We are evolving to pursue our mission: protecting your endpoints

By Grégoire Germain, CEO and co-founder of HarfangLab

HarfangLab is now 6 years old. This is an opportunity to look back at the genesis of the company's project. This, to share our vision of the future and reaffirm our identity now that we've gained in maturity. A company evolves over time, to remain relevant to the reality of the environment in which it gravitates. The cybersecurity world has changed since 2018, and so have we.

The beginning – all about performance

Fast forward to 2018. With Maxime Rameau, Xavier Boreau and Mathieu Gaspard, we saw a need that became our project. It then turned into our mission: to deliver organizations defense tools, that would be as performing as the ones used by cyber-attackers. As we consider the endpoint as the nerve center of the Information System, **has developped an EDR software**.

Since its creation, we have had three main ambitions, linked to three critical needs of defenders, our customers, and our partners:

- **The performance of our tool**, to stay one step ahead of cyber-attackers with intelligence and proven ability to anticipate, detect and block attacks. The solution is lightweight but yet robust. It runs on a single agent with 5 complementary detection engines, proprietary AI models and proven detection efficiency, both in "real life" and over independent tests, with minimal impact on the performances of the protected system.

- **Trust**, because an EDR software, with an agent installed on all an organization's endpoints, is intrusive by nature. It needs to have visibility of all possible points of entry for the threat. That's why we've made it a point of honor to provide a tool that adapts to our customers' architecture and trust space, and not the other way around. To this end, and in order to enable strategic autonomy, we are today the only EDR to offer the same performance for a deployment in a private cloud, within an organization's own infrastructure, or in the cloud chosen by our customer.

- **Intuitiveness and simplicity**, to enable the EDR users, whether they are analysts at our MSSP partners or our customers, to have a tool easy to operate. This requires strong technological choices, such as the implementation of AI algorithms to facilitate the exploitation of security events, an easy-to-use interface, and the transparency of detection rules, which facilitates resilience and continuous learning, with each security alert.

We are convinced that SOCs and cybersecurity *as a service* are the future of cybersecurity, because they enable greater proximity. This is why we have chosen to market our solution exclusively through MSSP partners.
But these players need effective, high-performing tools to cope with the shortage of human resources and growing needs. That's one of the reasons why we invest in and rely on technologies and particularly in artificial intelligence, but I'll come back to that later.

Today, we are proud of our product and our company, which now counts 100 employees in France and Europe. We are proud of the ecosystem we've built, and of the hundreds of customers who trust us. Our performance is recognized, as testified by our excellent results in the MITRE tests in 2023, positioning us among the best EDRs on the market. And this quest for performance and excellence will always be our top priority.

Thanks to our fundraising in 2023, we have been able to accelerate investments to reach a new stage in our development. Our ambition is to become a **key European player, offering a complete range of endpoint cybersecurity solutions.**

Growing also means evolving and adapting to the realities of the market and the international context.

For us, expertise is one of the keys to performance, in the contrary of the dispersion of an offer, and mediocrity.

Expertise also means addressing globally endpoint security issues, in response to the real needs of our partners and customers, and in line with our technological capabilities.

Further than the EDR, and thanks to the vision offered by our strategic observation position in the Information System, we now want to be the first line of cyber defense from the endpoint upwards. So, of course, we are maintaining our EDR and continuing to improve it by adding cutting-edge technological bricks, but as of this year, **we will also be offering IT monitoring technologies**. This offering will give organizations a better understanding of their attack surface from their endpoints, fight shadow-IT and facilitate IT auditing. This offer is in line with the need to increase corporate resilience in terms of cybersecurity, and with the European Union's regulatory and compliance requirements (NIS 2) aiming directly at achieving this same resilience objective.
In addition, we will also be **offering a new-generation antivirus solution**, fully complementary to our EDR. With this new approach, HarfangLab will offer a cybersecurity alternative, fully integrated within a single agent, from the endpoint. With this single agent, we aim to offer more advanced threat detection, seamless integration and comprehensive monitoring of an organization's digital health. And always within the trusted infrastructure chosen by the customer: public cloud, a private cloud, or directly on-premises.

This commitment is reflected in the various technological segments that will feed our tools and contribute to the collective intelligence when it comes to cybersecurity. We can no longer afford to take a reactive approach when it comes to protecting valuable assets. We need to study the threat, in a different timeframe from operations, to better understand and share it. As part of this approach, **a cybersecurity research team joined our workforce at the end of 2023.** We are also convinced that artificial intelligence can provide critical answers to this challenge of anticipation. We have been investing for over 5 years and we are continuing our research to provide concrete use cases for AI in cybersecurity, to multiply cyberdefense operators capacities.

To be more precise, we have our own AI engines, based on the complementarity of deep learning and machine learning. They are capable of refining threat detection and automating many responses. We believe that AI can also meet the need of processing information, identifying priorities, classifying and accelerating reporting procedures. The aim is always to make cyber analysis more accessible, but above all more efficient, and to refocus human skills on critical activities. In the coming months**, HarfangLab will be introducing a number of new AI features.**

The 2024 year represents a turning point. Our world is in tension. In addition to ongoing armed conflicts, it's also a war of information, sometimes discreet, but often formidable. It's the use of cyber tools to destabilize, disinform, spy on and disrupt organizations. It's the use of digital technology as a competitive advantage, enabling the domination of certain companies and states, or the subjugation of entire economies. It's a war that Europe cannot afford to lose. It highlights the need for Europe of being able to rely on its own technologies and to guarantee its autonomy to remain master of its destiny. More than ever, this legitimizes the choice of deploying cybersecurity tools in one cloud rather than another, in a SecNumCloud approach, or directly in one's own infrastructure.

This is why HarfangLab defines itself today as a player for European performance, autonomy and excellence.

I'm looking forward to presenting you with the fruits of our teams' labors, to exchanging ideas with you, and to pursuing our mission of providing powerful, high-performance tools in the ongoing fight against the damage caused by cyberthreats, without compromising trust or your independence.