ZEBRA

# Up-to-Date Printers Help Protect Patients and Your Organization

Your patients trust you. Trust your devices to help improve patient care.

# Table of Contents

# Diagnosing the Risks of Outdated Technology

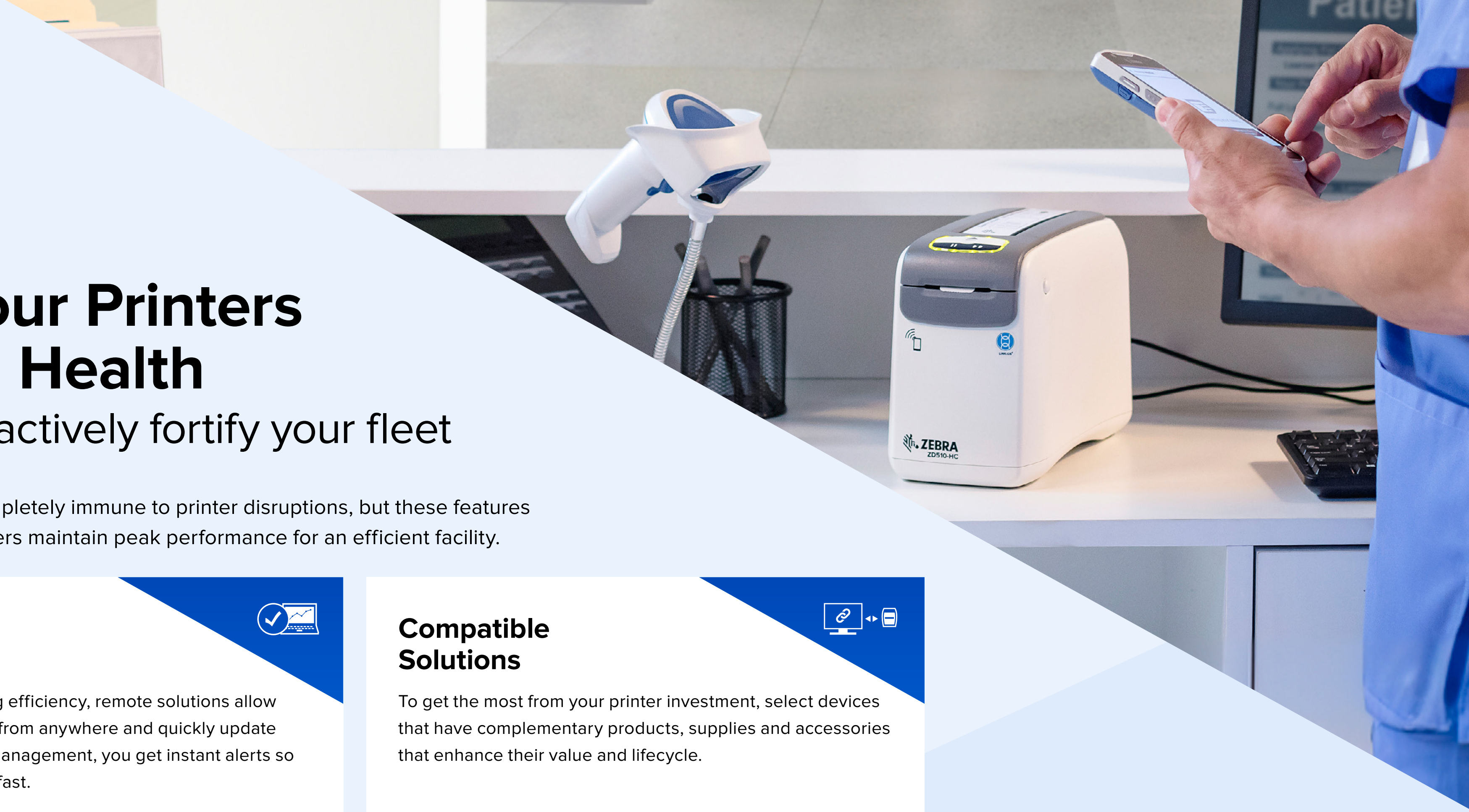
## Is it time to update your printers?

