VASION

Securing Your Business:

Addressing IT's Top 5 Security Concerns

An Executive Briefing by
Corey Ercanbrack, Vasion
Chief Technology Officer

Table of Contents

Whether you're a small business with 100 employees or a multinational enterprise with a workforce of 10,000, you have a shared priority: safeguarding the security of your network.

There's good reason for that prioritization. According to a recent Forbes report, over half (52%) of businesses experienced a cyberattack in the past 12 months, and 90% of technology professionals detected significant risk in their software supply chains in 2023.

These trends show no sign of stopping. Mission-critical security exploits like Log4j and PrintNightmare are cropping up every couple of months. With the shift to remote and hybrid work, organizations are scrambling to plug newly visible gaps without inconveniencing their end users.

Taking this as our starting point, let's examines five security concerns that are top of mind for today's CIO or IT Director:

- Minimizing the attack surface
- Protecting data
- Embracing Zero Trust
- Safely supporting remote work
- Mitigating cyberattacks

What often gets missed is that all of these security concerns intersect in the print environment. That's not just something we're saying as a printing solution provider. It's what our customers are telling us day in and day out.

With that in mind, this paper will also discuss how PrinterLogic's core solution and our Advanced Security Bundle solve these pressing challenges.

Let's kick things off by discussing how PrinterLogic helps to minimize your attack surface and protect proprietary data.

Attack Surfaces

Your attack surface is the number of points an unauthorized actor could breach to extract data or deliver a malicious payload. The size of your attack surface correlates directly with your infrastructure.

In the print environment, "infrastructure" equates almost entirely to print servers. If you have 50 print servers, you have 50 possible attack surfaces—each with multiple attack vectors and hundreds of megabytes of confidential user data as a target.

TOP FIVE SECURITY CONCERNS

PrintNightmare is a perfect—and scary—example of the power and scope of an exploit that leverages print servers as a ubiquitous (and therefore often overlooked) attack surface. It preys on untrusted drivers, turning those modules into rogue agents. But the present tense is important here. PrintNightmare hasn't gone away. It might no longer be grabbing headlines in the tech media, but its three variants remain a critical security vulnerability across the board. Some researchers have even argued that patched servers shouldn't be considered immune.

At the same time, the comprehensive fix for PrintNightmare and other print server exploits is both simple and obvious. To minimize your attack surface, just remove the vulnerable infrastructure from the equation. Problem solved.

At the same time, the comprehensive fix for PrintNightmare and other print server exploits is both simple and obvious. To minimize your attack surface, you just take the vulnerable infrastructure out of the equation. Problem solved.

This is why our customers didn't have to worry about exploited print servers while waiting for a patch. Why? Because PrinterLogic eliminated their print servers the moment it was deployed. Malicious actors can't attack what doesn't exist.

From the beginning, our core PrinterLogic solution has been laser-focused on eliminating print servers through a centralized, enterprise-grade, direct IP printing platform. Since then, PrinterLogic's footprint has only grown smaller and more secure as it evolved into a native SaaS offering with support for all major cloud identity providers (IdPs).

That reduction in infrastructure has huge benefits for cost savings, ease of use, and resiliency, as many organizations have already discovered. Now, they're realizing they can add security to that list too.

Data Protection

No doubt your organization is already taking serious steps to secure your digital data. If you have several individuals or teams of people working with important documents, you're probably making sure that all those folders and files have very specific access privileges. No unauthorized users can open or interact with them. The same goes for apps and other software.

But what about printed documents? That's a different story.

We can all probably share anecdotes about how unsecure everyday printing can be. I remember when I would have to sprint from my desk to the printer to grab a sensitive print job as soon as it hit the tray.

In the real world, however, things don't always go according to plan. You print a confidential job, get distracted by a phone call or a meeting, and then forget to pick it up. So it sits in the output tray, where someone else accidentally grabs it along with their own papers. Whether intentional or not, they've now seen private salary information or confidential details about an upcoming product or program.

