White paper

The distribution threat landscape

Cyberthreat security challenges and solutions for distributors

verizon business

Distribution is a prime target.

Distribution centers and logistics operations are more interconnected than ever. The collaboration between operational technology (OT) and information technology (IT) helps enable impressive efficiencies and higher throughput.

It has also painted a target on your back for cybercriminals.

Failing to invest in operational defense can be catastrophic to your reputation and your bottom line. In this paper, we will explore today's critical threat landscape; share best practices to help secure distribution center networks, devices and data; and discuss how to train employees to help keep your operation running safely.

One hack, multiple targets

Distribution centers are tempting targets for cybercriminals. A well-placed attack doesn't just have the potential to bring an operation to a standstill. It can also disrupt global supply chains and businesses around the world. What's more, a successful large-scale attack can up the stakes when it results in a sky-high ransom demand.

OT vulnerabilities
OT cyberattacks aim to bring your operation to a grinding halt. They usually focus on equipment, such as automated storage and retrieval systems, conveyor belts, robotic arms, and Internet of Things (IoT) sensors. And as you add new, connected equipment to your workflow, your attack surface expands.

IT vulnerabilities
IT attacks attempt to steal vital information, such as sensitive customer data and financial records. Other digital assets at risk include your warehouse management system, enterprise resource planning and payroll.

63%

of surveyed organizations that suffered downtime from a cyberincident reported major repercussions – a 16-point jump year over year.[1]

Here's how they target you.

Ransomware
This is the most common threat vector. Critical data is encrypted by hackers and then held for ransom, stalling operations. The median amount paid to ransomware groups in 2024 was $115,000.[2]

Supply chain attacks via third parties
To get access to your network, hackers sometimes sneak in through one of your vendors' less-secure systems. In 2024, the percentage of breaches where a third party was involved doubled from 15% to 30%.[3]

Phishing, smishing and social engineering
Tricking employees into divulging their credentials remains a primary tactic of hackers. In fact, 80% of surveyed organizations reported experiencing mobile phishing attempts targeting their employees.[4]

IoT device manipulation
To create back doors in your digital security, cybercriminals infiltrate unmanaged or unsecured devices, such as scanners, environmental controls and smart cameras. Edge devices and virtual private networks were the targets for 22% of exploits in 2024, an almost eightfold increase from the 3% reported in the previous year.[5]

Intellectual property theft
Hackers love to steal your most valuable information – proprietary algorithms, customer lists and business intelligence – and that can be a disaster.

It’s time for distributors to fight back.

The digital threat is clear. Distributors should train their employees to be digital gatekeepers and implement security solutions and protocols that align with industry best practices.