In fast-paced, high-intensity healthcare environments, patient wellbeing is the number one priority. That means people, technology and processes must be in synch to maintain safe environments and adhere to protocols. When systems fail, nurses, doctors and staff lose access to the tools and resources they need to do their jobs and must shift their focus from patient care to resolve the issue.

While trying to extend the life of outdated printers may seem like a financially sound strategy, in the long run it could be leaving you exposed to costly repairs and extended downtime. In this eBook, we'll discuss best practices for maintaining an action-ready fleet of printers and the benefits of regularly updating hardware to ensure teams are always prepared to provide best care for patients.

### Outdated printers cause:

- **Unexpected** downtime
- **Security** risks
- **Costly** replacements
- **Inefficient** workflows
- **Inconsistent** patient care



# Keep Your Printers in Good Health

## How to proactively fortify your fleet

No organization is completely immune to printer disruptions, but these features help ensure your printers maintain peak performance for an efficient facility.

### Remote Management

In addition to increasing efficiency, remote solutions allow you to monitor printers from anywhere and quickly update settings. With remote management, you get instant alerts so you can resolve issues fast.

### Compatible Solutions

To get the most from your printer investment, select devices that have complementary products, supplies and accessories that enhance their value and lifecycle.

### Secure Endpoints

Successful network security requires layers of protection across all connected devices—including printers. Leveraging advanced security features like authentication and encryption strengthens security infrastructure. Investing in technology that keeps your organization ahead of potential vulnerabilities will improve productivity and your ROI.

### Up-to-Date Operating Systems

There is no room for an “if it isn’t broken, then don’t fix it” attitude when it comes to printer firmware. While older devices with outdated operating systems may do the job in terms of printing, without ongoing firmware updates, they are more susceptible to disruptions and extended downtime. Choosing new devices that can be continually updated with bug fixes and patches throughout their lifecycle improves productivity.

For more information on printer security best practices and how to apply them, consult the Best Practices for Securing Enterprise Data and Devices White Paper and the Link-OS PrintSecure Printer Administration Guide.

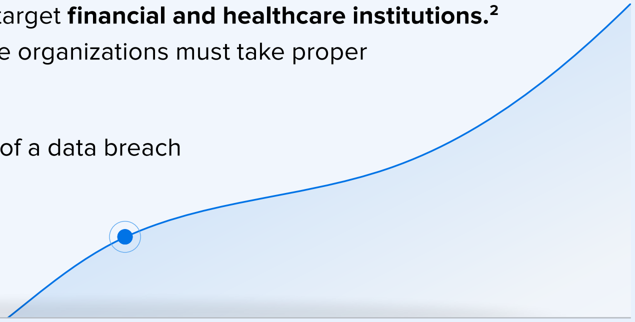
# Stronger Security Strategies

## Take a proactive printer approach

In addition to heightened performance, improved security is a top priority when updating your printer fleet. While it seems like a far-reaching risk, security and data breaches are more common than ever. In February of 2024, one of the largest healthcare security breaches in history occurred, and some repercussions of this attack have still yet to be mitigated.[1]

Data breach incidents most frequently target **financial and healthcare institutions.**[2] As prime victims for damage, healthcare organizations must take proper preventive measures.

According to Statista, the average cost of a data breach in 2023 was **$4.45 million.**



Like a virus attacking the body, when data and technology are compromised, disruptions to patient care are just the start of the many symptoms the organization will face. Cyber threats can plague a healthcare facility with hefty financial losses, cumbersome legal consequences and irreversible reputational damage, making simple, integrated and easily maintained data security crucial.

