Securing a dynamic business environment

Cintas helps customers get "ready for the workday" with workwear rental programs, facility services, essential first aid, safety, fire protection, and compliance products and services.

CINTAS READY FOR THE WORKDAY

Industry:
Professional Services

Location:
Cincinnati, Ohio

Organization:
43,000 employees

Solution:
Cisco ISE
Cisco Secure Client
Cisco Secure Firewall
Cisco Umbrella
Cisco SD-WAN
Cisco SecureX

Evolving security for a dynamic business environment

Headquartered in Cincinnati, Ohio, Cintas serves more than 1 million businesses in several industries across North America with innovative solutions and routine service visits. Cintas has a unique entrepreneurial business model—with almost 500 locations and over 14,000 delivery vehicles on the road—that creates a highly distributed security environment.

Cintas helps its customers get "ready for the workday" by offering products and services, including uniforms, floor care, restroom supplies, first aid and safety products, fire extinguishers, and testing and safety compliance training. "There should always be a balance between too many security controls and restrictions versus too little security vigilance," remarks Jacob Lorz, vice president and chief information security officer at Cintas. Lorz leads Cintas' security program by aligning security initiatives around business goals.

In evolving the security program, Lorz strives to keep the security strategy, goals, and objectives simple and aligned with industry standards. "For example, we align with the National Institute of Standards and Technology (NIST) cybersecurity framework and follow the Center for Internet Security (CIS) 18 Critical Security Controls. We measure ourselves against those industry standards and others, including the MITRE [Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)] framework," Lorz adds.

Cintas' mobile fleets with onboard equipment and personnel present unique security challenges. Lorz explains, "While servicing our customers, we must protect the onboard technology and data that rides along with our service trucks."

"Our service personnel carry personal route computers (PRCs) that store customer data. As an organization, we must protect not only the intellectual property associated with the data, but also its confidentiality. The risks to our data compound over time with different threats," Lorz adds. Cintas needs visibility into its network traffic with the many third-party technologies used at its sites. "Besides provisioning our systems, workstations, or servers, we have a lot of vendor technology at our sites and distribution centers at our plant facilities. We need visibility on the traffic," comments Lorz.

"We are pleased with how well the Cisco security solutions match our security needs. Cisco security solutions have reduced our cyber risk and improved our security posture. Pulling a holistic solution from the Cisco security portfolio helped reduce the burden on our staff and solution stack."

– Jacob Lorz, Vice President and Chief Information Security Officer

Lorz's team invests in security solutions that can reduce cyber risk to information systems at an enterprise level without getting locked to a particular domain or vendor. Lorz comments, "Many companies try to bring together best-of-breed security solutions. This can lead to deploying different solutions that might work well in silos but do not interoperate with other vendor solutions."

Cintas trusted Cisco security solutions to protect its data and infrastructure at multiple layers, and the solutions easily integrate and interoperate with Cisco and non-Cisco vendor solutions. Lorz said that the interoperability capabilities of Cisco security allowed Cintas to "not only maintain our existing investment with Cisco but also enhance our deployments by leveraging additional Cisco security capabilities."

Implementing integrated and layered security

With the Cisco security portfolio, Cintas achieved visibility and the ability to block threats at multiple levels.

Cintas implemented Cisco Umbrella cloud-delivered security to protect its systems from any outbound requests to malicious destinations. "Our investment in Cisco Umbrella began with our interest in its Secure Web Gateway proxy component," Lorz remarks. "Umbrella helps to block connections to malicious or suspicious sites before the connection is fully created or even initially established."

Implementing Umbrella's secure web gateway (SWG) proxy and security functions at the Domain Name System (DNS) layer allows Cintas to protect its resources from malicious websites while giving greater visibility to the security team. "We wanted the ability to block threats at multiple layers, and Umbrella helped with that," Lorz continues. "Umbrella is part of our layered security approach since it works with any port or protocol and complements our deployment of Cisco Secure Firewall technology."

Umbrella's cloud access security broker (CASB) functionality also helps Cintas uncover and identify cloud SaaS applications provisioned outside of IT control. "Umbrella allows us to monitor these applications, identify the risky ones based on a risk score, and then block access to the applications that present a security risk to our organization," says Lorz.

Lorz explains that as Cintas transitions from using air-gapped legacy vehicles to internet-connected vehicles, "We're using Umbrella to inspect the traffic from the mobile vehicle and Cisco AnyConnect to secure the connectivity."

Cintas deployed Cisco Secure Firewall strategically on-premises and in the cloud as part of a layered defense-in-depth approach. "In addition to providing traffic visibility and flow insight, Cisco Secure Firewall provides us a platform-based approach to segment various zones of trust, apply inspection policies across the organization, and proactively block intrusion attempts while providing context about the potential attackers," Lorz observes.

Cintas previously used Cisco Adaptive Security Appliance (ASA) Software for perimeter defense. The company eventually refreshed, migrating to Cisco Secure Firewall Threat Defense (FTD). Migration to Cisco Secure Firewall allows Cintas to run intrusion prevention with limited to no throughput impact. It also provides the ability to receive threat context and insight, along with always-on update capabilities to protect against a fluid threat landscape and zero-day exploits while simplifying integration with Cisco Identity Services Engine (ISE) and other Cisco Secure capabilities.