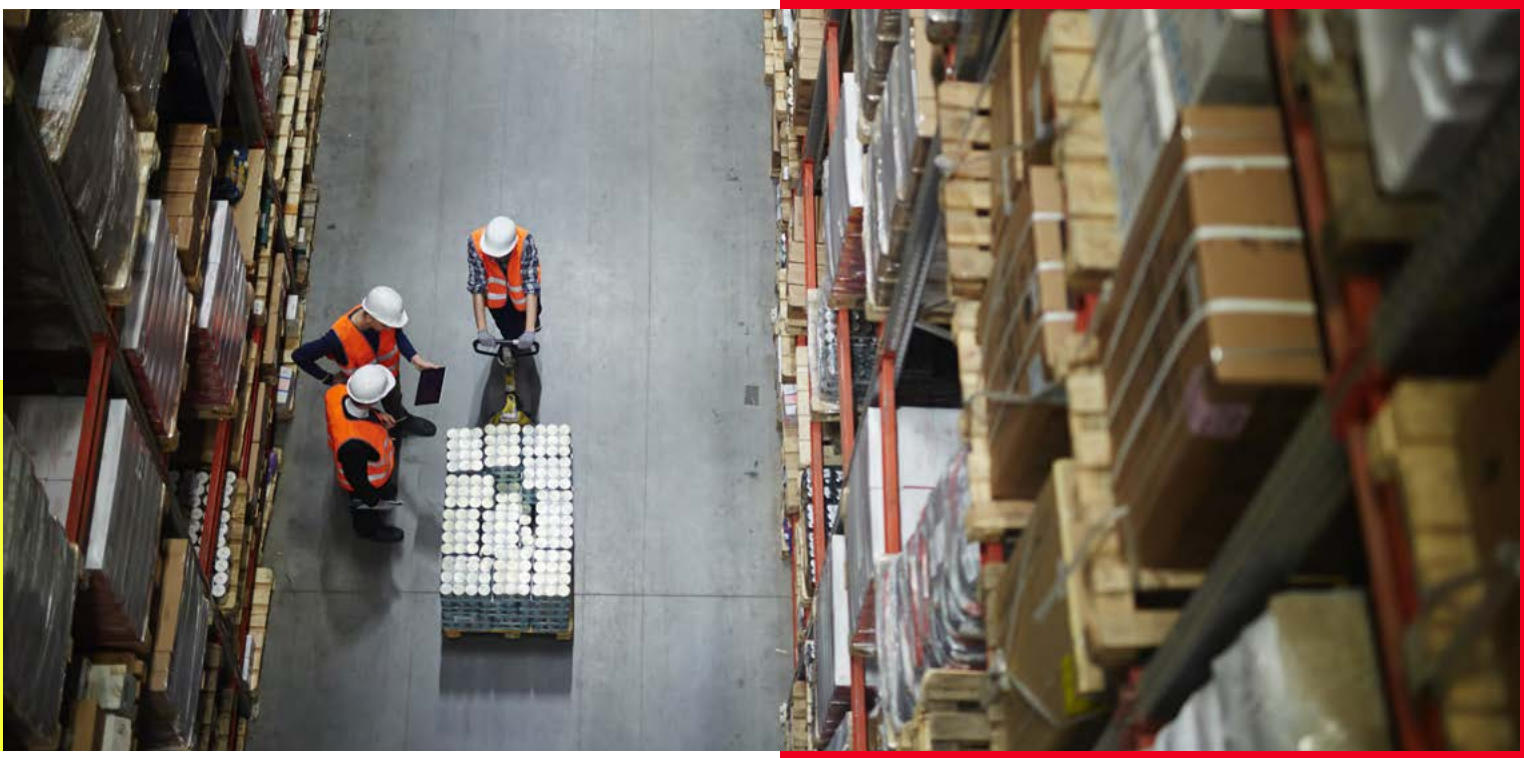
Identity and access management
This set of policies, processes and technologies can help you create an authentication system for your network. Once in place, an identity must be confirmed before access is granted to critical applications, data and network resources for a defined time.

Zero-trust architecture
Trust no one, and always verify. This set of strict security policies requires continual verification of nearly every user and device identity and authorization, regardless of location.

Endpoint protection
Endpoints are where cyberthreats often start, so advanced endpoint detection and response tools should be on servers, workstations and mobile devices.

Immutable backup strategy
Help protect your digital assets from ransomware with the 3-2-1 rule – three copies of data, two different devices, one off-site/cloud copy – to create immutable backups.

Proactive monitoring and defense
Stay vigilant. Integrate software or services into your network that identify and resolve potential security weaknesses. And as always, regularly update software, firmware and operating systems to close known security gaps.



2x

Data shows that bad actors are powering their cyberattacks with artificial intelligence. Synthetically generated text in malicious emails doubled over the past two years from 2023 to 2025.[6]

Digital defense best practices

Creating a more secure, resilient data network against cyberthreats won't happen overnight. With diligence, training and the right vendor partners, you can create a workplace culture that helps protect your company. Below are several best practices for your digital security.

Building the human first-line of defense

Continual education
Targeting humans with phishing attacks and social engineering continues to evolve, so institute mandatory training to help your team learn how to handle sensitive data securely.

Go phishing and smishing
Thirty-nine percent of organizations running simulations reported that between a quarter and half of their employees clicked a malicious link when tested.[7] Organizations should conduct regular internal phishing tests to gauge how employees respond. Those who fail the test should receive additional training.

Managing third-party risk

Due diligence
Your security is only as good as the weakest link in your extended environment. Examine the defense posture of third-party vendors and partners.

Contractual requirements
It's a simple but powerful step to include security clauses and breach notification protocols in vendor contracts.

Response and recovery

Document your response plan
A thorough incident response plan clearly defines roles and responsibilities when disaster strikes. It also guides your team through the next steps for various security threats.

Cyberthreat exercises
Conduct practice drills with IT, OT and leadership to build confidence in responding to different types of attacks.

