ZEBRA

Protect every mission.
Secure every service.

Every agency answers a call of duty. Modern printers help them protect public trust and mission readiness.

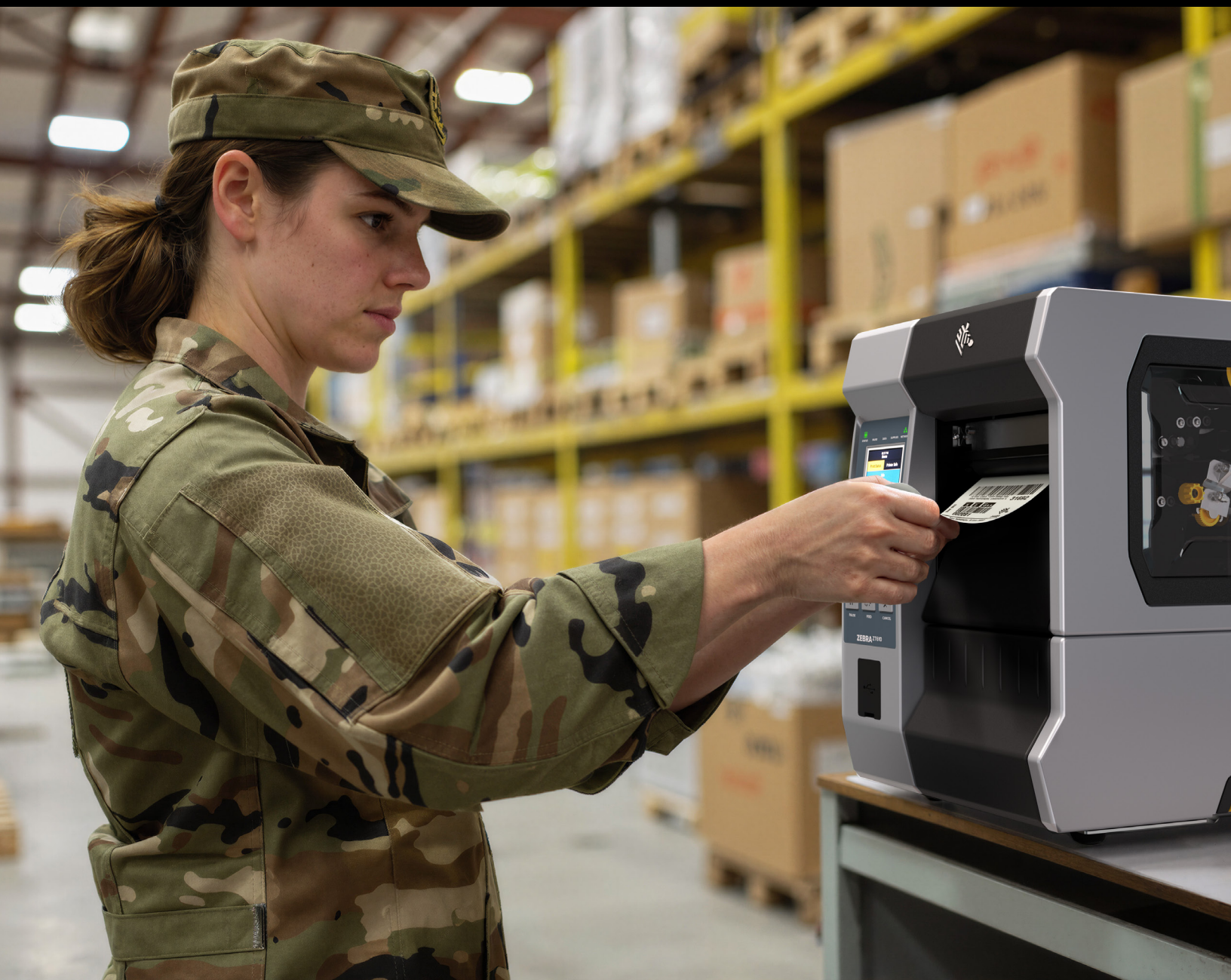
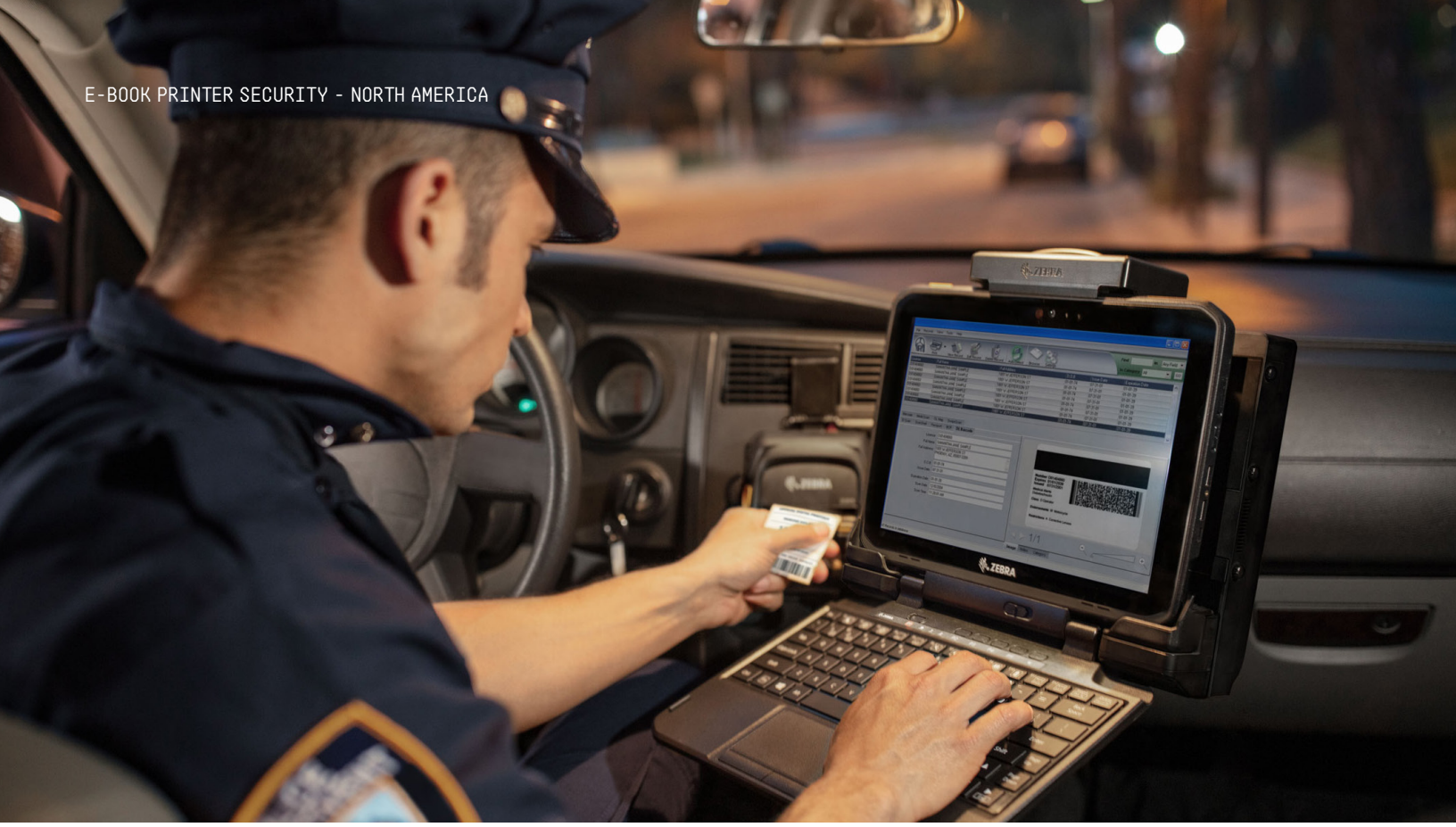


