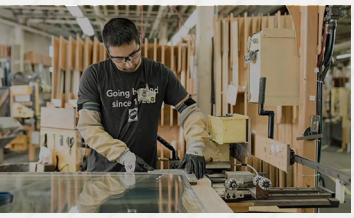
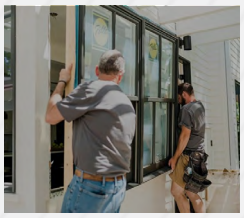
voices

CrowdStrike Customer Case Study





Pella Augments In-House Security Team with CrowdStrike Managed Services and Identity Protection

John Baldwin heads up the enterprise security team at Pella Corporation, a leading U.S. window and door manufacturer where he is Senior IT Manager, Cybersecurity. Baldwin and his team provide protection around the clock by delivering a highly effective CrowdStrike endpoint security defense for over 10,000 people, 18 manufacturing locations and numerous showrooms.

"As a veteran security professional, I hesitate to say I am not worried," said Baldwin. "But since deploying CrowdStrike, the quality of my sleep is much better."

Legacy Systems Insufficient to Protect Manufacturing and Other Systems

Pella, founded in 1925, markets its windows and doors to consumers as well as builders, running a just-in-time, made-to-order manufacturing operation with a lean and cost-effective way of producing goods. As a nearly 100-year-old legacy company, managing cybersecurity risks is a high priority for Pella.

"The building materials industry is now very busy following COVID-19 disruption and there is a lot of pent-up demand, so we are very mindful of anything disrupting our production flow," said Baldwin.

The company maintains an on-premises environment primarily to support its heavy-duty Oracle Enterprise Resource Planning (ERP) and manufacturing systems that are running Linux and Windows, and has been looking at shifting some services and applications to the cloud. In terms of cybersecurity, Pella's problem was that it did not have an effective endpoint protection solution. Instead, it had segmented antivirus tools that took too much time to manage, and any time changes were made in the IT environment, the tools required revisiting by Baldwin's team to see if they were still effective — a process that took valuable time and effort. Further, a lack of incident visibility meant the Pella security team was constantly chasing every incident in case it was serious. And with threats increasing both in number and in complexity, the existing solutions were no longer providing the required defense.

Baldwin explained that the threat level for manufacturing has changed from opportunistic ransomware attacks to attacks from organized criminals targeting time-sensitive businesses like Pella. "It is not a matter of if they come, but when and what we can do about it," he said. "Otherwise, we could suffer a systems outage for several days, which would disrupt production and be very costly, not to mention the delays impacting our customers and business partners."

Pella®

INDUSTRY
Manufacturing

LOCATION/HQ
Pella, Iowa

CHALLENGES
- Security staff lacked sufficient time and skills
- Evolving threat landscape
- Siloed, ad-hoc antivirus tools were no longer sufficient

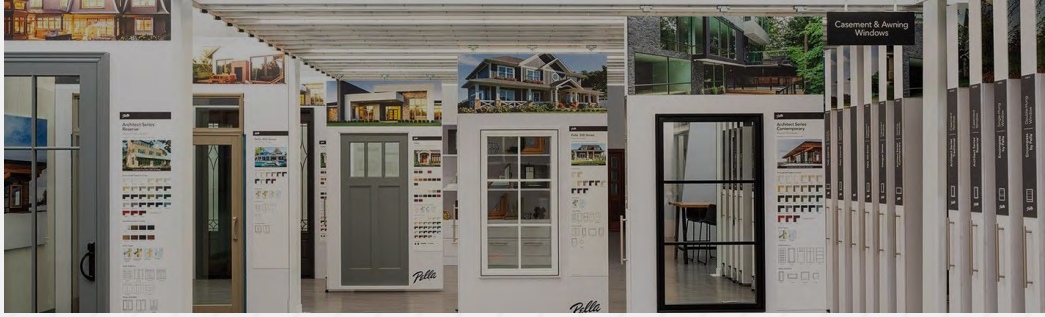
SOLUTION
Pella chose CrowdStrike to improve its security operations and supplement its busy in-house security team with world-class managed detection and response (MDR) and identity threat protection to fortify endpoint protection, drastically minimize the risk of identity-based attacks, and detect and respond to advanced adversaries that may target the organization.

"The visibility we get from CrowdStrike, knowing what is happening and getting ahead of the curve, has been a game changer for Pella."

John Baldwin
Senior IT Manager, Cybersecurity
Pella Corporation

voices

CrowdStrike Customer Case Study



Pella Deploys CrowdStrike Managed Services and Identity Protection Solutions

In seeking a replacement for its legacy systems, Pella spoke with analysts from independent third-party organizations, which confirmed what the company had discovered about the validity and effectiveness of CrowdStrike.

"The value for the money that CrowdStrike offered was hard to challenge. Pella is a growing business and we saw that investing in CrowdStrike would help us improve security in an expanding and more complex environment. Also, we found that CrowdStrike managed services have a level of maturity nobody else could match."

