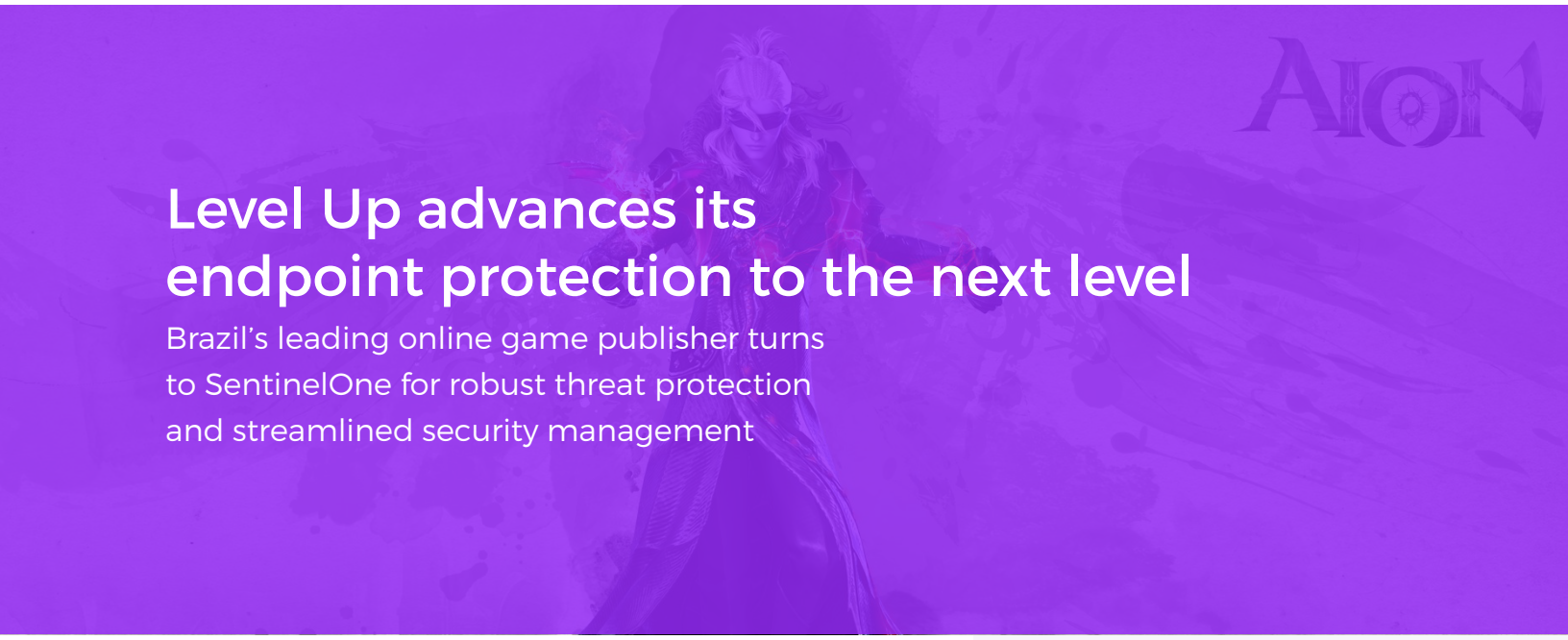
SentinelOne
The future of endpoint security



Level Up advances its endpoint protection to the next level

Brazil's leading online game publisher turns to SentinelOne for robust threat protection and streamlined security management

Overview

A pioneer in the Brazilian market of online games, Level Up develops partnerships with leading game producers worldwide, enabling the company to deliver the best and most anticipated content to its loyal user base. Level Up offers a set of fully translated titles in Portuguese, as well as exclusive access to international blockbuster games to millions of gamers across Latin America.

Level Up's IT department supports all of the infrastructure used for game publishing, localization, integration, and security. The team also supports the company's web presence and integration sites with other resellers. "We entered the online gaming market in Brazil 12 years ago," noted Rogério Torres Fernandez, IT Manager for Level Up. "We had a very successful launch with the Ragnarök game, and now offer seven additional games to our users in Brazil. We are in charge of the infrastructure and localization of those games, as well as sales and marketing of all of our offerings in Brazil."