This is the number-one way data gets leaked in many companies. The 2023 Quocirca Print Security Landscape study found that 61% of companies reported data loss due to unsecure printing practices like these.

The 2022 Quocirca Print Security Landscape study found that 68% of companies reported data loss due to unsecure printing practices.

Here's where Secure Release Printing comes in.

Secure Release Printing has been an optional feature for PrinterLogic customers for many years, and we're now making this proven technology a cornerstone of our Advanced Security Bundle. What Secure Release does is ask the user to authenticate via badge or credentials while physically present at the printer before the job can be executed. The user who initiated the job is the only one who can retrieve it.

PrinterLogic's Advanced Security Bundle also includes a convenient technology called Mobile App Release. This, too, is a feature we introduced several years ago and have been refining ever since. It functions like other secure release mechanisms, except it employs the user's phone as the authentication tool.

It's important to mention something about simplicity here. We know from experience that forcing users to jump through all sorts of hoops in the name of security is self-defeating because it only makes those users want to circumvent those protocols. That's why Secure Release and Mobile App Release are incredibly intuitive. Users can seamlessly

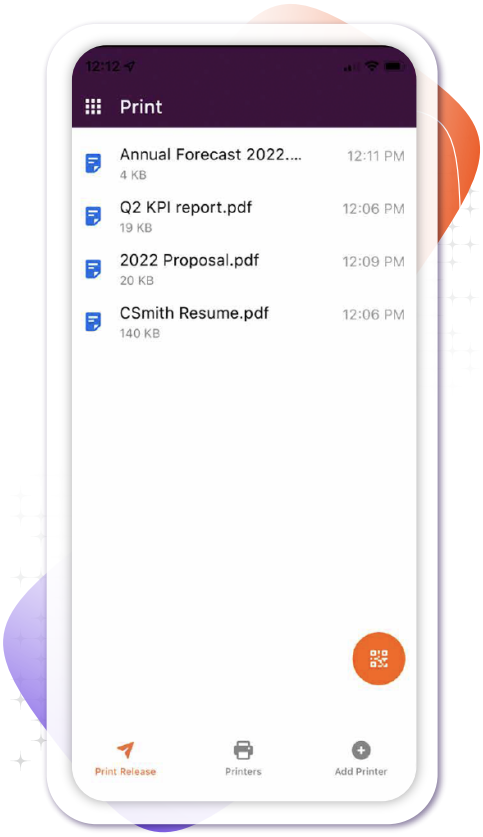

FIGURE 1: The PrinterLogic App makes it easy for users to release secure-release print jobs.

incorporate them into their workflows, so data protection becomes a natural and fundamental part of their productivity.

Another important thing advanced features like these have in common is that they tap into the inherent security of the core PrinterLogic solution. By eliminating print servers, we haven't just reduced an attack surface. We've also ensured that print data never sits in some intermediary point like a server-based print queue. With PrinterLogic, the TLSencrypted print job goes from the user's device directly to the printer. This direct IP paradigm avoids single points of failure where someone could tap into that data stream.

If you look at the full feature set of our Advanced Security Bundle, you'll spot something else that's interesting: Off-Network Printing. This might sound like it goes against our "keep it local" philosophy when it comes to protecting print data. But the reality is that remote work—which I'll cover in more detail below—is now a dominant force in the modern workplace, and we need to find a way to support it securely.

Off-Network Printing mirrors the direct IP approach of our core solution but extends these capabilities to any authorized off-network device. It does this by establishing a secure tunnel between the initiating device and the local destination printer behind the firewall—no VPN required! All the print data is TLS-encrypted along that single path, and it's never at rest.

We also offer a cloud-only model—Off-Network Cloud Printing—that encrypts print jobs temporarily at rest in the cloud. Authorized users will then be able to execute the job locally using one of our release mechanisms to push the encrypted cloud data to our software directly on the destination printer. This method also eliminates the need for additional on-premise infrastructure, like an Internal Routing Service or VPNs, which continues to reduce potential attack surfaces.