### To strengthen protection of systems, data and sensitive patient information look for printers that:

- Assess printer settings to help identify ways of improving network security
- Automatically maintain security certificates
- Prevent unauthorized setting changes
- Avoid accidental connections
- Allow only those with validated access to alter operating systems
- Encrypt all connections
- Feature embedded security in both the hardware and software that can be continually updated

# Stay Secure with Specialized Support

## Zebra has the tools and resources to help you update Zebra printers on your network

Zebra DNA$^{\text{TM}}$

Link-OS$^{\text{TM}}$

Securing your healthcare network doesn’t have to be a tiresome and costly process. With integrated solutions, emulation capabilities and ongoing support, Zebra is positioned to make the process simple and painless.

Zebra printers are powered by the state-of-the-art Zebra DNA$^{\text{TM}}$ software suite—powered by our Link-OS$^{\text{TM}}$ operating system—that utilizes the latest security protocols to optimize performance and efficiency, securely. With continuous updates, users get ongoing upgrades and bug fixes that support new features and functionality to keep printers secure and relevant over their entire lifecycle while optimizing ROI. Unlike with competitors, you can count on Zebra to consistently bring innovation and security to the forefront of product and solution designs.

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

Link-OS™

# A Portfolio of Protection-Ready Printers

## Discover Zebra’s lines of enterprise printers outfitted with the latest security features

When you invest in a Zebra printer, you’re taking preventative action that will save you time and money, now and into the future. Our printers are developed with the latest security features and industry-leading Zebra DNA software tools, powered by Link-OS. And with ongoing firmware updates, you can be confident in your security, today and tomorrow.

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

## Legacy Models

| Desktop Printers | | |
|---|---|---|
| **A100** Series | **HT146** | **HC100** |
| **A300** Series | **DA402** | **GC** Series |
| **Bravo** Series | **R402** | **GK** Series |
| **Companion** | **T300/T402** | **GX** Series |
| **Encore** Series | **LP/TLP** Series | |
| **Tiger Writer** | **LP/TLP-Z** Series | |

| Mobile Printers | | |
|---|---|---|
| **Cameo** Series | **PT400** Series | **P4T** |
| **MP** Series | **TR220** | **RW** Series |
| **QL** Series | **ZQ110** | **iMZ** Series |
| **PA400** Series | **QLPlus** Series | **QLn** Series |

| Industrial Printers | | |
|---|---|---|
| **Z60** Series | **Z4M/Z6M** | **2746** Series |
| **Z90** Series | **ZM400/600** Series | **105SL/105SL Plus** Series |
| **Z140** Series | **S300** | **XiII** Series |
| **Z200** Series | **S400** | **XiIII / XiIII Plus** Series |
| **105Se** | **S500** | **Xi4** Series |
| **Z4000/Z6000** | **S600** | |

## Replacement Link-OS Models

| Desktop Printers | | |
|---|---|---|
| **ZD400** Series | **ZD510-HC** | **ZD600** Series |

| Mobile Printers | | |
|---|---|---|
| **ZQ300/ZQ30 Plus** Series | **ZQ500** Series | **ZQ600/ZQ600 Plus** Series |

| Industrial Printers | | |
|---|---|---|
| **ZT231** | **ZT400** Series | **ZT510** Series |
| | | **ZT600** Series |

For the most up-to-date information about Link-OS printers, the equivalent legacy models and security features included, please consult the **Link-OS PrintSecure Printer Administration Guide.**

## Trade in your current devices and earn a rebate to put towards a next generation purchase with The Go Zebra Trade-In Program.

**Or contact your Zebra representative to discuss upgrading to the latest Link-OS printers.**

1. LLP, Schubert Jonckheer & Kolbe. “Privacy Alert: Unitedhealth and Change Healthcare under Investigation for Massive Data Breach.” PR Newswire: press release distribution, targeting, monitoring and marketing, March 7, 2024. https://www.prnewswire.com.
2. Statistics can display more up-to-date data than referenced in the text. This text provides general information. Statista assumes no liability for the information given being complete or correct. Due to varying update cycles, “Topic: Data Breaches Worldwide,” Statista, accessed May 22, 2024, https://www.statista.com.

ZEBRA

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

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

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

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