KEY CHALLENGES

- Having dificulty blocking an increasing number of DDoS attacks
- Existing antivirus solution was unable to identify or prevent cyberattacks

BUSINESS BENEFITS

- Blocked 1900 intrusion attempts
- Obtained the ability to easily see the status of attacks
- Simplified management with an intuitive user console

level up

IT and business challenges

The online game market has long been a target for cyber criminals. “We are continually trying to defend ourselves against people trying to attack our servers, and our company undergoes several DDoS attacks and intrusion attempts each year,” noted Fernandez. “Our business is to sell the ‘currency’ of the game. A lot of malicious users try to invade our systems to obtain the ‘coins’ within games, and either use the currency themselves or resell it to other players. Most of the attacks are from China.”

Level Up was relying on a traditional antivirus solution that involved a lot of manual steps for attack identification and prevention. “We came to the conclusion that just using a normal antivirus solution was no longer enough to prevent attacks,” admitted Fernandez. “We were looking for a more powerful solution that could perform application behavior analysis to improve our security posture.”

After hearing that Netflix was migrating to SentinelOne, Level Up decided to investigate the solution for its online game sites. “Once we saw a demo of SentinelOne, we knew it was the powerful endpoint protection tool that could solve our security problems and let us sleep at night,” Fernandez said.

Rogério Torres Fernandez,
IT Manager, Level Up Interactive Ltda

“Once we saw a demo of SentinelOne, we knew it was the powerful endpoint protection tool that could solve our security problems and let us sleep at night.”

Solution

Level Up began implementing the SentinelOne Endpoint Protection Platform (EPP) with a small pilot project for its internal oice systems. After seeing how well it performed for those applications, the IT team started installing SentinelOne in the much larger games environment. “We performed the installation process very cautiously, because with our games, anything that afects system performance decreases the playability of our games. Luckily, the deployment went very quickly and smoothly, without impacting the end user experience.”

Business benefits

SentinelOne is now providing Level Up with the ability to detect malicious behavior across major attack vectors. SentinelOne's solution enables Level Up to achieve greater management efficiency by alleviating the need for regular interaction with the management console. SentinelOne also provides Level Up with heightened visibility into all threats coming into their network, providing broader and more robust threat detection that substantially reduces the company's risk of a data breach.

"We don't have to interact directly with the SentinelOne console on a daily basis, we just use it to access the system to see why a particular service was blocked," Fernandez explained. "We now run the SentinelOne management tool in automatic mode. When a service stops working, when someone makes a complaint, or an alert comes in from the tool itself, that's when we log in and analyze the situation. With its intuitive management console, we can immediately see the status of an attack and take steps to prevent the intrusion."

Summary

"By using SentinelOne, we have been able to detect 1900 infection attempts that we wouldn't have been able to detect if we were just using the anti-virus solution," Fernandez concluded. "We are very happy with the SentinelOne Endpoint Protection Platform and are now extending its protection to all of our other IT environments. SentinelOne is an excellent security product and has enabled us to prevent a much larger number of attacks. We would definitely recommend SentinelOne to other companies that want to improve the security of their connected endpoints."

About SentinelOne

SentinelOne is shaping the future of endpoint security with an integrated platform that unifies the prevention, detection and remediation of advanced threats from all major vectors of attack. SentinelOne's unique approach is based on deep inspection of all system processes combined with innovative machine learning to quickly isolate malicious behaviors, protecting devices against advanced, targeted threats in real time. SentinelOne was formed by an elite team of cyber security experts from IBM, Intel, Check Point Software Technologies, McAfee, Palo Alto Networks and the Israel Defense Forces.

To learn more visit sentinelone.com or follow us at @SentinelSec.

SentinelOne
The future of endpoint security

For more information about SentinelOne Next-Generation Endpoint Protection Platform and the future of endpoint protection, please visit: sentinelone.com