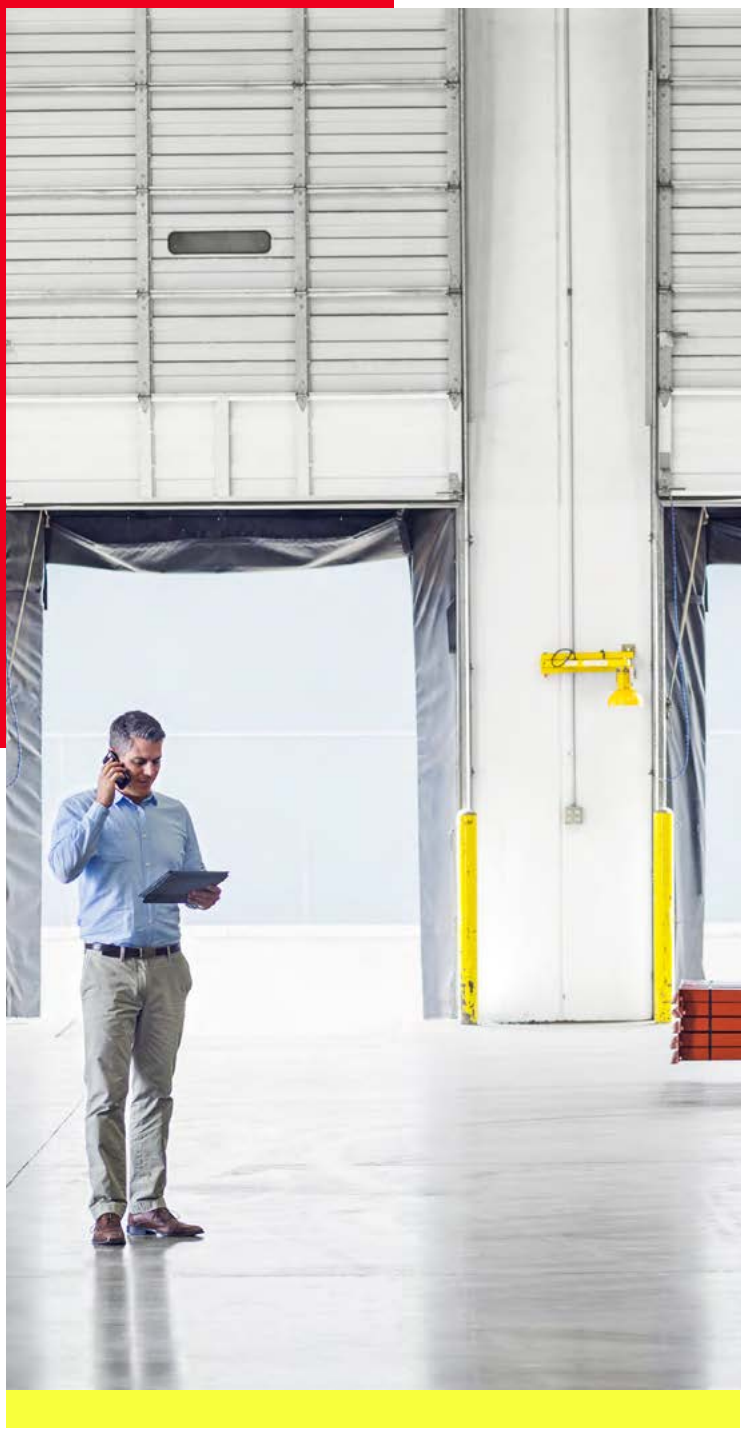
A strong defense can keep distribution rolling.

Your company needs to grow its digital security capabilities, and expert help can accelerate the process. Verizon Security Operations Service provides near-real-time threat detection and rapid response, virtually 24/7. Verizon Security Operations Service can also help with enhanced incident investigation and extended analysis to help safeguard your critical systems. Verizon designs security into its products as well. Verizon's 5G network, for example, can handle high data volumes with ultralow latency with advanced, built-in security.

Distribution digital safety for the long haul

When it comes to distribution, a commitment to cybersecurity is a must. New threats emerge daily, and the barrage of malware and social engineering is relentless. Organizations must create a proactive, resilience-focused security mindset. Investing in zero-trust architecture, multifactor authentication and security training are essential to your success.

A great way to jump-start your security plan is to have a security audit. Security experts can assess your vulnerabilities and develop a comprehensive response plan.



Why Verizon

With more than 30 years of experience managing complex networks worldwide, we understand cyberthreats and how they can disrupt logistics and supply chains. Our network security solutions can help protect your operations and digital assets so you can focus on keeping your distribution moving smoothly.

Learn more

For more information about Verizon and how we can help secure your distribution centers, contact your Verizon Account Representative or visit verizon.com/distribution.

1. "2025 Mobile Security Index," Verizon. Oct 16, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf
2. "2025 Data Breach Investigations Report," Verizon, Apr 21, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
3. Ibid.
4. "2025 Mobile Security Index," Verizon. Oct 16, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf
5. "2025 Data Breach Investigations Report," Verizon, Apr 21, 2025. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf
6. Ibid.
7. "2025 Mobile Security Index," Verizon. Oct 16, 2025. https://www.verizon.com/business/resources/reports/2025-mobile-security-index.pdf

OGWP6040825