Between our core PrinterLogic solution and the functionality in our Advanced Security Bundle, you now have three scenarios that cover any use case while still protecting print data by design:

- Local, direct IP printing enhanced by Secure Release and Mobile App Release.
- Our Off-Network Printing solution, where data is not at rest.
- The sister functionality, Off-Network Cloud Printing, where data is encrypted at rest through the cloud.

Attack surfaces and data protection are what you might call big-picture security issues. Although they've been on IT's radar for a while, the way we approach them is evolving. They now include a wider variety of user protocols and IT practices that can touch a lot of different areas of an organization.

Next, we'll narrow our focus a little by delving into Zero Trust and remote work—two recent trends that are not only deeply intertwined but also profoundly impact the print environment.

Zero Trust

Zero Trust is a computer security concept that first appeared in 1994, yet it didn't start seeing mainstream adoption for another two decades. The name says it all. In a Zero Trust environment, the assumption is that every device is potentially compromised. To mitigate these risks, there should be multiple authentication mechanisms and access control policies in place for users as well as their machines.

That's a tall order—very simple in theory, a lot more complicated in practice. As a result, you have IT leaders asking themselves and their teams, "How do we get to Zero Trust while stillkeeping all the essential pieces of our IT puzzle?"

TOP FIVE SECURITY CONCERNS

Printing has historically been one of the trickier pieces. After all, the very concept of printing is a holdover from the analog world of ink and paper. Its primary purpose is to turn what we see on our screen into something we can hold. Maybe that's why it sometimes feels like there are light years separating today's print environment from modern cloud computing, where the user's location is fluid.

So, when you're talking security best practices, maybe the question is better phrased like this: *How can a technology with such a classic pedigree as printing be modernized for the era of cloud-based Zero Trust models?*

The starting point is authentication.

First, you've got to get single sign-on (SSO) in place. You can think of SSO as the one-stop authentication shop for users where they sign in to all their cloud services at the same time. SSO works hand-in-hand with—but is also distinct from—the identity provider, or IdP. The IdP is the data store for digital identities and functions like a guest list. If you're not on the list, you don't get in.

What makes IdP different from traditional authentication is that it's all about the user, unlike traditional authentication methods which are focused on the system. In keeping with the Zero Trust philosophy, IdP also verifies apps, devices, and any other entity that wants to connect to the network.

The second step is multi-factor authentication (MFA). It's designed to double (or even triple) check the validity of any authentication process—similar to presenting your passport after showing your driver's license. Everyone has run across MFA with SMS verification codes that deliberately slow down access to sensitive websites or accounts.

For the third and final step, you'll need to implement adaptive identification. This is a context-based security concept that emerged in response to mobile device adoption, and it's taken on more importance during the global shift to remote work. In simple terms, adaptive ID means, "I'm going to trust you a lot more if you're working out of your home office than if you're in the local coffee shop." At home, you might be able to go for days without re-authenticating. At the coffee shop, it will be more frequent.

In simple terms, adaptive ID means, "I'm going to trust you a lot more if you're working out of your home office than if you're in the local coffee shop." At home, you might be able to go for days without re-authenticating. At the coffee shop, it will be more frequent.

All of this is difficult—if not impossible—to apply to the traditional print environment. That's why PrinterLogic, as a native SaaS solution, creates

a bridge between the two. Our core platform supports all major IdPs, including Okta, Azure AD, Google Identity, and several more. We tightly integrate with industry standards like Security Assertion Markup Language (SAML), System for Cross-domain Identity Management (SCIM), and OpenID Connect (OIDC) to update and authenticate principals and authorize access to printers.

Before a print job can come through, PrinterLogic checks with the IdP's authentication policies to ensure that the user and their device is thoroughly vetted.

And as far as admin tasks go, PrinterLogic's role-based access control (RBAC) lets you limit the scope of access while also delegating more responsibility to power users. You can even let users install printers themselves without worrying about them doing anything beyond that. So you get granular security and fewer support calls.

