Are your ID card printers leaving your organization vulnerable?

A preventative guide to avoiding attacks

ENTRUST

SECURING A WORLD IN MOTION

INTRODUCTION

When not properly secured, connected printers can act as an entry point for unauthorized users, i.e., hackers, looking for high-value data. An important part of many corporations, ID printers are often under-secured and overlooked IoT devices, making them a target for cybercriminals. While a 2019 study revealed that 59 percent of organizations reported an incident of print-related data loss in the previous year,* you can protect your organization and avoid such attacks.

The state of the network: All connected devices are vulnerable to attacks

Printers have been part of connected ecosystems for decades. Even your basic desktop office printer is connected to an online server. Today, ID card printers are another attractive target for cybercriminals.

A 2019 study showed that 11 percent of security incidents reported by organizations over the previous year were print-security related.* Sophisticated cybercriminals are looking to exploit your vulnerabilities, whether that's with your basic desktop printer or more specialized printing operations such as those for secure credential issuance.

For organizations with credential issuance operations for the enterprise and healthcare worlds, a breach to the secure printing environment could spell disaster.

* Quocirca Global Print Security Landscape, 2019

The danger of compromised sensitive issuance data from a secure ID operation is clear, but these attacks don't just target the information transmitted to a printer.

Whether for sport, for ransom, or to gain access to higher-value data, cybercriminals are waiting to exploit the vulnerabilities that are common, even standard, in ID card printers. They can gain access to other databases and networks via a "hacked" printer, compromising more sensitive information.

A print-related breach could also lead to a DoS attack that shuts down an entire issuance operation for an extended period of time – an equally devastating threat.

"REST ASSURED, AS A SECURITY COMPANY, ENTRUST DOES REGULAR ROUNDS OF INTERNAL VULNERABILITY AND PENETRATION TESTING OF OUR PRODUCTS – INCLUDING ID PRINTERS – BY QUALIFIED THIRD-PARTY ASSESSORS."

- Mark Ruchie, VP and Chief Information Security Officer, Entrust

Avoid attacks by creating a secure print environment

Easy for us to say, right? Well, creating a secure print environment is actually very manageable. Just follow these four steps:

1. Look at the security of your entire printer environment.

Be sure to include all connected elements of both physical and digital issuance and your personalization ecosystem.

Physical security requires securing facilities, employees, personalization software, supplies, card stock, and the printers themselves. The range of technology is constantly expanding: Alarms, locks, security cameras, identification badges, and access cards all help control who can physically access the spaces of your issuance operation. Also consider hours of operation, separation of duties between staff for appropriate checks and balances, activities that require multiple approvers, and logging of key activities.

Remember, any time human activity is required, it's important to provide proper screening and training to prevent internal threats or vulnerabilities to social engineering schemes.

Digital security begins with protecting the software applications used to issue credentials, manage printers in a fleet, manage inventory, or connect with other components of your digital ecosystem. Many traditional applications are likely already behind a firewall to limit access, but externally hosted solutions (i.e., cloud software) bring about new challenges in terms of access and network security.

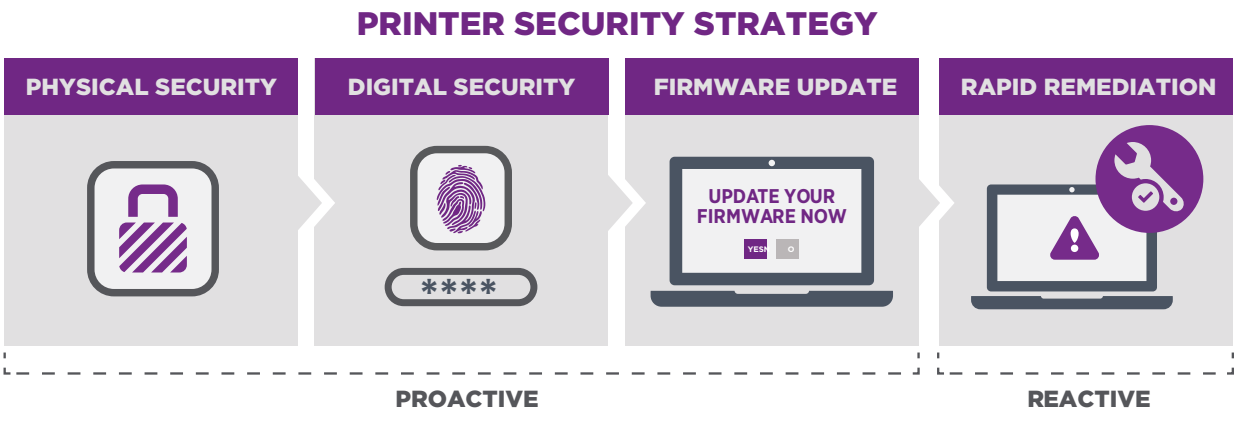
THE DEVICES IN YOUR ECOSYSTEM – INCLUDING YOUR ID CARD PRINTERS – MUST BE AUTHENTICATED TO PREVENT SOPHISTICATED CYBERCRIMINALS FROM GAINING ACCESS TO YOUR ENTIRE PRINT NETWORK AND BEYOND.

2. Construct a map of all parts.
Include all printer hardware, all software and devices connected to your print network, and how your print environment fits within your larger connected ecosystem.

3. Prioritize firmware updates.
It's imperative that maintaining up-to-date printer firmware becomes a core component of your printer maintenance protocol – and your overall security strategy. While updates certainly improve functionality and resolve reported issues, they also provide security features and address new security threats. By ensuring your print environment is using the latest printer firmware, you can help protect your printers against ever-evolving threats, while ensuring optimal performance and efficiency.

4. Understand what is "normal."
Once you identify what normal activity is, "abnormal" activity can quickly be isolated and neutralized. We call this rapid remediation, because unfortunately, even proactive security can't always prevent a print-related breach. If an attack does happen, identifying it and limiting its impact is the key to mitigating overall security risks.

Security threats are constantly evolving, and to be effective, your security efforts must evolve too. An important step is prioritizing the regular firmware updates for your printer hardware. This will keep you at the leading edge of security for your print environment. Regularly conducting reassessments of the security of your print environment will help identify new vulnerabilities before they turn into breaches.



The Entrust difference: outstanding performance, exceptional security

When you get your printer from a security company like Entrust – as opposed to getting your security from a printer company – you get the confidence and trust, as well as outstanding performance and exceptional security, that comes with 50 years of industry experience and innovation.

Our experts are constantly monitoring security threats and vulnerabilities, and developing new security measures to keep our printer hardware one step ahead of cybercriminals.

WHAT TO DO TO KEEP YOUR PRINTERS SECURE:

- ✔ Change passwords as soon as you set up your printer
- ✔ Disconnect from unused functionality and/or ports
- ✔ Keep firmware updated

We regularly release printer firmware and driver updates that provide powerful security features – printer locks and alerts, enhanced security logs, updated networking components, and beyond – as well as new functionality and enhancements that drive print productivity. These firmware updates ensure your printer hardware continues to deliver outstanding performance while maintaining exceptional security. (So please: Update your firmware on a regular basis!)

Entrust also has a complete portfolio of identity authentication and credentialing solutions that help our customers enact optimal physical and logical security – in their print environments and across the entire organization.

> **Sure, our printers produce compelling, high-quality cards. But without security, none of that matters. That's why we consider ourselves a security company first.**
>
> —Martin Hoff, Product Marketing Manager

For more information

888 690 2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com