CROWDSTRIKE CASE STUDY

TRANSPAK

WANTED:
CUTTING-EDGE PROTECTION AGAINST RANSOMWARE AND OTHER ADVANCED THREATS FOR A WIDELY DISTRIBUTED ORGANIZATION

Mark Sauer is director of information technology at TransPak, where he is tasked with improving security across its global locations. With an IT background that includes 20 years as an officer in the U.S. Navy, Sauer brings a wealth of experience and knowledge to his position. As he explained, "When I came on board, the company was in a period of rapid expansion. What I found is that processes and procedures — and in some cases the technology — needed to grow in order to meet customers' demands and the company's demands for system availability and performance. One of the pain points was information security — being able to protect our systems and our ability to do our work."

In addition to increasing available bandwidth at TransPak so processes could function properly, Sauer assessed its security systems and found an abundance of malware and unwanted programs that were eroding performance. However, he felt the biggest threat was ransomware, which he first encountered in September of 2016. "We were attacked and the ransomware started to traverse through our organization, getting to our file servers and then our terminal servers — running over the course of about five or six hours before it was detected." He said they were manually tracking the attack back to the infected workstation, which took them hours to locate. "Meanwhile, the ransomware was running rampant and encrypting files as it found them," he said. "Depending on how much the ransomware has gotten to, it can take up to 48 hours to get backups restored. Meanwhile, we have employees sitting idle, waiting for systems to be restored."

Quick Facts:

BUSINESS OVERVIEW

TransPak is a crating, packaging, logistics and design company founded in 1952 in Silicon Valley during the nascent era of what is now the world's largest and most well-known technology center. The company's purpose was to provide customized crating and packaging to ensure that sensitive products and equipment produced or used by Silicon Valley manufacturers would arrive in perfect condition and on time at destinations worldwide. As a private, family-owned business, TransPak has grown into a global provider with over two dozen locations throughout North America, Europe and Asia, 1,500 employees and facilities of over 1.5 million square feet.

MISSION

"TransPak forms partnerships with its clients that are built on trust, dependability and collaboration. Depend on TransPak for consistent, reliable service every hour of every day on a global scale. TransPak gets practically anything to anywhere, fast."

Website: www.transpak.com

The Story:

CHALLENGE

TransPak was experiencing a period of rapid expansion. Having developed a strong U.S. presence, it was focused on quickly growing its market in Asia, and though Europe was an emerging market, the company had ambitious plans for growth there as well. Supporting more than two dozen global locations and ensuring the availability of systems and software was an increasing challenge for the IT team, and many TransPak employees were frustrated that systems were not performing at peak efficiency and as a result productivity was suffering. As a result, productivity was suffering. In addition, the company had been the target of numerous ransomware attacks that had required extensive backups to restore files, causing more interruptions and further productivity losses.

NEXT-GENERATION ENDPOINT PROTECTION
Cloud-Native Architecture Enabled Ease of Deployment with Zero Impact on Endpoints

Sauer decided it was time to find new security technology that could help TransPak avoid attacks that interfered with its day-to-day business operations. After evaluating a few competing solutions, TransPak chose the CrowdStrike® Falcon® platform. "From the second we deployed the CrowdStrike Falcon agent, we were protected and I had control and the ability to deal with malware and security incidents at the touch of a button," Sauer said. "Before, it took me hours to even detect an incident and then once I did, I would have to do research to find it and it was a very manual process. With the CrowdStrike Falcon agent that all goes away — it just melts away instantaneously when you deploy."

Sauer was particularly impressed with how easy the Falcon platform is to manage, even when he is offsite. On one occasion, he was attending his child's basketball game when his phone buzzed with an email indicating a high-severity alert from the Falcon agent. "I logged into the Falcon console from my phone and saw there was some malicious activity going on." he said. "It identified the computer, the location and the user that was logged into it, right there on my phone at a basketball game! I merely touched the contain button and my problem went away," he said. A similar incident prior to having the Falcon agent in place would have taken hours to handle, Sauer explained, forcing him to miss the game, log into the network and begin a protracted manual process of locating and remediating the problem. With the Falcon platform, he could easily handle the situation from his phone.

A common headache many IT professionals encounter when introducing new solutions companywide is disrupting users and generating a flood of help desk calls. This was another problem that the Falcon platform helped TransPak avoid. As Sauer told it, "I had zero support tickets, zero complaints and zero issues when we deployed the Falcon agent. It didn't affect anything that we were doing and we were able to continue our business operations completely unaffected by the deployment."

