guararapes

Brazilian Fashion and Retail Business Protects 30 Million Customers' Financial Data With CrowdStrike Solutions

When the Brazilian fashion powerhouse Guararapes Group decided to set up Midway bank to offer financial services to its customers, it kick-started the company's journey to building a robust, financial-class cybersecurity infrastructure for the entire business.

"It is like this," said Rodrigo Godoy, CISO at Guararapes Group. "Imagine you have a simple house. Then you renovate it into a beautiful home with a swimming pool, fancy cars and the like, which attracts the bad guys. Now you need a wall, an electric fence, but without an alarm you are in trouble. In setting up our bank, we were mindful that a bank relies on customer trust and if trust is lost because of inadequate security, it's gone."

Guararapes is the largest fashion group in Brazil with a national retail operation comprising over 360 retail stores, including the Lojas Riachuelo retail chain. It collaborates with both Brazilian and international designers and fashion celebrities and luxury brands, such as Versace and Karl Lagerfeld. The group's 40,000 employees encompass most of the fashion lifecycle with the company describing itself as "involved from the thread to the last installment."

Legacy Antivirus Could Not Protect the New Digital Bank

Company executives realized the group was increasingly handling more of its customers' money and offering them financial services such as store cards, insurance and loans. They decided to set up digital-only Midway bank to support customers. Having prior experience in the banking industry, Godoy was hired to address cybersecurity not only for the bank, but also for all of Guararapes and its 30 million customers. He formed a new security group with a mission to strengthen defenses and bring the company up to financial cybersecurity standards. This was set in the context of a group-wide digital transformation strategy, shifting services and applications to the cloud, improving ecommerce and developing a digital marketplace. There also were new data regulations, such as the Brazilian General Data Protection Law (LGPD), that needed to be respected.

The group had a traditional antivirus solution in place but managing it was complex and time-consuming. It had to be physically installed on 7,000 devices and then reinstalled every time a device was replaced. Once installed, the application would slow down the endpoint, especially older machines, which impacted user productivity.

INDUSTRY
Retail

LOCATION/HQ
Natal, Brazil

CHALLENGES
- Launch of banking services demanding financial-class security
- Protecting data and financial information for 30 million customers
- Existing antivirus outdated, underperforming and a drain on resources

SOLUTION
When Guararapes Group decided to set up a bank to offer financial services to 30 million retail customers, it used CrowdStrike to improve endpoint security protection for the bank as well as the rest of the group's operations.

"CrowdStrike really stood out against other solutions. We scaled the solution quickly and in just three months, had the whole deployment installed and working, identifying incidents in the environment and creating specific rules."

Rodrigo Godoy
CISO
Guararapes Group

CrowdStrike Deployed to 7,000 Endpoints After Extended Pilot

As a seasoned CrowdStrike user, Godoy wanted to make CrowdStrike one of the key pillars of the new security infrastructure. However, first he wanted to ensure CrowdStrike worked for the group's mixed retail, manufacturing and finance operations. The company evaluated various products to see if they could support 7,000 endpoints. Then, in three days, Guararapes worked with CrowdStrike to set up a proof-of-concept pilot. "That is when we saw the simplicity, the ease of operation and functionality of CrowdStrike," he said.

The pilot was supposed to last 15 days, but it proved so successful that it ran for 60 days and became part of the full project rollout. "CrowdStrike really stood out against other solutions," said Godoy. "We scaled the solution quickly and in just three months, had the whole deployment installed and working, identifying incidents in the environment and creating specific rules."

Guararapes now uses numerous CrowdStrike Falcon® platform modules to protect 7,000 endpoints across all parts of its business operations from point-of-sale devices to computers in its factories. Godoy has set up a 24/7 security operations center (SOC) integrated with Falcon Complete™, CrowdStrike's managed detection and response service.

In partnership with CrowdStrike, the company is using the Falcon platform to develop use cases (e.g., when an incident occurs and there is an alert) backed up by an action playbook to handle similar incidents in the future. For example, if a machine shows signs of abnormal behavior, it generates an alert in the SOC so the machine can be isolated from the network without causing any harm. "This has helped us a lot," Godoy said. "And it is a huge gain in our incident response process."

Security Team Relieved of Huge Support Burden

CrowdStrike has relieved the security team of a huge maintenance and support burden. "I no longer need a focused team to look at endpoint security, to look at the health of servers and systems to see if they are working because this is what CrowdStrike does," said Godoy.

Unlike the previous antivirus solution, CrowdStrike has had little, if any, impact on endpoint performance. CrowdStrike has been easy to integrate with other systems, such as DevOps, in the business. "When you have a traditional antivirus solution, it slows down servers and applications," said Godoy. "Sometimes an antivirus product is misconfigured or has an inappropriate time signature distribution which causes problems. With CrowdStrike, we have had none of these issues."

One of the main challenges prior to CrowdStrike was visibility into what was happening within the Guararapes environment.

"My greatest difficulty before CrowdStrike was having visibility to attacks in real time. And since CrowdStrike does not need constant updating, it is able to spot new malware and viruses automatically. Before, these could sit there quietly on a machine waiting to attack. Greater visibility means we can respond faster to these malicious attempts and incidents."

Intelligent Threat Analysis Improves Productivity

Guararapes uses CrowdStrike for intelligent threat analysis by identifying new incidents and scenarios, documenting them and developing remedial actions. Godoy added that CrowdStrike has

RESULTS
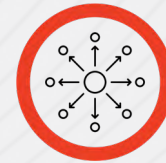
Raised security stance to financial-class protection

Fast, seamless and simple solution deployment

Built a strong, trust-based and collaborative partnership

ENDPOINTS

7,000

CROWDSTRIKE PRODUCTS

- Falcon Discover™ security hygiene
- Falcon Complete™ managed detection and response
- Falcon Intelligence automated threat intelligence
- Falcon OverWatch™ managed threat hunting
- Falcon Insight XDR™ endpoint detection and response
- Falcon Prevent™ next-generation antivirus
- Falcon Spotlight™ vulnerability management

a series of dashboards to monitor and visualize activity using a real-time heat map. The solution even helps him and his team monitor whether a device is running the correct applications. Before, this would take months to resolve.

These improvements in visibility, real-time monitoring and automation, in addition to the CrowdStrike solution's cloud-native architecture, have improved productivity significantly. "One of the biggest benefits of CrowdStrike was the time I had to execute the project," said Godoy. "It was all very quick because we did not have to go machine by machine, or use the infrastructure team on long, drawn-out projects that typically could take a year before showing results." For the technical team, CrowdStrike has improved productivity by 70%, enabling staff to spend time on more valuable functions and services.

Partnership with CrowdStrike Is Key to Success

The partnership that Guararapes has established with CrowdStrike has been key to the success of the solution. "We have a partnership with CrowdStrike, not a relationship between client and supplier," said Godoy. "Whatever we need, CrowdStrike is always there for us. When several competitors suffered attacks, CrowdStrike worked with us and shared knowledge to identify what happened, if those incidents could impact Guararapes, and how we can protect ourselves. This has been a great aspect of the relationship with CrowdStrike, which continues to grow."

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: https://www.crowdstrike.com/

Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/