



Zebra Security Platform

Protect your performance edge

The pervasive connectivity that accelerates your business can also expose it to potential security risks. While putting up firewalls is a start, it's by no means an end-all in the face of emerging and sophisticated threats. Discover the best practices and enterprise solutions that can better defend your organization and data.





How to stop security threats from stopping your business



Security is Imperative

Credit card numbers. Health records. Social security numbers. Passwords. Whether you're in the business of serving customers, patients or citizens, you're expected—and frequently mandated—to keep personal information private.



Risks Will Rise

That will only become increasingly challenging with time. For one, the Internet of Things and cloud technology are connecting people and information like never before, giving your organization unprecedented operational control and visibility. While the prospects are exciting, they're not without risk.

The estimated 50 billion¹ interconnected devices anticipated by 2022 could open organizations and confidential data to countless points of vulnerability. Motivated by high profits and a low probability of repercussions (only five percent of hackers have been prosecuted²), cybercrime shows no signs of slowing down.



What's at Stake?

One breach alone can extol a hefty price, costing you dearly in productivity and financial loss, as well as jeopardizing your reputation.

What can you do? Take security seriously. Even if your organization has a security program, chances are that misperceptions are undermining its integrity and creating unnecessary vulnerabilities.

\$3.9 million:

Average cost of a data breach³

25,575 records:

Average size of a data breach³

12 hours:

Average time for 88% of hackers to break through cyber security defenses⁴

197 days:

Average time for an organization to realize there's been a breach.³

Targets:



Retail:

80% of online retailers' login traffic is accredited to hackers using stolen data⁵



Government/ Public Sector:

Prime target with espionage and financial gain the key motivators⁶



Healthcare:

Second most targeted industry, accounting for 15% of cyberattacks⁶



Manufacturing:

Experienced a higher level of espionage-related breaches than other verticals in the past few years⁶

Don't let misperceptions weaken your security

Despite the spate of widely publicized security incidents, many organizations remain complacent about security. Don't be lulled into a false sense of safety. The truth is that if you find yourself saying these things, you could find yourself in trouble.

“My organization isn't large enough to be a target.”

Forty-three percent of cyberattacks target small businesses.⁶ Hackers exploit small businesses' lack of resources and knowledge. They may even use your organization to access your connections with larger entities.

“We're protected by our network.”

A sound security initiative is multi-layered and constantly evolving. Locking your front door won't stop a thief from entering a window if you leave it open. In fact, one study revealed that traditional countermeasures, such as firewalls and antivirus, almost never slowed hackers down, but endpoint security technologies were more effective at stopping attacks.⁴

“We haven't had a breach, so our security works fine.”

You may not realize a breach has already occurred. Research shows it can take a company as long as 197 days simply to detect one.³

“We already have a formal security program.”