UNRIVALED TIME-TO-VALUE
The CrowdStrike Platform is a "Game-Changer"

Because TransPak runs a very lean IT team — only four help desk technicians supporting over two dozen sites — Sauer recognizes the platform's exceptional time-to-value. "With the CrowdStrike Falcon platform, we've turned the game from responding to incidents that consume nearly all our time and doing very little to advance the interests and the systems that support our company, to being able to spend a lot more time focusing on delivering customer service systems, new processes and capabilities so we can be more productive and get our business done more efficiently," he said. "That's the game-changer that the CrowdStrike Falcon platform brings."

TASK

TransPak wanted to fortify its widely distributed infrastructure with next-generation protection that could ensure the security and availability of systems, allowing employees to perform their jobs more efficiently. It also sought to avoid ransomware attacks that had plagued the company and interfered with productivity. Finally, it needed a solution that wouldn't burden its busy IT team with complex deployment and management tasks.

WHY TRANSPAK CHOSE CROWDSTRIKE

Although TransPak was succeeding and growing rapidly in U.S. and international markets, it needed to do more to ensure the security and availability of its network resources. The ransomware attacks had been particularly damaging in an industry that relies on client loyalty and the ability to perform at the highest levels of efficiency and response.

After evaluating several security solutions, TransPak chose the CrowdStrike Falcon® platform. Not only was the Falcon platform easily deployed without impacting users, the IT team saw immediate results as the lightweight Falcon agent instantly detected issues across the company's widely dispersed endpoints. The comprehensive visibility and power of the Falcon platform to deliver the complete context of threats enabled the TransPak IT team to pinpoint issues that had troubled them for months and to instantly mitigate vulnerabilities, while purging the network of dangerous malware and unwanted software. The streamlined deployment and minimal management requirements of the Falcon platform helped conserve valuable IT resources, allowing the IT team to focus on other areas critical to ensuring an efficient and productive workforce.

PROTECTION AGAINST ADVANCED THREATS
CrowdStrike Replaced TransPak's Legacy Antivirus

Sauer found that with the Falcon platform's next-generation AV solution he could easily replace the legacy AV TransPak was using. "The Falcon platform allowed us to eliminate an AV software package that was not effective," he said. " It was signature-based and detecting known malware, which we needed it to do, but quite frankly, most of the malware we found and the security incidents we had didn't have signatures. We needed to be able to move to a more behavioral-based security system that could detect the threats that don't have signatures. So, our AV is gone. We're not using it anymore. We are now using the CrowdStrike Falcon platform alone as our security system — our AV and our endpoint protection — across the board. It's a single solution that meets our needs for securing and protecting our IT infrastructure."

PROACTIVE MANAGED THREAT HUNTING
CrowdStrike Falcon OverWatch Augments TransPak's Security Team

TransPak also added CrowdStrike Falcon OverWatch™ managed hunting service, which provides a team of security experts to proactively hunt, investigate and advise on threat activity in a customer's environment, effectively working as an extension of its IT team. He related an incident in which the Falcon OverWatch team had identified a bad actor attempting to sell access to one of the company's servers — a potentially very serious breach. As Sauer explained, "Falcon OverWatch contacted me to tell me that they had detected activity associated with a known server-hijacking organization. We sent Falcon OverWatch some screenshots and they very quickly responded and said, 'Here's the information we have on this attempt.' Its actions prevented us from having one of our servers sold on the black market for spammers or other bad actors to use."

When asked to sum up TransPak's security posture since adding the CrowdStrike Falcon platform to his cybersecurity arsenal, Sauer had this to say: "The tools that the CrowdStrike Falcon platform provides give me the ability to sustain our business processes, to keep the systems running so that the business can continue to operate. I wish I had more tools that were as easy to deploy, maintain and manage as the CrowdStrike Falcon platform. It increases the value of my security program at TransPak to be able to deliver systems that work for the company and keep us free of malicious activity."

About CrowdStrike

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. CrowdStrike Falcon protects customers against all cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator-of-attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates over 70 billion security events from across the globe to immediately prevent and detect threats.

To learn more about how CrowdStrike can help protect your organization, contact us today at sales@crowdstrike.com or visit www.crowdstrike.com/seedemo to request a demo.

CROWDSTRIKE

sales@crowdstrike.com | (888) 512-8906
www.crowdstrike.com