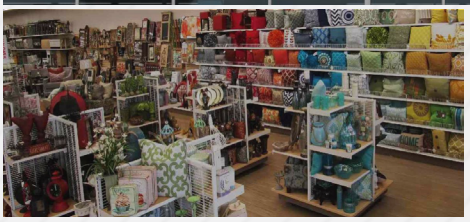
voices

CrowdStrike Customer Case Study



Tuesday Morning

National U.S. Retailer, Tuesday Morning, Set to Save $750,000 in Four Years with CrowdStrike Falcon

While onstage presenting to the entire Tuesday Morning Corporation IT team, from administrative staff to the CIO, Tom Sipes, director of IT security and compliance, glanced at an adjacent screen and watched in awe as CrowdStrike Falcon® spotted and stopped a security attack in real time. It was the first such detection since the retail giant had deployed the Falcon platform and typified how the solution has transformed the way the business manages and mitigates the risk of cyberattack.

About Tuesday Morning

Tuesday Morning is a national retail chain established in 1974 that specializes in selling high-quality and designer-brand closeouts at discounts between 20% and 60%. There are 490 stores across the U.S. selling a range of luxury home textiles, home furnishings, housewares and seasonal décor. Five thousand employees staff Tuesday Morning's stores, while 350 work at the head office and distribution centers.

Like many businesses, Tuesday Morning is subjected to frequent threats such as ransomware, phishing and malicious attacks. With thousands of people visiting stores every day and thousands of endpoints, the company's threat surface is particularly broad. However, Sipes' main focus is on business continuity. "In retail, the mantra we live by is, 'make sure the dollar goes into the register,' otherwise we are not making money," he explained. "Sometimes, security is seen as a detractor to that aim. It is not that I am trying to shut the door, rather I am opening the window so the business can function without letting the bad guys in."

Response Slowed by "Cobbled-together" Legacy Security Tools

Sipes inherited a legacy security platform at Tuesday Morning. "Our security posture was not bad, it was just that a lot of stuff was cobbled together because of spending limitations and challenges like the pandemic," he said.

The retailer's existing managed detection and response provider was slow and often left Sipes and his team on their own to chase relevant information. Sometimes it could take 72 hours to get a reply. "Even 24 hours in the life of an incident is forever," Sipes said.

With Sipes and several new senior IT executives in place, things began to change. The company's new CIO stood up in front of 125 senior staff to emphasize the importance of security and launch

INDUSTRY

Retail

LOCATION/HQ

Dallas, Texas

CHALLENGES

- How to improve security without restricting business operations
- Broad attack surface with point-of-sale (PoS) devices in 490 retail stores across the U.S.
- Old and inefficient legacy security infrastructure
- Poor and slow response from an external service provider

SOLUTION

Tuesday Morning, a leading U.S. retailer, uses CrowdStrike to transform security management while reducing costs, improving productivity and ensuring business continuity so that there is no impediment to "getting the dollar into the register."

"CrowdStrike is an outstanding security platform that has raised our security posture. While I work for Tuesday Morning, I am also a customer. When I walk into a store and hand over my credit card, I know it is safe."

Tom Sipes
Director IT Security and Compliance
Tuesday Morning Corporation

voices

CrowdStrike Customer Case Study

an initiative to find a new solution. They looked at several competitive products as well as the incumbent solution.

For Sipes, one of the main reasons for choosing CrowdStrike was to ease the burden of handling security manually. "Our security team is small, just two others and me," he said. "The solution we needed had to be manageable, functionable and something that I could leave to operate automatically and still have the confidence that everything would be protected. That is what CrowdStrike promised and has certainly delivered."

CrowdStrike Deployed to 2,800 Endpoints Across 490 Stores — in a Month

Tuesday Morning decided to become a CrowdStrike customer in late September 2021, and by mid-October, the solution was fully deployed across the business. Tuesday Morning has an on-premises IT environment running Microsoft systems from two data centers. The company has 2,800 endpoints — comprising desktops, laptops and servers at the head office and point-of-sale registers in stores — that are now protected by CrowdStrike Falcon. Even the control systems and switches for the in-store card readers are protected by Falcon.

CrowdStrike was deployed to corporate users in just three days, while the store rollout was done in stages to minimize any effect on sales. After a few stores were completed with no issues reported, full deployment was quickly accomplished. Now when a new endpoint is set up, like a register in a new store, CrowdStrike recognizes the device and deploys the Falcon agent within 20 minutes.