There are two more important aspects of Zero Trust that are worth mentioning here. One involves shrinking your network. The other has to do with conducting ongoing audits.

Both of these are also addressed with our core PrinterLogic platform.

PrinterLogic was designed from the outset to eliminate infrastructure—specifically, print servers. That doesn't just minimize your attack surface. It also shrinks your network: fewer devices, less exposure, and less to keep tabs on and lock down.

In addition, PrinterLogic's core platform includes powerful auditing capabilities. From end-user print activity to admin configuration changes, you can see exactly who did what, where, and when. That rich oversight, coupled with PrinterLogic's authentication and access control, creates a secure print environment that supports Zero Trust policies.

Remote Work

Any conversation about Zero Trust is incomplete if it doesn't tie into remote work.

Coming off the heels of the COVID-19 pandemic, some form of remote work—or its close cousin, hybrid work—is widely acknowledged as the workplace standard going forward. A recent survey we conducted revealed that over 80% of our customers envision their employees in remote or hybrid work models for the foreseeable future.

Generally, many of the same technologies that are enabling Zero Trust are also key to hardening the security around remote work. These include the cloud-based IdPs, MFA, auditing, RBAC, and other protocols and practices I laid out above.

But let's look at things from the remote user's point of view. For this, we'll use an example we featured during a recent live demo. We had Greg, one of our employees, sitting by the pool at a downtown hotel. He was connected to the hotel's Wi-Fi, enjoying some downtime, and checking social media feeds on his phone.

He remembered he needed to print a document at the office. The printer, of course, was connected to our corporate network.

Think about all the moving parts involved in that device chain. How in the world does Greg print without resorting to all kinds of inconvenient network acrobatics? And more importantly, how does he do it securely?

Coming off the heels of the COVID-19 pandemic, some form of remote work—or its close cousin, hybrid work—is widely acknowledged as the workplace standard going forward. A recent survey we conducted revealed that over 80% of our customers envision their employees in remote or hybrid work models for the foreseeable future.

This is where PrinterLogic's Off-Network Printing feature plays a huge part. Using this feature in our Advanced Security Bundle, Greg could remotely print a job from his mobile device to one of our in-house printers with a few taps. PrinterLogic handled the authentication and access control along the way—even if that required concurrent IdPs. We encrypted the print job from end to end to avoid possible interception.

From Greg's point of view, this was as simple as printing from inside the office. He was able to stay productive from an offsite location. And his print data stays secure. A win-win.

This scenario would apply equally well in a workplace hoteling or desk-sharing scenario. Then add PrinterLogic's location-aware functionality, where we figure out where a user or device happens to be, based on criteria like their IP address. If someone who works in several places sits down at a desk in a new building, they are automatically associated with a nearby printer. That printer even auto-installs on their compatible device.

On the horizon, we have additional technology in the works that will make life even easier for guests, freelancers, and hybrid workers—enabling them to print securely without having to deal with a conventional print dialogue. When they want to print, they're simply taken to a PrinterLogic portal page where they can upload their file. The portal gives them a unique identity so they can walk to the printer, enter their ID, and tell the printer to release the job. That's it: serverless, clientless, and driverless.

Additionally, our robust offline printing capabilities are especially useful when a remote user prints a job to the in-house corporate printer for later retrieval. Let's say they send a print job

from their laptop at home, then come into the office the following day without their computer. They can still release yesterday's print job simply by swiping their badge. This PrinterLogic feature already works with Windows endpoints, and we plan to make it fully OS-agnostic—like everything else in our solution.

But we know even features like secure tunneling, offline printing, and end-to-end encryption can't stop every single hacker from trying to break in—the same way that outfitting a building with deadbolt locks, an alarm system, CCTV cameras, tall fences, and a guard dog doesn't mean that criminals won't still try to find a way inside. To assume otherwise risks turning a blind eye to the reality of today's cyberthreats.

