ZEBRA CAPTURE YOUR EDGE

Best practices for securing enterprise thermal printers

Security risks are real, and attacks are getting increasingly sophisticated. Endpoints are becoming popular targets—including networked thermal printers. Securing entire business networks—including endpoints such as thermal printers—is critical to ensuring complete protection of an organization's digital assets and infrastructure. Fortunately, enterprises can apply best practices to strike a balance between thermal printer security and workforce productivity.

ZEBRA CAPTURE YOUR EDGE

Increasing connectivity opens the door to opportunity and risk

Across countless industries and around the globe, companies depend on devices that are connected, agile, intelligent and manageable remotely. These features are integral to optimal productivity—a critical competitive differentiator. It's how organizations maximize value and minimize waste.

However, with advanced technology, modern connectivity and mobile integration come greater risk and security vulnerabilities. And, attacks aren't slowing, they're growing.

According to the most recent Cost of a Data Breach Report, **"Since 2014, the share of breaches caused by malicious attacks surged by 21 percent, growing from 42 percent of breaches in 2014 to 51 percent of breaches in 2019."**[1]

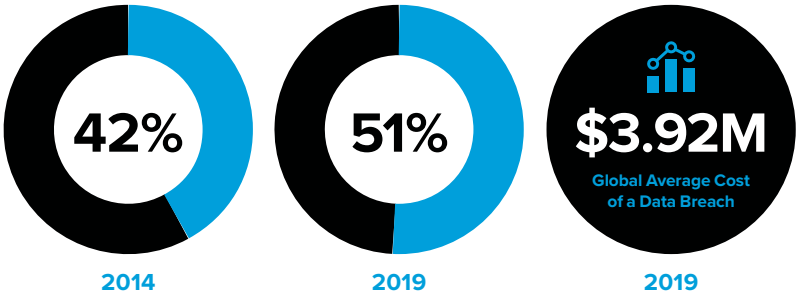
Additionally, the global average cost of a data breach in 2019 was $3.92M.1

Considering the financial, compliance and legal implications—along with the potential damage to a company's reputation—it's no surprise businesses are seriously focusing on security. While networks and firewalls are critical components, security measures shouldn't end there. As devices become more intelligent, those endpoints can introduce vulnerabilities—including networked thermal printers.

According to a recent study, **"Printer security has been identified by IDC as a particular blind spot in the consideration of enterprise security...And printers are much more difficult to harden after they are shipped."**[2]

Companies can harden their security posture—including endpoints such as thermal printers—to safeguard enterprise data with the best practices found in this paper.

Share of breaches caused by malicious attacks:



1. Ponemon Institute, 2019 Cost of Data Breach
2. IDC's Government Procurement Device Security Study, 2018

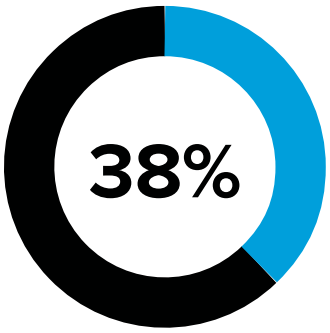
Why Security for Endpoints?

Internet of Things (IoT) devices are increasingly the targets of security attacks. Not only consumer devices—**an alarming 38 percent of attacks targeted enterprise IoT devices.**[3]

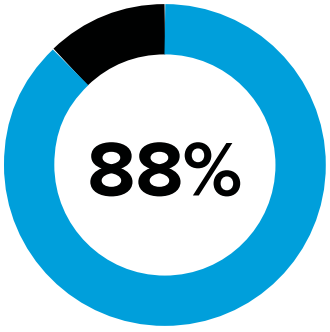
These seemingly benign endpoints can present a point of entry to organizations' primary networks. And worse, they can allow "island hopping"—a method attackers use to target organizations with the intention of accessing an affiliate's network. This puts not only the targeted organization at risk, but also their customers, partners and entire supply chain.

Eighty-eight percent of professional hackers can breach [a] perimeter in less than 12 hours according to a recent report disclosing survey insights from known hackers, professionally known as penetration testers.[4] The same report found that **"[e]ndpoint security is the countermeasure that presents the greatest challenge to hackers during a penetration test."**[4]

Adding new technology, such as thermal printers, to your network should increase productivity—not introduce security vulnerabilities. And, as endpoint attacks are on the rise, selecting a secure thermal printer is critical to protecting your data and infrastructure, along with those of your customers and partners.



OF ATTACKS TARGETED ENTERPRISE IOT DEVICES



OF PROFESSIONAL HACKERS CAN BREACH A PERIMETER IN LESS THAN 12 HOURS

3. Carbon Black Incident Response Threat Report, Nov. 2018
4. Black Report, Nuix 2017

Implement Security Best Practices to Bolster Protection

When selecting a thermal printer, consider the manufacturer. Are they committed to security? Do they have an internal security organization? Do they engineer their products and solutions using best practices and incorporate security into the design of the product? Or, is security put in place after the printer is built?