Lorz adds, "The key benefits for migrating to the newer next-generation firewalls has been the ability to run our systems with limited throughput impact and receive the context of threats. FTD and [Cisco Secure] Firewall Management Center provide a single-pane-of-glass view. We no longer need to manage devices individually."

Additionally, migration to Cisco Secure Firewall offered deeper insights and always-on, automated update capabilities to defend against Cintas' dynamic threat landscape.

Cintas deployed ISE in its network access control (NAC) center. ISE integrates with third-party tools to enforce device posture policies that protect the corporate VPN and wireless infrastructure and allow only valid, healthy, and secure systems to connect to the Cintas environment. In its daily operations, ISE helps Cintas identify, authenticate, and authorize the PRCs used by service sales representatives in the delivery vehicles.

"With tens of thousands of PRCs on the road every day, we need to have confidence that these PRCs are legitimate Cintas assets authorized to access the Cintas environment," Lorz explains. "Our network and security engineers appreciate the flexibility that ISE offers regarding connection types and control of endpoints."

Cisco Talos threat intelligence is integral to Cintas' larger threat-hunting practice. "Cisco Talos helps us understand malicious actors and advanced persistent threat (APT) groups attempting to gain access to our environment," Lorz remarks. Cintas uses Cisco Talos Incident Response (CTIR) to review incidents and receive guidance on how to improve and enhance its incident response plans and playbooks. "It gives an added measure of comfort to know that the Cisco Talos professional IR team helped us strengthen the plans and playbooks," Lorz adds.

Achieving resilience and business continuity

Cisco helped Cintas achieve greater visibility and proactive threat defense to improve resilience and security posture. "A compromised system, data loss, or a successful external attack—depending on the severity—could impact our normal revenue-producing operations.

20,000

intrusion attempts blocked in 30 days

Our security team's mission is to protect Cintas' systems and data from cyber threats," Lorz explains. "Cisco security solutions help us achieve that mission by providing increased threat visibility and protective controls to reduce cyber risks and to ensure business continuity." Lorz continues "We are pleased with how well the Cisco security solutions match our security needs. Cisco security solutions have reduced our cyber risk and improved our security posture. Pulling a holistic solution from the Cisco security portfolio helped reduce the burden on our staff and solution stack. It further ensured the technology we put in place can be implemented more efficiently and effectively."

Cisco's integrated security solutions help Cintas simplify security operations and threat response time. Risk-based context analysis helps Cintas prioritize and address the top risks to promote uninterrupted business operations. Lorz comments: "Implementing Cisco security solutions has simplified threat detection and helped us improve the response time from our security operations team, particularly for network-based events, thanks largely to better visibility paired with threat context from Talos. The single console approach of Cisco Secure Firewall combined with threat intelligence insight and analysis from Cisco Talos help us identify and protect against new threats quickly.

Integrating the different Cisco Secure components into a layered security approach helps Cintas become more resilient. "This provides the case for greater resiliency in terms of being able to withstand or fend off an attack," Lorz explains.

"Cisco AnyConnect works with ISE to check the security health and posture of devices. That rolls into Umbrella's DNS-layer security to stop threats regardless of the port or protocol. This is topped with analyzing applications and assigning a business risk score, all of which flow through different next-generation application-aware firewalls, which can then filter or block based on zones of trust and act on suspicious traffic via intrusion prevention. This level of integration is key to achieving greater resilience and defense-in-depth."

The migration to Cisco Secure Firewall helps Cintas reduce service outages and security-related downtime. Lorz remarks: "Cisco Secure Firewall helps protect us against security-related downtime due to attacks from external threat actors. We can block those threats that are coming in, whether it's some type of privilege escalation or an attempt at credential compromise. From a day-to-day business operation, we're protecting against those outages that are related to cyber events, preventing impact on revenue."

Greater resiliency with Cisco security solutions is helping Cintas protect its customers. Lorz observes, "These days, vulnerabilities in the supply chain are a cause of great concern for businesses. Protecting our organization's information systems and infrastructure helps reduce supply chain risks for our customers. Cisco security is helping us achieve the organizational outcomes the supply chain needs, which is very important."

1. Improved visibility paired with threat intelligence from Cisco Talos
2. Improved resilience and posture with multilayer security defenses
3. Simplified threat detection and improved response time
4. Reduced cyber risk

At Cintas, Lorz strives to balance security investments to avoid the too-little-versus-too-much security conundrum. Lorz adds, "Cisco has helped ensure our success by providing training so that our staff can fully capitalize on our investments by working with us to right-size our deployments and license requirements."

Cintas is enhancing its Umbrella CASB deployment and using Cisco security components to achieve a true secure access service edge (SASE) architecture. "A true SASE deployment requires the right architecture consisting of multiple components, including CASB deployments, Zero Trust Network Access (ZTNA) concepts, SWGs, and software-defined wide area networks (SD-WAN)," Lorz adds. "We have several SASE components already in place or currently being implemented. The ability to integrate the different components of the Cisco security portfolio certainly lessens the difficulty and complexity of a data center to SASE transition."

Lorz concludes by re-emphasizing the importance of interoperability and integration in the security ecosystem: "The challenge cybersecurity presents must be addressed globally. Vendors need to be open to providing comprehensive solutions, similar to how Cisco's platform approach does, integrating not only with Cisco solutions but also with other security vendors."