reflected in its innovations, world-class quality standards, high service levels and cost-efficiency.

About Edgescan

Edgescan offers a Vulnerability Management Security as a Service (SaaS) solution. The edgescan™ SaaS security solution manages thousands of assets across the globe for both enterprise and SME clients helping them to continuously detect, prioritise, monitor and fix security weaknesses for Internet-facing systems, such as web applications, websites, mobile apps, servers, firewalls, VPN's or VoIP services. Due to analyst validation of all discovered vulnerabilities, the solution is highly accurate and virtually false positive free.

"Our partnership with Archroma has been a great success, Edgescan has assisted them with improving their security posture on a continuous basis.

By helping organisations such as Archroma address ongoing cyber security issues and vulnerability identification they enjoy a lower attack surface, the ability to measure improvement and monitor their security posture on an ongoing basis. The commitment we see from Archroma when it comes to securing their assets is truly impressive, and we look forward to continue working with them in the future."

Eoin Keary, CEO and founder of Edgescan

Archroma Case Study

Questions & Answers

What were the challenges Archroma was facing from a security perspective?

We are a relatively young company, and we brought Edgescan on board quite early on, so rather than transitioning from another vulnerability management solution it was more a case of deploying the Edgescan SaaS across our IT infrastructure. We operate in the Operational Technology (OT) space, as well, but currently we have a different approach to securing that side of the business.

When we adopted Edgescan, our focus was to ensure that security was designed into our processes, building it from the ground up and embedding it into our operations.

Did you consider other solutions before you settled on Edgescan?

Yes, we went through our regular sourcing process, but the other vulnerability management solutions that came up against Edgescan were all fully automated. The human factor was what tipped in favour of Edgescan: we really saw the value in having a team of qualified pen testers verifying each and every vulnerability, providing us with intelligence and patching support should we need that.

“Edgescan gives us the peace of mind that comes with knowing that our vulnerability management solution is virtually false-positive free.“

How did you find the onboarding process?

The onboarding was very swift. We started with an asset discovery, and it didn’t take more than two weeks to have the solution up and running, and set up across Archroma’s entire IT infrastructure.

How has Archroma benefitted from using Edgescan?

Edgescan gives us the peace of mind that comes with knowing that our vulnerability management solution is virtually false-positive free. The accuracy that comes with human validation, paired with the efficiency of automatic, continuous scanning, means that my team now knows that whenever a vulnerability is flagged, the vulnerability is there, and they can continue working until they find it and fix it.

Archroma Case Study

Questions & Answers

Have you seen a quantifiable return on investment after you brought Edgescan on board?

ROI is notoriously difficult to quantify in cybersecurity, but according to Edgescan's own data, the validation of vulnerabilities saved 4500 staff hours.

I think that's where the real value of this solution lies: having a team of qualified professionals on the case 24/7 means that my team can focus on higher tasks in the security function. Furthermore, the certainty that when an alert is raised this will not be a false positive is another crucial time saver: my analysts trust that if the platform tells them there is a vulnerability to fix, the vulnerability will be there.

This didn't happen overnight: the team needed to gain trust that the solution was accurate. When they realised that there were virtually no false positives, Edgescan's vulnerability management platform really helped us stay one step ahead. Time saving has been the best observable outcome since we brought the Edgescan's SaaS on board.

As part of the ROI we have also been free of major cybersecurity impacts due to proactive management and mitigation of vulnerabilities across our infrastructure.

Are you planning to expand your adoption of Edgescan solutions in the future?

"Edgescan Penetration testing" is definitely something that we are looking into. At this point, we definitely see the value of going with a vendor that is already familiar with our infrastructure and has helped us during last years. Thus, we'll evaluate it through our regular internal sourcing procedure against other alternatives in the near future.

The OT side of our business is also an area we are looking to further enhance capabilities: we currently have strong protections in place, but as we approach into advanced Internet of Things (IOT) solutions, automations and other digitalization initiatives, we'll be looking at Edgescan as a possibility to strengthen particularly the OT area vulnerability management.

Trusting your provider is key

The key here, I think, is trust. You can't buy trust, and the fact that my security team already trusts Edgescan's platform, its intelligence and expertise is a very important factor for me. This is where customer support also comes into play: the solution is so accurate that we didn't find ourselves in need of this service very often, but whenever we needed support or advice, it has been flawless. Every time my team asked for their help, Edgescan's analysts would instantly investigate the issue and explain it in detail.

Archroma Case Study

Questions & Answers

“As part of the ROI we have also been free of major cybersecurity impacts due to proactive management and mitigation of vulnerabilities across our infrastructure. “

Is there any other benefit that you’ve been able to observe since you brought Edgescan on board?

I see two main benefits, the first one is the support with our commitment to Sustainability, in all business functions, something that

Archroma is incredibly serious about sustainability. We know that the future of our planet is in our hands, and we are committed to maintain our environmental impact at the absolute minimum.

Our choice of cybersecurity vendors might seem irrelevant in this context, but Edgescan’s solution has a hidden benefit in terms of reducing emissions via its IP scanning function. Set up as to alert the customer whenever a machine is turned on, this allows us to keep track of the IT infrastructure both from a security and a sustainability perspective by enabling us to see which assets are active and when, and consequently assessing whether they should be or not.

The second benefit I see is the easy and straightforward reporting.

Reporting can be time consuming, but we found that the Edgescan platform provides the team with all the metrics they need for easy and seamless reporting. This is also a time saver, which is particularly relevant as the skills gap in cybersecurity makes it ever so important to optimise how an IT security function’s time is used. This allows my team to focus on higher level security tasks, as reporting is really a no brainer.