Table of contents



Uncovering the risks of outdated or inferior technology

Is it time to update your printers?

Thermal printers may not be the first devices you think of when it comes to cybersecurity. But they connect to your network and touch almost every part of government work.

In logistics, they track high-value assets. In hospitals, they identify patients, medications, and specimens. In citizen services, they handle sensitive data like drivers' licenses and health records.

When these printers are outdated or poorly secured, they become easy targets for cybercriminals. Weak security systems can allow hackers to view print data, change settings, or shut down critical systems, putting public trust and mission readiness at risk.

Together, we can help you avoid these risks. Start with this e-book to learn how to secure your printers. Then, choose a partner who keeps innovating hardware and software, so your agency is ready for what's next.

Modern secure printers strengthen government operations

- Fewer interruptions
- Better protected infrastructure
- Lower replacement costs
- More consistent services
- Faster work

Operational readiness starts with secure printers

How to strengthen protection and operations

Remote management

Remote tools let you check printers from anywhere and update settings in seconds. Instant alerts allow you to fix problems before they slow you down.

Secure endpoints

Every device on the network matters, even printers. Features like authentication and encryption add layers of protection. With strong defenses in place, your team can focus on serving the public.

Compatible solutions

Get the most from your Zebra printers. Pair them with products, supplies, and accessories made to work together. Your devices will last longer and run better.

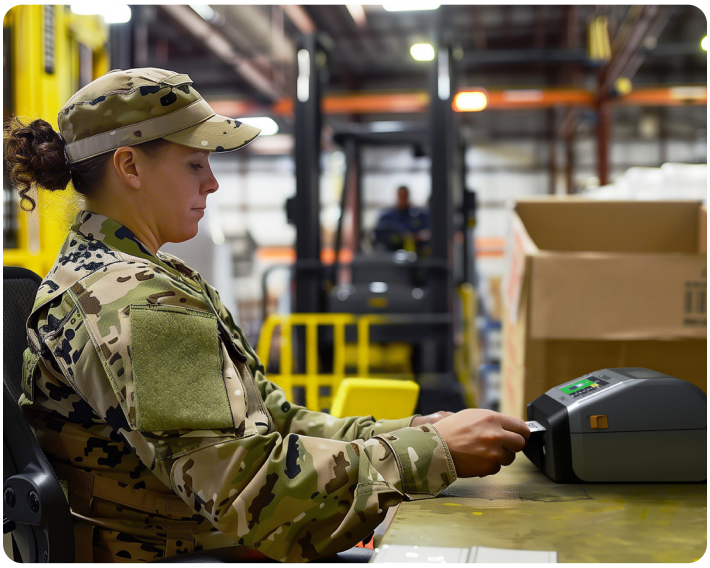
Up-to-date operating systems

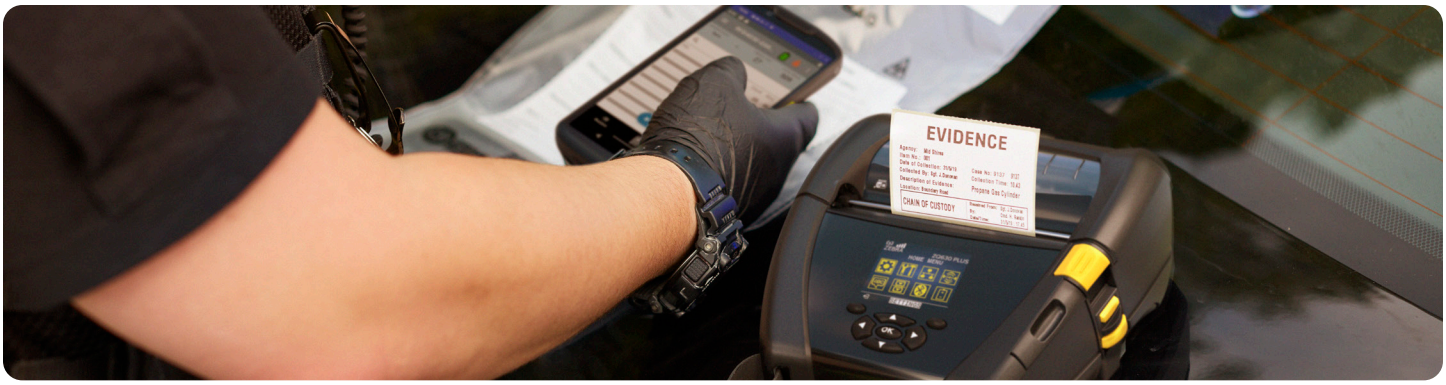
"If it isn't broken, then don't fix it" doesn't apply to printer firmware. Outdated operating systems leave the door open to cyber vulnerabilities, disruptions, and breakdowns. Modern printers, on the other hand, get regular patches and updates, keeping them strong year after year.

For more information on printer security best practices and how to apply them, consult:

Best practices for Securing Enterprise Data and Devices white paper

Link-OS PrintSecure Printer Administration guide





Stronger security strategies

Take a proactive printer approach

Hackers are getting smarter

Cyber threats are advancing fast, powered by AI and machine learning. For government agencies, that makes it critical—not optional—to shore up weak security points. Many admit they aren't fully prepared, with more than half the U.S. government agencies receiving a D grade or worse for cybersecurity.[1] Defense leaders echo the concern. Nearly a third say U.S. communications are falling behind adversaries.[2]

The cost of waiting

The consequences are steep. The average breach now costs $4.88 million, and stolen credentials can hide in systems for nearly a year before anyone notices.[3]

