voices

CrowdStrike Customer Case Study

TUI GROUP

TUI Deploys CrowdStrike to Protect Unique Holiday Experiences for its Customers

Around the Canary Islands, North Africa or the Middle East you will find the Marella Explorer, the largest cruise ship in the TUI Group fleet. It has 10 restaurants, 13 decks and 962 cabins serving almost 2,000 passengers. Alongside its mission to deliver unique holiday experiences, TUI makes sure its customers and their data are safe and secure. So, at endpoints on board the ship — from passenger information and excursion booking computers to tills in shops and restaurants — sits a selection of CrowdStrike solutions ensuring that customer information is protected.

Being a leading global tourism group with some 60,000 employees, cruising is just one of the vast array of holiday experiences that the TUI Group offers. Besides its fleet of 16 cruise ships, the company's portfolio includes 400 hotels and resorts, tour operators with over 1,000 travel agencies and five airlines with 100 aircraft. Approximately 21 million customers choose a TUI holiday every year.

Every element of the vast volume of personal data associated with delivering a finely tailored holiday experience — including booking flights and hotels, transfers, excursions at destinations, financial transactions, passport documentation and more — must be vigorously protected.

Increasing Threat Intensity and Sophistication

Under the watchful eye of its CISO, Nick Jones, TUI has done a great job of mitigating the threat of cyberattacks. According to Jones, however, the challenge facing all organizations gets harder every day.

"In today's business environment, the intensity and sophistication of cyberattacks have increased significantly," he said. "Just look at the global Log4j issue. In just 10 days, there were two new versions exploiting multiple new vulnerabilities. It is an interesting case study of how attacks have become so much more complex and fast moving. The security community is talking about Log4j as the coronavirus of cybersecurity."

Constantly innovating, TUI launched a "mass individualization" strategy to give its customers a truly unique and rewarding holiday experience. It also is continually developing new products as well as expanding into new markets like river cruises or its pioneering idea of offering "work-cation holidays" during the COVID-19 pandemic where people could book a safe and secure hotel for a month.

Delivering these innovations dictated some fundamental changes to the company's IT infrastructure and a renewed look at cybersecurity. IT at TUI had traditionally been centered around having discrete

INDUSTRY
Travel

LOCATION/HQ
Hannover, Germany

CHALLENGES
- Increased risk of intense and sophisticated cyberattacks
- Support business strategy to digitize and deliver a unique holiday experience
- Existing endpoint security solutions no longer fit for purpose

SOLUTION
Global travel business, TUI Group, has deployed a range of CrowdStrike solutions to support and protect the company's digital, unified and cloud-based IT environment critical to delivering its unique holiday experience strategy

"CrowdStrike holds itself as being an industry leader in protecting today's enterprise, and I agree. The tagline of 'We stop breaches' is clear, focused and direct. This is exactly what businesses like TUI need and why we buy CrowdStrike solutions."

Nick Jones
CISO
TUI Group

voices

CrowdStrike Customer Case Study

systems in its main operating regions in Germany and the UK. However, this strategy was becoming inefficient and increasingly unable to cater to the dynamic needs of TUI's travelers.

"Everyone wants a unique holiday experience, but you need a secure infrastructure; something that makes the traveler feel special," said Jones. "Digitization makes it relatively easy for us to create differentiation such as additional checked luggage, a personal pick up or crafting their itinerary so it feels like their own unique holiday, not a packaged one."

TUI started to replace its siloed systems with a global IT platform for key applications such as bookings and managing hotel room inventory, as well as standardized business operations that could deliver a consistent experience in any region. By developing each application in house, TUI benefits from intellectual property (IP) ownership but most importantly retains full control over the capabilities and applying internal standards.

To meet the growing attack risk of transitioning applications to the cloud in the next few years, TUI set up a global security center with a team of 35 employees to provide centralized management and control. One of the taglines TUI has adopted is "Every engineer should be a security engineer."

TUI had a legacy endpoint security product in place, but it could not meet the requirements of the new cloud-based infrastructure. After an extensive review of multiple solutions, the company decided to partner with CrowdStrike, a decision that was rewarded immediately. "The CrowdStrike solution looked really good, had a wide variety of capabilities, and was rated very highly by independent analysts," said Jones.

"What impressed us most was how CrowdStrike got so deeply involved right from the start. The team was very proactive during the whole onboarding and learning process, and even opened its university to our staff. One thing that was less obvious but has proven to be a huge benefit is we were immediately able to use CrowdStrike Falcon Prevent™ to replace our legacy antivirus software that was coming up for renewal. That alone meant CrowdStrike has largely paid for itself from the outset."

Because CrowdStrike supports centralized management, it has been the catalyst for TUI establishing and controlling its entire organization's global security center.

CrowdStrike Targets over 50,000 Endpoints

TUI has deployed a suite of CrowdStrike solutions designed to protect customer data across over 50,000 endpoints worldwide, ranging from computers, servers and cloud domains at headquarters, to devices in its hotels and resorts, and even endpoints on its ships cruising at sea. Initially, TUI aimed to cover 80% of its endpoints, but due to the success of the project — especially driven by employees taking home their PCs during the global pandemic — this number has rapidly increased to over 90%.

The company's IT environment includes a diverse range of Microsoft, Linux and cloud workloads and environments, applications and operating systems and also integrations with external

RESULTS

Replaced existing antivirus products and services

Supported over 50,000 global endpoints, even on cruise ships

Underpinned single, centralized and global security operation

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Device Control™ for cloud-delivered device control
- Falcon Discover™ IT hygiene
- Falcon Insight™ endpoint detection and response (EDR)
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus (NGAV)
- Falcon Spotlight™ vulnerability management

systems including airline booking applications. At no point has the company's rapid approach to the CrowdStrike rollout resulted in any business disruption or device performance problems. Even deploying CrowdStrike on ship-based endpoints, where connectivity is limited and intermittent, was straightforward.

While the main purpose of CrowdStrike is to deliver protection, the solutions also have helped to improve visibility to enable TUI to identify assets and manage versioning and patching.

CrowdStrike is a Wonderful Partner
"Besides CrowdStrike being a wonderful partner, the solutions are a critical part of our security portfolio," said Jones.

"Without the scope of protection that CrowdStrike delivers, TUI would not be able to handle the sophisticated threats that businesses like ours face today."

CrowdStrike sits within a framework of other security products and services, enabling TUI to defend against potential attacks and repel threats automatically. If an attack is successful, CrowdStrike helps TUI to quickly isolate an individual server or endpoint so that the threat can be contained and prevented from running across the infrastructure. "The scale, level of control and risk mitigation that CrowdStrike delivers is a huge benefit to our business," said Jones.

"CrowdStrike gives us the time and space to deal with exceptions, whereas we previously had to deal with almost every attack individually," he continued. "The automation capabilities of CrowdStrike are a massive time saver for TUI, and help us to deliver elevated levels of protection with lower demands on resources. CrowdStrike holds itself as being an industry leader in protecting today's enterprise, and I agree. The tagline of 'We stop breaches' is clear, focused and direct. This is exactly what businesses like TUI need and why we buy CrowdStrike solutions."

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (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.

CrowdStrike: **We stop breaches.**