Pella has deployed a range of CrowdStrike products and services — including CrowdStrike Falcon Complete™ managed detection and response (MDR) and CrowdStrike Falcon Identity Threat Protection — to protect 5,200 endpoints and 800 servers.

"I was pleasantly surprised by how easy it was to deploy CrowdStrike in our environment," said Baldwin. "The CrowdStrike Services team was great about onboarding and gave us some very good templates to follow for incident response playbooks."

Falcon Identity Threat Protection Helps Defend Against Lateral Attacks

Pella followed up the initial deployment with Falcon Identity Threat Protection. Pella carried out a red team/blue team exercise that highlighted a few gaps in a particular lateral movement. "The CrowdStrike Falcon Identity Threat Protection solution has been fantastic and highly valuable," said Baldwin. "We are very happy with the way it provides visibility and helps with baseline anomaly detection. Given that a lot of threats are identity-driven, you need to watch what your credentials are doing. CrowdStrike does not get enough recognition for its remarkable identity threat protection solution."

Pella ran a table-top exercise with CrowdStrike where the Oracle ERP system was disrupted by a simulated cyberattack to assess impact and rehearse how to respond to a similar attack. "This is precisely the sort of thing we are using CrowdStrike to protect against," said Baldwin. "There is a lot of complexity, as well as interconnections and dependencies in our business, and the idea is to get ahead of an attack as much as possible."

CrowdStrike products and services have come into Pella to raise security to a level of sophistication and effectiveness that the business could not have otherwise achieved in-house without significant investment in people and resources. "We would have had to hire, train and retain six full time employees to achieve the level of SOC we achieve with the CrowdStrike solution," explained Baldwin.

CrowdStrike Is a Force Multiplier for Pella's Security Team

"One of the key benefits of CrowdStrike is constant vigilance," said Baldwin. "Falcon Complete has been a great force multiplier for my team. Once we got the playbooks set up, we have had very good and surprisingly painless success with the solution. CrowdStrike is the first time we have used a third-party, managed security service. We went from wondering if something is happening to CrowdStrike proactively alerting us to issues and recommending next steps. That has been great and frankly a better job than we could do in-house."

RESULTS

Decreased stale and over-privileged accounts by 75%, drastically reducing the attack surface

Reduced incident resolution from days to 30 minutes

Removed need to hire six full time employees to run 24/7 SOC

ENDPOINTS

5,200

CROWDSTRIKE PRODUCTS

- Falcon Complete™ managed detection and response (MDR)
- Falcon Discover™ IT hygiene
- Falcon Insight XDR™ endpoint detection and response (EDR)
- Falcon OverWatch™ managed threat hunting
- Falcon Prevent™ next-generation antivirus
- Falcon Identity Threat Protection
- Falcon Spotlight™ vulnerability management
- Falcon Intelligence™ automated threat intelligence

voices

CrowdStrike Customer Case Study

With CrowdStrike, time to resolution has dropped from hours or days to an average of 30 minutes. Business staff are disrupted far less often because the need to shut down and re-image a user's PC has been reduced. "When you have salespeople on the road who seldom come into the office, getting hold of their laptops is extremely disruptive," said Baldwin.

"The beauty of CrowdStrike is that incidents are detected quickly and do not progress beyond the initial detection phase, so the resolution is simple and non-invasive."

CrowdStrike also brings clarity to managing endpoint security. "The visibility that CrowdStrike enables has been a key differentiator for Pella," said Baldwin. "We were being constantly pinged by our old systems and it was hard to see what was important and what was not, so we always had to react. Now we can ignore most of the incidents because CrowdStrike has it covered. This means the security team can focus on high-value projects and develop a Zero Trust security architecture. The change is moving from firefighting to fire marshal where we are looking for things that could go wrong."

One of the standout capabilities of the CrowdStrike solution is identity threat protection, which offers improved multifactor authentication (MFA) through seamless integration with MFA providers such as Okta. The capability has given Pella a holistic view of elevated privileges in its complex environment, enabling the company to reduce unnecessary and legacy privileges by 75%. "The visibility that identity brings reduces the attack surface and helps Pella defend against identity-based attacks," said Baldwin. "The difference is night and day."

Pella has found other CrowdStrike managed services such as Falcon OverWatch highly valuable. With a security team focused on running projects, the company is enhancing security by adding the resources and skills that a trusted partner like CrowdStrike can provide. "Now I cannot imagine going forward without the support and insight that CrowdStrike provides to our business," said Baldwin.

Pella prides itself on the quality and service it delivers to customers, and with CrowdStrike as one of the company's top two security solutions, Pella is delivering the same quality of service to endpoint protection. "The visibility we get from CrowdStrike, knowing what is happening and getting ahead of the curve, has been a game changer for Pella," said Baldwin.

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/