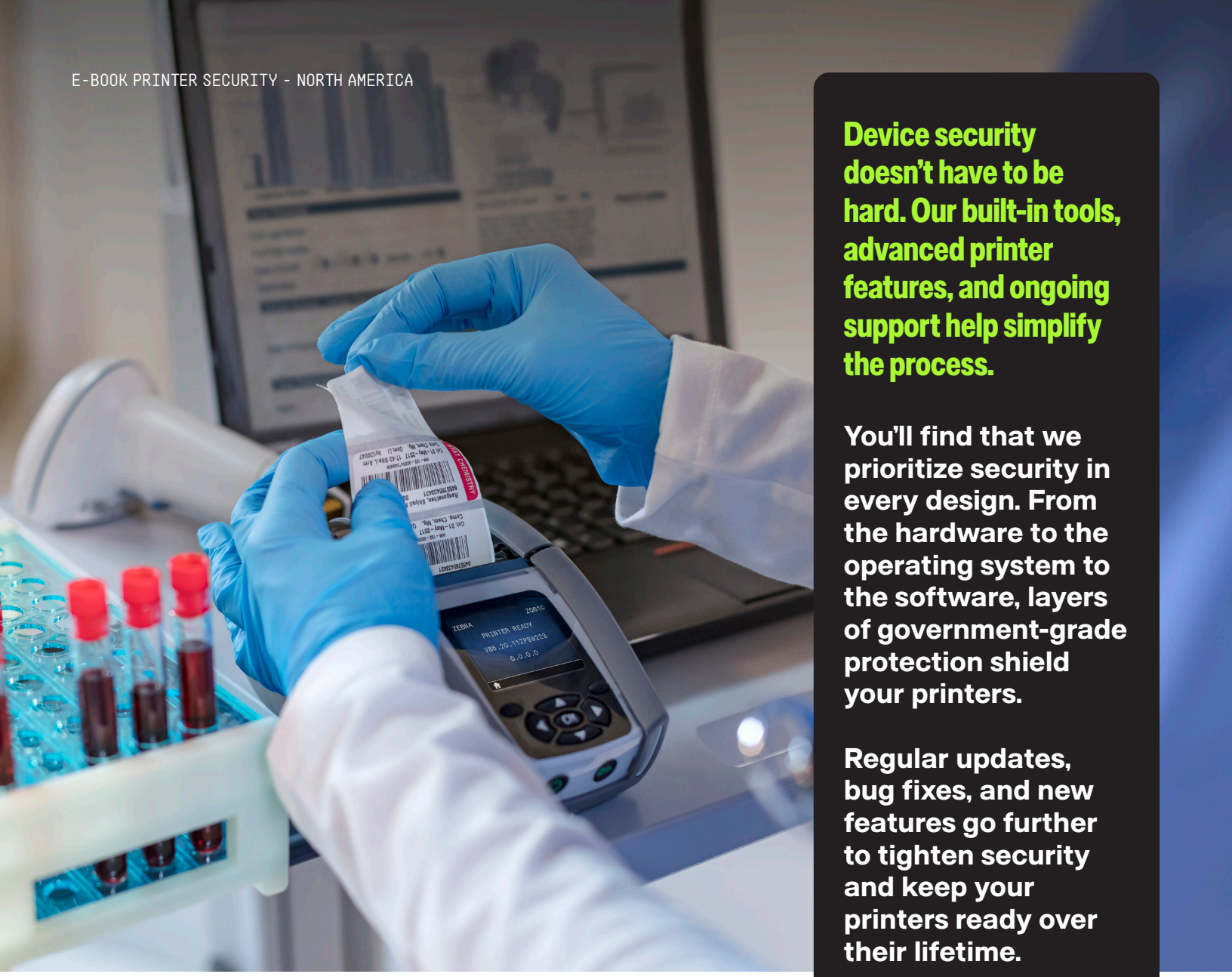
Ward off risk

While the cost of an average breach shows that threats are real and growing, your printers don't have to be part of the problem.

Zebra builds devices with layers of defense that block intruders, protect data, and keep your work moving. With ongoing updates, those defenses only get stronger. That means your agency can stay focused on its mission, not the next attack.

Look for printers with defenses that ...

- Spot risks in settings
- Identify ways to improve network security
- Automatically keep security certificates current
- Block unauthorized setting changes
- Prevent accidental connections
- Allow only approved access
- Encrypt every connection
- Build security into hardware and software that's continually updated



Device security doesn't have to be hard. Our built-in tools, advanced printer features, and ongoing support help simplify the process.