Does the printer manufacturer incorporate and support all areas of a universally accepted security organization's standard such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework?

Your organization, together with your partners and solutions, should be able to address all areas of the NIST Cybersecurity Framework:

Identify

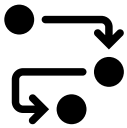
Evaluate and assess vulnerabilities and compare them to security best practices to make informed settings selections

Protect

Establish safeguards, secure-by-design development principles, security updates and tamper-prevention tools to minimize vulnerabilities and enable secure configurations

Detect

See events in real time to continuously manage your printers to detect vulnerabilities and take swift, corrective action



Respond

Create a response plan and be equipped with tools to quickly decommission and re-provision a printer in the event of an incident

Recover

Select a partner who can help you restore services and make improvements to your security plan to prevent future vulnerabilities

Nine Considerations for Selecting a Secure Thermal Printer

You now have a greater understanding of security risks and best practices. How can you adequately evaluate technology to ensure what you integrate adds protection to your enterprise, and doesn't introduce vulnerabilities?

Consider these nine factors, as they align to the NIST Cybersecurity Framework pillars:

Identify

1. **Assess Security Settings:**
   Select a printer with a robust assessment tool to uncover potential vulnerabilities, and compare settings against security best practices so you can make informed choices based on your conditions.

Protect

2. **Maintain Security Certificates:**
   Individual Wi-Fi® security certificates are critical to preventing widespread printer outage from an attack; however, updating individual printers is an error-prone and onerous task. Select a printer with automated, individual Wi-Fi security certificate update capabilities.

3. **Prevent Unauthorized Changes:**
   Prevent accidental or malicious tampering of printer settings changes with administration tools that require authentication.

4. **Avoid Accidental Connections:**
   Ensure Wi-Fi and Bluetooth® connections are secure by default.

5. **Protect Printer Operating Systems:**
   Permit only authorized staff with validated access to alter a printer's operating system.

Detect

6. **Monitor and Manage in Real Time:**
   See events as they occur to quickly apply security updates, detect events and maintain productivity.

7. **Encrypt all Connections:**
   Ensure you can configure your printers using secure connections, block unauthorized access and control data exchanges to safeguard your enterprise.

8. **Ensure Lifecycle Protection:**
   Choose printers that feature embedded security in both the hardware and software that can be updated to support new security capabilities throughout their lifecycles.

Respond

9. **Safely Relocate or Retire Printers:**
   Select a printer that allows you to quickly and easily protect data by resetting all user settings and removing user files.

Performance You Expect + Peace of Mind Security You Need

Technology and solutions—like thermal printers—should increase productivity and drive efficiencies to give your business a competitive edge. At the same time, security is critical to your enterprise and business workflows. You need a proven partner you can trust to deliver innovative technology that adds to your security posture and improves your operations.

Count on Zebra

Zebra is known for innovative engineering, with a broad and deep reputation for purpose-driven design. Our printers, and suite of product and solutions, are developed to improve your business performance—and safeguard your enterprise security.

Security is at the forefront of all our product and solution design. It is a core competency that products and solutions need to deliver exceptional performance that propels high productivity in real-world work environments. Zebra incorporates and embeds security from the beginning—it is not an afterthought or a feature that is added at the end. And, we base our security policies and procedures on universally accepted industry best practices.

PrintSecure: Printer Security Like No Other

To defend against potential printer security breaches, our innovative Link-OS® printers feature PrintSecure, part of our powerful Print DNA ecosystem. Transforming printers from the inside, they give you the tools to:

- **Easily configure your printers to use secure connections**
- **Assess security settings and apply best practices**
- **Block unauthorized access or OS changes**
- **Remotely monitor and manage in real time**
- **Automate updates and certificate management**
- **Control your data exchanges**
- **Decommission printers or reset user settings and remove user files with a single command**
- **Ensure security across the printer lifecycle**
- **And, much more**

PrintSecure gives you the printer security you need, and it's seamless to your frontline workers to allow optimal productivity.

We believe your focus should be on your business, not worrying about printer security. That's why Zebra proactively guards against security vulnerabilities by integrating multiple layers of protection with PrintSecure. Count on Zebra to provide peace of mind that helps you implement your business and technology strategies at the edge.

Secure your thermal printers—and protect your business enterprise—with Zebra's PrintSecure. Contact your Zebra reseller or visit **zebra.com/printsecure**

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
+1 847 955 2283
la.contactme@zebra.com