Tuesday Morning uses a wide range of CrowdStrike products and solutions, including the Falcon OverWatch™ threat hunting service. The company was one of the first organizations to deploy Falcon FileVantage™ — CrowdStrike's file integrity monitoring module that provides real-time, comprehensive visibility for the creation, deletion and modification of all critical assets, and which Tuesday Morning used to resolve a SOC remediation issue in eight hours with minimal cost or interruption to operations.

One of the standout features of CrowdStrike is using an industry-wide approach to detection and remediation.

"Before, we were relying on legacy heuristic scanning tools that usually catch things after the fact," Sipes said. "Now I am getting machine learning that is not just reliant on something unique to my environment. Rather, it is pulling in experience from the entire CrowdStrike ecosystem to deliver far more robust protection."

CrowdStrike Transformed Security Management

For Tuesday Morning, this approach and the comprehensive CrowdStrike Falcon platform transformed its approach to security. "In security, we're always reacting to an event," Sipes explained. "What CrowdStrike does is what I call 'proactive reactive.' We can now get very close to the time of the attack so that we are almost executing the kill chain as soon as the event happens."

CrowdStrike has transformed the way Tuesday Morning manages security, from reducing costs and workload to increasing visibility, streamlining operations and improving protection.

RESULTS

Saves $250,000 USD in the first year and $500,000 USD over the next three

Resolves incidents in as fast as eight minutes

Protects thousands of PoS terminals in hundreds of stores

ENDPOINTS

CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response (MDR)
- Falcon Discover™ IT hygiene
- Falcon FileVantage™ file integrity monitoring (FIM)
- Falcon Firewall Management™
- Falcon Insight™ endpoint detection and response
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus
- Falcon Spotlight™ vulnerability management
- Falcon Intelligence automated threat intelligence
- Humio log aggregation, storage and analysis
- Falcon Identity Protection

voices

CrowdStrike Customer Case Study

Tuesday Morning did a cost/benefit analysis on CrowdStrike, and with no staff changes, the company forecasts that CrowdStrike willsave the business $250,000 in the first year and $500,000 over the next three years based on efficiencies.

Alongside cost savings, CrowdStrike is delivering significant security and operational improvements. Sipes cited one example where CrowdStrike Falcon detected an incident and eliminated it in eight minutes. An engineer was upgrading some software and inadvertently downloaded information that contained malicious code. Within two seconds, Falcon detected the code, and within eight minutes it had stopped the incident. "The only thing the developer knew was the installation stopped for about 10 seconds while the malicious code was removed," Sipes said.

Critically, neither Sipes nor his security staff needed to intervene. "I was sitting at home in the morning drinking a coffee and noticed an email alert," Sipes said. "I pulled up the dashboard and watched the entire kill chain as CrowdStrike dealt with the incident automatically."

This example highlights how CrowdStrike has taken over the burden of mundane security. "I have been in the cybersecurity business for a long time and seen all sorts of breaches, but with CrowdStrike we do not see many indicators of compromise," Sipes said. "I see potential attacks, but CrowdStrike stops them. Whether it is the OverWatch team or an identity alert — having used Falcon Identity Protection to extend our existing multifactor authentication (MFA) to legacy on-premises apps to help stop lateral movements — attacks are being contained and I do not need to take action."

Falcon Identity Protection not only integrated seamlessly with Tuesday Morning's existing MFA solution, but also extended this MFA to protect legacy on-premises applications that were developed internally. This was achievable without requiring any additional configurations or customizations to these existing legacy applications — enabling protection with risk-based MFA tied to the appropriate security policy.

Users across the business also are seeing minimal disruption.

"The biggest comfort that CrowdStrike delivers is to give my users the ability to do their job safely, with virtually no impact at all."

With a small team, Sipes oversees the cybersecurity of 5,000 staff, and with CrowdStrike falcon, is now able to do a lot more. "One of the biggest benefits of CrowdStrike is taking away the need to look at consoles, search for malicious code or analyze incidents," he said. "Instead, CrowdStrike enables us to focus on more important work and taking the business to the next level. CrowdStrike gives us a great work/life balance and, in terms of improved productivity and adding value to the business, the difference is night and day."

"CrowdStrike is an outstanding security platform that has raised our security posture," Sipes said. "While I work for Tuesday Morning, I am also a customer. When I walk into a store and hand over my credit card, I know it is safe."

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.**