voices

CrowdStrike Customer Case Study

GMG

Global Company Reduces Annual Incident Remediations by Over 96% with CrowdStrike Managed Detection and Response

Whenever a GMG customer shops at one of over 500 retail stores across the Middle East, North Africa and Asia or via the company's ecommerce website, their personal data and financial information is being protected by a managed detection and response (MDR) solution built on the industry-leading and cloud-native CrowdStrike Falcon® platform.

Increased Cyberattacks an Unintended Outcome of Growth

Founded in 1977, GMG is a global retailer, distributor and manufacturer of sporting goods and food and health products that markets 120 brands in 12 countries. The conglomerate in recent years has undergone two significant efforts: a rebranding to make GMG more recognizable, and a broad digital transformation to enhance its operations, drive growth and improve the customer experience.

While the two projects have been highly successful, an unfortunate outcome is that GMG has increasingly been the target of cyberattacks. "GMG has been one of the most active brands in the Gulf region and that has put the business in the limelight," said Prabhat Kumar Prabhat, IT Director, Technology and Security for GMG. "As a result, we have seen a significant increase in cybersecurity incidents. One of the critical elements of our security management is ensuring customer and user data is safe so everyone feels confident."

GMG had been using legacy antivirus tools to protect its endpoints, but it soon became obvious the outdated technology was insufficient to protect against the increasingly sophisticated attack methods of the modern threat landscape. Prabhat and his team were no longer 100% sure they were capturing every incident. "Threats today are far more intelligent than they have been in the past," he said. "It is not just the good guys using technologies like artificial intelligence (AI); the bad guys are using them as well. When we did spot an incident, it was difficult and complicated to deal with because of the time and effort required to quarantine and clean the affected device."

"To stop these threats, we needed a solution with similar or better intelligence than the threats," Prabhat continued. "For instance, it had to be probability-based and use historical data analytics, as well as automated to stop threats before they could enter our environment."

INDUSTRY

Retail and manufacturing

LOCATION/HQ

Dubai, United Arab Emirates

CHALLENGES

- Protecting critical customer and user data
- Triaging up to 10,000 incidents a month with limited security skills on staff
- Replacing legacy antivirus tools and moving to a proactive MDR operational model

SOLUTION

Using CrowdStrike Falcon Complete™ managed detection and response (MDR), GMG transformed its global security operations, gaining modern endpoint security capabilities along with elite, proactive detection and response. As a result, GMG reduced incident remediations by more than 96% annually, increased user and SecOps productivity, and improved its risk profile — all while creating significant ROI.

"CrowdStrike is designed to protect our customers, staff and the business and that is what it has achieved. The value that delivers cannot be quantified."

Prabhat Kumar Prabhat
IT Director, Technology and Security
GMG

voices

CrowdStrike Customer Case Study

GMG Chooses CrowdStrike for 24/7 Managed Detection and Response

After evaluating several solutions, GMG selected CrowdStrike Falcon Complete MDR, which combines CrowdStrike's flagship endpoint security modules with highly skilled security analysts to monitor GMG's environment, configure and optimize systems, and conduct full-cycle detection and response every day, hour and minute of the year. Included with Falcon Complete is CrowdStrike Falcon OverWatch™, CrowdStrike's managed threat hunting service that proactively detects, disrupts and alerts GMG to advanced attacks operating in its environments.

"CrowdStrike does not just talk about delivering first class-security — the company and its portfolio deliver it," said Prabhat. "What we particularly like about CrowdStrike is the proactive, predictive and intelligent approach to detection and remediation that Falcon Complete MDR provides for us 24/7."

Deployment to 3,500 endpoints — comprising laptops, desktops, servers, on-premises and cloud systems, and retail point-of-sale devices — was managed jointly by GMG and CrowdStrike. The process was simple and required minimal involvement from GMG engineers. "The partnership with CrowdStrike and the support and service it provided to GMG has been fabulous," said Prabhat. "Any time we requested help from CrowdStrike, the response was instantaneous."

An important factor behind GMG choosing CrowdStrike was the single, lightweight CrowdStrike Falcon agent, which does not overload the endpoint or consume excessive amounts of processing power as GMG's previous antivirus product did. "In past endpoint security deployments at GMG, the security software put a significant and noticeable strain on our machines," said Prabhat. "They would slow down and decrease the performance of our laptops, workstations and servers, and in some cases even crash or corrupt systems right from the start. In contrast, CrowdStrike operates silently and seamlessly."

Prabhat said GMG plans to eventually extend its CrowdStrike deployment to an additional 1,500 endpoints.

GMG Confident in the Face of 10,000 Monthly Attacks

GMG faces upward of 10,000 malware and phishing attacks a month, a situation Prabhat said can be "very dangerous, unpredictable and scary." Yet he quickly noted that very few if any of those incidents have been able to break through their security defenses.

"While we have multi-layered security, a lot of credit for that success must go to CrowdStrike," Prabhat said. "Whether it is one or 10,000 attacks, the way CrowdStrike protects our customers, staff and data is amazing."

Security at GMG has changed significantly in other ways since Falcon Complete was deployed. Previously, the security team dealt with around five incidents per month, each requiring the compromised device to be shut down and reformatted, locking out the user in the process. This could take days and involve two or three skilled people. After deploying Falcon Complete, Prabhat saw his team's incident remediation drop dramatically — cutting machine recovery and reprovisioning to one or two incidents per year, a reduction of 96%. In addition, threat investigations are usually closed within 12 hours instead of 3-5 days, and user productivity is improved since users no longer need to wait for device repairs to get back to work.

RESULTS

Eliminated user system downtime

Improved productivity significantly

Created significant ROI for the business

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response (MDR)

voices

CrowdStrike Customer Case Study

For Prabhat, the contrast is stark when compared to not having CrowdStrike. "With CrowdStrike, when there is an incident, I rarely have to do anything," he said. "The process is seamless and resolves quickly and easily," said Prabhat. "CrowdStrike has taken a lot of pain away. The improvement we've seen after deploying CrowdStrike Falcon is huge."

Although deploying CrowdStrike was not intended to save money, it has had a huge indirect impact. "The data GMG is responsible for protecting is highly personal and sensitive," Prabhat said. "One data leak can create millions of dollars in loss of brand reputation, not to mention the actual cost of breach repair. CrowdStrike is designed to protect our customers, staff and the business, and that is what it has achieved. The value that delivers cannot be quantified."

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/