OVERVIEW

Founded in 1889, Carhartt, Inc., is a U.S.-based manufacturer that is world-famous for the quality and durability of the work clothes it produces. A family-owned company for over 120 years, Carhartt originally produced clothing primarily for railroad workers. Over time, the company’s clothing items evolved to further extend durability by including the use of high-tech materials resistant to flames, abrasion, and water. Today, Carhartt manufacturers a variety of clothing commonly found on construction sites, farms, and ranches. Carhartt’s apparel is carried by major chains, such as Bass Pro Shops and Cabela’s and international retailers in North America, Europe, Japan, and Australia.

CHALLENGES

Recognizing that the manufacturing industry is a significant target for cyberthreats, Carhartt felt it lacked the security strategy and tools to protect its IT environment, data, and endpoints. In mid-2016, Carhartt hired Tim Masey as Director of Cybersecurity, and tasked him with improving security and compliance for Carhartt’s business. “When I came on board, I recognized that we needed to consolidate security controls and create a framework that would allow us to become a risk-adverse organization,” explain Masey. One of Masey’s initial concerns was the company’s reliance on less than effective IT security tools. “We had very little interaction with our prior vendor and we were disillusioned with their security products,” said Masey. “We were eager for a better solution with visibility into security events and improved manageability.”

In addition to state-of-the-art connected threat protection, Carhartt was interested in improved compliance capabilities. Carhartt is growing its ecommerce and retail businesses, so compliance with the Payment Card Industry Data Security Standard (PCI DSS), particularly with key capabilities like file integrity monitoring, was essential. Carhartt also conducts business in Europe, so compliance with the European Union’s General Data Protection Regulation (GDPR) was critical.
WHY TREND MICRO

Carhartt was first introduced to Trend Micro through technology partner, CDW. Cybersecurity implementation partner, Optiv, helped Carhartt understand the quality of Trend Micro solutions for both on-premises and cloud environments. Combined with the layering of connected threat defense, both on-premises and cloud environments can be monitored on a single-pane, in one central system.

After a thorough review process of both traditional security players and single-solution companies, Carhartt chose Trend Micro. They felt its state-of-the-art solutions were the most thorough and reliable for their needs. Carhartt’s final decision was reinforced by the recognition of Trend Micro in the Gartner Magic Quadrant for Endpoint Protection Platforms (EPP). “We needed more than a point solution. Trend Micro’s industry model and the fact that they’ve been a leader in this space for a long time, and in business for almost 30 years was very important to us,” said Masey.

SOLUTIONS

Carhartt implemented Trend Micro™ Smart Protection for Endpoints, to reduce the number of threats coming into its environment through various endpoints. “Malware protection, integrity monitoring, and the ability to have intrusion protection and detection are critical for us,” explained Masey.

Carhartt uses Trend Micro™ OfficeScan™ XG software to improve security for the company’s 5,600 users. Trend Micro™ Cloud App Security solution, with data loss prevention (DLP), is supplementing the protection of Microsoft® Office 365® products, improving cloud threat detection, and adding sandbox malware analysis and DLP policies, which help with PCI DSS and GDPR compliance. Trend Micro™ Deep Security™ platform allows Carhartt to develop extensive policies for intrusion protection (IPS) and leverage built-in integrity monitoring to protect their entire VMware virtual server environment.

To improve visibility through centralized monitoring and alerting, for devices across the company, Carhartt uses Trend Micro Control Manager™ solution. Control Manager solution centralizes visibility and produces reports that document how they are meeting compliance and regulatory requirements. It is also integrated with Carhartt’s security information and event management (SIEM) tool for 24/7 monitoring.

RESULTS

“We've reduced IT risk throughout the organization and we are ensuring the confidentiality, integrity, and availability of our data is consistent and rolled out on a programmatic basis.”

Tim Masey, Director of Cybersecurity, Carhartt

“We've reduced IT risk throughout the organization and we are ensuring the confidentiality, integrity, and availability of our data is consistent and rolled out on a programmatic basis.”

Tim Masey, Director of Cybersecurity, Carhartt

WHAT’S NEXT?

Now that Carhartt’s IT security is on track, the company is considering adding Trend Micro™ Deep Discovery™ Analyzer to help them avoid zero-day threats. “Manufacturers are a target for cyberattacks, so it’s important to develop a solid security framework with proactive capabilities,” said Masey. “We are also looking at IoT-enabled technologies to help with our supply chain and manufacturing floor processes. It takes much more than a single point solution vendor to protect all of that. That’s where Trend fits in.”

MORE INFORMATION

For more information, please go to www.trendmicro.com