That's why our final security concern might be the most important.

Cyberattacks

It wasn't all that long ago that cyberattacks seemed like a peripheral threat. Sure, there were always script kiddies knocking at the door, and once in a while, you'd see something serious emerge with the media educating us on a widespread vulnerability that was ripe for exploitation. But on the whole, as long as your software was reasonably up to date, you weren't biting your nails every time a device connected to the Internet.

How times have changed.

TOP FIVE SECURITY CONCERNS

During the pandemic, malicious e-mails—arguably the most public-facing form of cybercrime—soared by 600 percent. However, according to McAfee's 2020 report, titled The Hidden Costs of Cybercrime, less visible threats of malware and spyware now pose the biggest financial risk to organizations. Cybercrime Magazine predicts that annual global cybercrime costs will top $10 trillion (USD) by 2025. In 2015, it was one-third of that amount.

In short, cybercrime is a moneymaker. Malicious actors are more organized, savvy, and mobilized than ever. They've grown bolder and more sophisticated.

With cyberattacks, it's no longer a matter of if. It's a matter of when. Software is developed, installed, configured, and used by humans—so it's never going to be impervious. And unfortunately, there's a group out there who will seize any chance they get to exploit a chink in the armor. Of the 1,500 companies included in McAfee's report, only one in 20 managed to avoid some form of cyber-incident in (pre-pandemic) 2019.

According to McAfee's 2020 report, titled The Hidden Costs of Cybercrime, less visible threats of malware and spyware now pose the biggest financial risk to organizations.

Every organization is going to feel the sting at some point.

The good news is your hands aren't tied. There are solutions. Cybercrime prevention and mitigation are already baked into the way companies like ours deliver and maintain software in the SaaS era.

Previous to SaaS, software models used a more protracted release cycle. You'd install a software solution on-prem, often taking a wait-and-see approach to gradual updates that enhanced functionality or plugged security holes. The cycle was measured in months or even years.

But then news of an exploit would emerge. You'd learn that CVE-1234 enabled a shady user to gain control of the entire network by printing a black-and-white document in color! It became a race to adjust settings, disable functionality, and limit access in the near term while you waited for a patch. PrintNightmare, which I addressed in the "Attack Surfaces" section, is a classic example of this old-school horror story.

By contrast, PrinterLogic's cloud-native SaaS solution is both more proactive and more responsive. They're always being updated behind the scenes to pre-empt possible exploits and close existing loopholes. It's like getting into your car every morning knowing that overnight it received a tune-up, safety inspection, and performance upgrade.

Compared with old-school software release cycles, PrinterLogic's hosted solution maintains quality and fends off potential threats via thousands of small improvements, metered out in a steady cadence. We had a record-breaking number of code deployments in recent months, and in doing so, we've maintained 99.98 percent uptime. In fact, we publish rolling updates that improve functionality and address potential security gaps about one hundred times a day.

This approach is a big win for our customers. When automatic SaaS deployments become common code, everyone is updated at the server level. There's no more damage control followed by a long, anxious wait for a security patch that IT has to apply across the board. Instead, vulnerabilities can be addressed universally in a matter of hours. We're also working on some exciting functionality that will further capitalize on the advantages of this architecture. In the future, at IT's discretion, every software component that's part of the PrinterLogic solution—like endpoint clients or printer apps—will be able to receive automatic updates in the background.

Agility like that is how you manage cyberattacks. It's also how PrinterLogic's modern SaaS approach saves time, headaches, and costs several times over.

The Takeaway

Your organization's security posture is dependent on it's ability to minimize attack surfaces and implement Zero Trust-caliber printing to keep cyberattackers at bay. If you aren't keeping a close eye on such an important part of your broader IT environment, you're exposing your organization to serious risk.

PrinterLogic's approach to ensuring your print environment is protected changes the rules of the game. Between our serverless SaaS platform and our Advanced Security Bundle, we solve the most pressing security issues by systematically hardening day-to-day printing and removing key vulnerabilities altogether.

