CUSTOMER CASE STUDY

MAZ increases and simplifies protection of its endpoints with SentinelOne

Overview

MAZ was founded over a century ago and has 80 healthcare centers and two of its own hospitals, providing services to more than 88,000 member companies in all Regional Communities and Towns. This life insurance company is linked to the Ministry of Employment and Social Security and manages healthcare and economic services (collection of sick leave) for over 600,000 workers suffering from occupational accidents and professional illness.

This philosophy of supplying services to companies and individuals prevented MAZ from ignoring aspects like innovation and helped it to increase its technical and medical capacities, whilst protecting clinical and personal information on its members. As a life insurance company, MAZ must guarantee that all third party data in its possession is "particularly protected", following the guidelines contained in article 7 of Organic Law 15/1999 regarding Personal Data Protection (LOPD) for its processing.

INDUSTRY

Life Insurance Company

MAZ PLACES ITS TRUST IN SENTINELONE TO INCREASE ITS PROTECTION AGAINST

- Sophisticated exploits
- Next-generation threats

MAZ DEPLOYMENT

- SentinelOne Endpoint Protection Platform (EPP) solution in its network topology to protect over 1000 endpoints
- SentinelOne EndPoint Protection to protect 100 servers.

BENEFITS

Both agent-based platforms are highly scalable and lightweight solutions offering real time detection, protection, remediation and forensic analysis of new generation malware.

Towards a new endpoint security paradigm

Wi-Fi networks, Cloud mobility and applications make endpoint more difficult to protect.

With 20% Internet traffic, MAZ used to receive 2000 potentially dangerous attacks/threats a day from the outside. However, this data was only an estimate as endpoint is not currently equipped with a tool capable of generating these statistics and quantifying the threats specifically directed towards the job and not only against network entry/exit points.

Eduardo Gistau Arbués,
Systems, Telecommunication and Security Supervisor at MAZ.

"We used to use a traditional antivirus solution for endpoint protection. Like any other legacy solution, its main problem was its incapacity to detain advanced attacks by modern ransomware, for example, "Although the protection offered by many other security barriers prevented us from suffering the impact of any threat, MAZ remained focused on excellence and decided to start producing a next-generation endpoint protection solution."

After carrying out an in-depth laboratory study of solutions existing on the market (consolidated and niche) and analyzing the results using stress tests, it was concluded that SentinelOne was the best balanced solution: with nearly 100% levels of effectiveness, simple to use and capable of minimizing the increase in costs. Therefore, the fact that SentinelOne covers all current operating systems: Windows, Linux y Mac, as well as older versions of other operating systems like Windows XP, it was a key factor for the IT department at MAZ.

"Absolute security does not exist but SentinelOne alone allows us to restore any infected devices to their original state with a single click of the mouse. Some previous alternatives stopped the attack but that was not sufficient. Impact caused by cyber threats must also be quickly identified, stopped and computers reverted to an original state with confidence", adds **Eduardo Gistau**.

A single suite deployed as a single agent

As this is a hybrid solution (Cloud/on premise) where no Cloud intervention is necessary and a very lightweight endpoint agent is deployed that consumes very few resources of the end device, start-up is almost immediate.

Therefore, several processes (Analysis, Evaluation, Laboratory tests, Retrospective and technical/executive scaling and Selection) took place before a preliminary approach through Exclusive Networks in May 2016 to finally start production in June of the same year.

Six months later, the endpoints park at MAZ is now fully protected, with no intrusions or incidents and with extremely low false positives. Endpoints are also much less saturated in a CPU and when accessing a disk, so they are released to other production processes.

It is important to mention that the platform receives feedback from thousands of endpoints deployed at clients like MAZ, meaning that accurate marking of threats and losses of resources found when analyzing false positives/negatives are significantly reduced.

Summary

""The product totally satisfies clients. It was quick and easy to use and the fact that users do not interact in any way with the solution prevents any wrong or undesired decision from being reached due to human error or omission", says Eduardo Gistau. "The quality of the technical service supplied by our reliable wholesaler and the manufacturer is also 100% effective and therefore highly recommended. Today, SentinelOne is undoubtedly the best-balanced platform with the best objective price."

SentinelOne™

To find out more, visit www.sentinelone.com
or follow us on Twitter @SentinelSec.