SentinelOne™

SentinelOne helps Labeyrie optimise the security of its endpoints

Labeyrie was able to free itself from legacy antivirus software and opt for a next generation, full cloud solution for endpoint protection which is outsourced and managed in IMS Networks' SOC to increase security effectives, save time, and increase efficiency

SentinelOne Proof Of Concept

Layberie Fine Foods is a rapidly evolving industrial group which regularly integrates new acquisitions. This results in a strong need to optimise time and resources, as well as simplicity of administration. Finding solutions that are efficient, resulting in better outcomes while saving time is key to the group's digital transformation. This is why the security team decided to outsource parts of its security to specialists, and in doing so, upgrade to cutting-edge solutions.

In this context, in 2016 the security department decided to review the protection of its workstations: "We had worked with two different antivirus software vendors over 10 years, and we hoped to optimise the solutions in place to not only be more cohesive but also more effective," said **Benjamin Guiroy, CISO of the Labeyrie Fine Foods Group**. "The arrival of cryptolocker was a game-changer and showed us that we needed to tighten the net and be much closer to users. Furthermore, in the current climate antivirus solutions were no longer enough to guarantee optimal protection. Changes could bring with them new issues: extra modules, time-consuming updates, slower endpoints, etc. We needed to find an effective solution which wasn't likely to obstruct and slow down work."

LABEYRIE FINE FOODS

Based in St Geours de Maremne in the Landes region, Labeyrie Fine Foods is a European group in the agro-food sector which owns the brands Layberie, Blini, Delpierre, le Traiteur Grec, Farne of Scotland, Lyons Seafoods, Père Olie and King Cuisine. The group totals a workforce of around 5,000 people spread across 20 sites.

LABEYRIE
FONDÉ EN 1945

The security group, which is constantly evaluating new technology, identified a number of solutions that could fit the bill, including the EPP (Endpoint Protection Platform) from SentinelOne, which offers next-generation automated protection for endpoints and servers. SentinelOne's EPP combines the prevention, detection and management of threats in a unified platform. The EPP solution benefits from next generation machine learning (automated learning) and automated processing that enables even earlier detection of malicious behaviour from the main attack vectors, while identifying exploits, scripts and file-less malware in real time, and all this without having to wait for threat signature updates to be published or download multiple agents.

The security department carried out a test of the solution over several months in full-cloud mode, and it proved to be particularly successful. "The POC was a revelation because the solution is very effective and handles the complexity of the threat analysis in a totally transparent way. It has caused us to change our perspective and remove our reliance on a black box solution," explains Benjamin Guiroy.

Choosing SentinelOne

Its mind made up, the security team decided to opt for the SentinelOne solution, which is integrated and managed directly from the SOC of its partner, IMS Networks. The ease of integration to the SOC and the inherent reduction in administration of the solution have been two of the main benefits. The SOC receives alerts and an escalation process has been defined to prioritise threats according to their level of severity. The security team also appreciates the feedback on the logs which allows them to identify trends in ongoing activity, for example the detection of non-conforming executables. According to the relevance of the feedback, the team refines its security and processes. The team has shifted from a reactive to a proactive and pre-emptive posture.

Another interesting point that the security team has noticed relates to the user's desktops: "We have far fewer calls. The solution seems to have a lighter impact on the end point devices and we don't need to keep doing regular scans to find potential threats. This means less "hassle" for the security group and more comfort for the users. In the final analysis, the solution perfectly meets our needs, allows us to optimise our time, improves management and therefore optimises efficiency, both on the Labeyrie side as well as the analysts in the SOC of IMS Networks," concludes **Benjamin Guiroy, CISO of the Labeyrie Fine Foods Group**.

About SentinelOne

SentinelOne is shaping the future of desktop and server security with an integrated platform which unifies the detection, prevention and resolution of threats launched by nation states, terrorist organisations and organised crime. The unique approach of SentinelOne is based on in-depth inspection of all the processes within a system combined with the abilities of artificial intelligence and innovative automated machine learning. This permits the rapid identification and isolation of malicious behaviours, protecting the devices against targeted and advanced threats in real time. SentinelOne was created by an elite group of security and cyber-defence experts from IBM, Intel, Check Point Software Technologies, McAfee, Palo Alto Networks and Israeli defence forces. To find out more, visit www.sentinelone.com or follow us on Twitter @SentinelSec.

SentinelOne™

Media Contact : Cymbioz
Rémi Brossard – Account Director
T. +33 (0)1 42 97 93 80
P. +33 (0)6 62 70 56 50
remi.brossard@cymbioz.com
www.cymbioz.com