

Let's help make your smart distribution center more secure

Cybersecurity risks and emerging new technologies are reshaping today's industrial landscape—let us help you keep your assets protected.



The smart distribution center cyberthreat environment

Distribution and logistics companies are under pressure to remain competitive while navigating global supply chain disruptions, rising costs and rapid technological advancements. As they attempt to do this by embracing innovations such as automation, artificial intelligence (AI) and the Internet of Things (IoT), new opportunities for efficiency and growth arise—but so do new security risks. Cybersecurity threats, in particular, are becoming a major concern as interconnected systems can make distribution centers more vulnerable to attacks. A single cybersecurity breach—caused by a ransomware attack or industrial espionage, for example—can disrupt operations, damage reputations and lead to costly recovery efforts.

As many distribution centers and logistics companies incorporate new technologies, they are creating more and more connections that, if left unsecured, could become attack surfaces that bad actors could exploit.

90% of breaches

in North America involve system intrusion, social engineering and other anomalous exploitations.¹

The role of security in an increasingly connected industrial world

You already know that security is a key imperative. But beyond just safeguarding your operations, improving your cybersecurity posture can help empower your workforce and help maintain business continuity and operations. Types of breaches targeting the distribution industry may include web application attacks, system intrusions, malware, hacking and social engineering. Investing in robust security solutions doesn't just help you defend against cybersecurity threats; it also helps you create a strong foundation with the intersection of IT and operational technology (OT) systems as well as IoT connectivity.



\$10.22M

In the U.S., the average cost of a breach surged²



\$860K

The incremental cost of the average breach, year over year³

Help protect your innovation with cutting-edge security solutions.

As your distribution center becomes smarter, potential attack surfaces increase, so securing your environment from cyberthreats becomes even more critical. Verizon offers tailored solutions that can enhance protection from evolving threats, such as system intrusions and third-party breaches. We have partnered with Accenture, adding their experience to our expertise in cybersecurity and networking to help you protect your valuable assets and keep your systems operational.



Stay ahead with continual monitoring and testing.

Cybersecurity is an ongoing process, not a one-time fix. We can help you stay ahead of emerging threats with regular risk assessments, compliance checks and vulnerability scans. This helps assess and test your distribution environment to enhance security.



Enhance your defenses with advanced services.

Sophisticated threats demand a proactive approach. Our Verizon Security Operations Service (VSOS) provides 24/7 monitoring, near-real-time detection and rapid response. We also offer threat simulations and identity protection to help safeguard your team and systems, letting you focus on growth with confidence.



Help defend against cyberattacks and social engineering.

Distribution and logistics companies are often prime targets for cybercriminals. 90% of breaches in North America involve system intrusion, social engineering and exploitations that don't fit into other classifications.⁴ so the risks are real. Our penetration testing and ransomware simulations help identify weaknesses, while advanced monitoring helps you be ready to respond quickly—stopping attacks before they disrupt operations.



Guard your critical assets from external threats.

Your devices, systems and data are the backbone of your business. We can help enhance security to these critical assets through trusted connections, zero-trust access and mobile device management. This proactive approach can help protect your systems from external threats and keep sensitive information safe, even as your operations evolve.



Help mitigate third-party breaches.

Although third-party breaches might not be top of mind for many distribution and logistics companies, they're an emerging risk because these companies rely heavily on third parties to support their supply chains. Credential abuse and malicious actors can turn external partners into attack entry points. We offer solutions such as Secure Access Service Edge (SASE) Management, Red Team Operations and voice security to help monitor, protect and control third-party access.



Help prevent disruption from denial-of-service attacks.

Denial-of-service (DoS) attacks can halt operations and hit your bottom line. Our DDoS Shield, along with our monitoring and mitigation services, can help protect your systems and network, maximize your productivity, maintain smooth operations, and prevent costly disruptions.



Protect your web applications.

Your web applications are crucial to operations, but they can create vulnerabilities. We offer advanced web security services, including identity and access management and zero-trust frameworks, to help mitigate these vulnerabilities from being exploited and help keep your applications protected.

Why Verizon

For more than 25 years, Verizon has helped organizations of all sizes protect critical applications, information and services from potential attacks. As you continue to deploy more advanced technologies, let our extensive security portfolio help protect your business from growing cybersecurity challenges. And with access to the 2025 Data Breach Investigations Report at [verizon.com/dbir](https://www.verizon.com/business/resources/reports/dbir), you can get details that can help you prepare your defenses and educate your organization on how to stay ahead of evolving cyberthreats.

Learn more

Contact your Verizon Account Representative or visit [verizon.com/business/products/security](https://www.verizon.com/business/products/security).

1. "2025 Data Breach Investigations Report," Verizon, Apr 2025. <https://www.verizon.com/business/resources/reports/dbir>

2. "Cost of a Data Breach Report," IBM, Jul 2025. <https://www.ibm.com/reports/data-breach>

3. Ibid.

4. "2025 Data Breach Investigations Report," Verizon, Apr 2025. <https://www.verizon.com/business/resources/reports/dbir>