You'll find that we prioritize security in every design. From the hardware to the operating system to the software, layers of government-grade protection shield your printers.

Regular updates, bug fixes, and new features go further to tighten security and keep your printers ready over their lifetime.

Government-made protection without the hassle

Trust Zebra for ongoing updates and support to help protect your printers long after purchase.

ZEBRA DNA

Link-OS™

→ **Download the latest version of Link-OS at Zebra.com**

A portfolio of protection-ready printers

Discover Zebra's lineup of printers outfitted with the latest security features for government

Choosing a Zebra printer gives your government agency greater confidence, savings, and ease.

Here is why: Security runs through every layer, from the body of the printer to the Link-OS™ operating system to Zebra DNA tools. Together, they keep devices safe, simple to use, and easy to manage. Regular updates strengthen protection year after year.

Use the table below to find your existing printer models and make plans to upgrade to the newer equivalent Link-OS models equipped with the latest security protocols.

Easily meet standards. Zebra has a wide range of FIPS 140-2/3 and TAA-compliant printers available through contracts your agency already uses. Contact your Zebra representative for more details.

Legacy Models (End of Service)

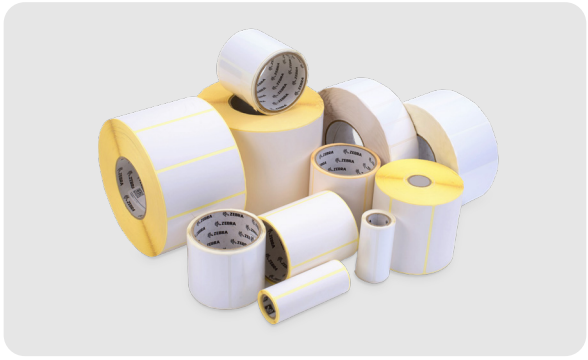
Desktop Printers		
A100 Series	DA402	GK Series
A300 Series	R402	GX Series
Bravo Series	T300/T402	ZD410/ZD410-HC
Companion	LP/TLP Series	ZD420/ZD420-HC
Encore Series	LP/TLP-Z Series	ZD620/ZD620-HC
Tiger Writer	HC100	
HT146	GC Series	
Mobile Printers		
Cameo Series	TR220	iMZ Series
MP Series	ZQ110	QLn Series
QL Series	QLPlus Series	ZQ310/ZQ320
PA400 Series	P4T	
PT400 Series	RW Series	
Industrial Printers and Print Engines		
Z60 Series	ZM400/600 Series	XiII Series
Z90 Series	S300	XiIII/XiIII Plus Series
Z140 Series	S400	Xi4 Series
Z200 Series	S500	ZT410
105Se	S600	ZT420
Z4000/Z6000	2746 Series	ZE500-4
Z4M/Z6M	105SL/105SL Plus Series	ZE500-6

Current Link-OS Models

Desktop Printers		
ZD411/ZD411-HC	ZD510-HC	ZD611/ZD611-HC
ZD421/ZD421-HC		ZD621/ZD621-HC
		ZD611R
		ZD621R
Mobile Printers		
ZQ310 Plus	ZQ511	ZQ610 Plus/ZQ610 Plus-HC
ZQ320 Plus	ZQ521	ZQ620 Plus/ZQ610 Plus-HC
	ZQ511R	ZQ630 Plus
	ZQ521R	ZQ630R Plus
Industrial Printers and Print Engines		
ZT231	ZT411	ZT610
ZT231R	ZT411R	ZT610R
	ZT421	ZT620
	ZT421R	ZT620R
	ZT510	ZE511
		ZE521

Take the next step toward security

Explore Zebra printers built for protection



Zebra Certified Supplies

Our careful attention to small details has a big impact on your workday. We rigorously test our labels, tags, RFID, and linerless media for consistency and high quality.

So, they work well every time.

→ Ready to secure your printers?
Talk to your Zebra rep or visit zebra.com

Sources:

1. Cybernews Business Digital Index, 2025
2. Assessing the State of Military Communications, Government Business Council, 2021
3. Cost of a Data Breach Report 2024, IBM, 2024

ZEBRA

NA and Corporate Headquarters
+1 800 423 0442
inquiry4@zebra.com

Asia-Pacific Headquarters
+65 6858 0722
contact.apac@zebra.com

EMEA Headquarters
zebra.com/locations
contact.emea@zebra.com

Latin America Headquarters
zebra.com/locations
la.contactme@zebra.com