We achieve this through capabilities such as:

- Eliminating and consolidating print infrastructure
- Offering concurrent support for leading IdPs
- Multi-factor authentication (MFA)
- Secure Release Printing with easy badging and secure print job retrieval
- Mobile App Release for end user convenience
- Role-based access control
- Off-Network and Off-Network Cloud Printing for remote printing from any device
- Automatic and timely SaaS updates

Change the rules of the game by ensuring your print environment is protected with PrinterLogic.

And when you're ready to bridge the gap between your print environment and the digital work critical to a modern organization, look for a solution that can unify the entire organization. The leaders who can see beyond the current state, to one where the most critical business processes and systems are orchestrated and automated, while still offering a Zero Trust-enabled SaaS print environment that enables on-the-ground work to get done, will be the leaders who unlock true operational efficiency and scale. Let's have a conversation about Vasion Automate, and where your future could go. Visit us at vasion.com to learn more.

Features that Fit Your Business

All Vasion Automate customers receive the core features outlined below. You may select up to three bundles to tailor your solution to your business needs.

Vasion Automate Core

Includes: ✓ 5 Automate Creators ✓ 2500 completed workflows ✓ Up to 25 print queues

Print

- Print Object Management
- Printer Driver Management
- Print Job Management
- Driver Profile Management
- Self-Service Installation Portal
- Printer Driver Deployment
- OS Agnostic Support (Windows, Mac, Linux & Chrome)
- VDI Support (Citrix, AVD, Horizon)
- Printer Manufacturer Agnostic
- Mobile Direct IP Printing (iOS & Android)
- Print Server Data Migration Utility
- Data Warehouse & BI Integration
- Role-Based Access Control
- Administrative Auditing
- Print Job Reporting & Analytics
- Printer Monitoring & Alerts (SNMP)
- Identity Provider Integrations (Single & Concurrent)

Forms

- Web and PDF Forms
- Drag-and-Drop Functionality
- Customizable Branding
- Collect Signatures
- View and Export Real-Time Results

Workflow

- Streamlined Business Processes
- Drag-and-Drop Functionality
- Fully Customizable Fields
- Signature Routing
- Built-in Email Notifications

Simplified Scanning

- Scan to Email
- Scan to Cloud Storage (Box, One Drive, SharePoint & Google Drive)

Signature

- Ability to add to forms
- Upload, Draw, or Type Signature Options

Administration

- Account Management
- User Permissions
- IdP Configurations

Add-Ons

Additional Automate Creators

Additional 10,000 Workflows

Bundles

+Advanced Security

- Secure Release Print
- Mobile App Print Release
- Offline Secure Release Print
- Off-Network Print
- Off-Network Cloud Print

+Output Management

- EMR/EHR Support (Epic, Oracle Cerner)
- ERP Support (SAP)
- API Print Service
- Rules & Routing
- Batch Printing
- Confirmed Delivery*
- Document Transformations*
- Document Conversions*
- Highly Available Zones*
- Print Queue Management*

+Cost Management

- Print Quota Management
- Copy Quota Management
- Scan Quota Management*

*Coming soon
+Core - licensed on print queues

About the Author

Corey Ercanbrack is Chief Technology and Product Officer at Vasion. He directs product design, engineering, quality assurance, and product support for Vasion's expanding product line, including the company's bedrock brand, PrinterLogic. Corey brings over 25 years of experience to the table in software engineering, IT, support, and leadership.

Before joining PrinterLogic, Corey held several engineering leadership roles, including Vice President of Product Development at InsideSales.com, Chief Technology Officer at Radiate Media, and Vice President of Global Engineering at LANDesk. He has repeatedly built enterprise development teams with excellent engineering processes and delivered award-winning solutions. Corey also spent nine years at Intel, where he held various engineering positions, including Director of Validation for software products and services and Director of System Integration and Validation for internet management and appliance.