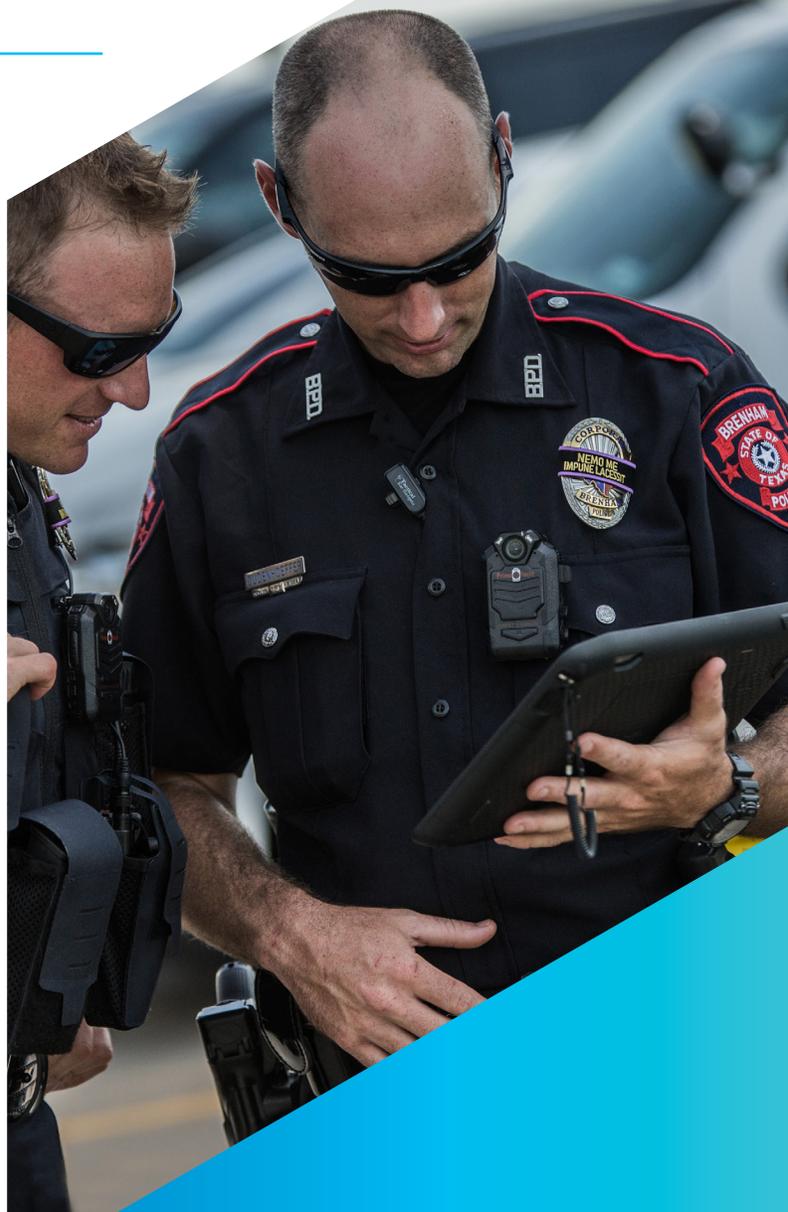
Great. Is it constantly evolving to keep pace with ever-changing threats? Does it cover all your technology? A one-and-done approach is no match for today's sophisticated cybercriminals.

“Security is too complicated.”

Security that's well engineered is intuitive and easy to implement. Count on it being seamless for your workers and simplified for your IT to manage.

“Security negatively impacts productivity.”

Grievances, such as security systems being too cumbersome, too difficult to integrate or stalling operations, are all too common. Yet, a breach can bring work to a grinding halt. The solution is to select technology embedded with security in its design. That's how security can support rather than impede productivity.



Shield your organization with multiple layers of defense

Not all security measures can measure up to your needs. When considering technology, consider these critical security attributes intrinsic to Zebra Technologies and peace of mind.



Built-In Protection and Performance:

Choose the brand that integrates security and productivity into technology from the start. You'll find that our solutions are intentionally designed to elevate your performance, while seamlessly incorporating a range of highly effective security protocols and features.



Automated Security Capabilities:

Wi-Fi® certifications that once took your IT department weeks to complete can now be done automatically, accelerating a secure connected environment for you and your team.



Customizable for Your Needs:

Prefer to set your own security tolerance? Zebra makes it easy to do so with our configurable solutions that adjust security levels based on your company or department needs.



Simpler Maintenance and Service:

Trust that our security features, software and hardware has been developed and tested to perform with minimal maintenance and maximum uptime. Plus, our 24-hour service response team is there should you need them.



Effortless Integration:

Smooth, swift integration is yours with Zebra. Thanks to our deep understanding of your industry and applications, we've already designed our solutions to anticipate and fulfill your integration needs.



Continuous Vigilance and Support:

Pair years of OS security updates and firmware enhancements with troubleshooting, vulnerability assessments and internal security collaboration.



Follows Globally Recognized Best Practices:

Take comfort in knowing that Zebra follows best practices and guidelines set by the world's security experts, including ISO, The National Institute of Standards and Technology (NIST), and The Center for Internet Security Benchmark Controls. Our products and solutions are used in applications that help organizations comply with HIPAA, PCI-DSS and GDPR.



A Leader in Secure Enterprise Technology:

Partner with the name that hardened Google Android's™ operating system for enterprises and offers up to ten years of security OS support. From our fortified enterprise mobile computers to our secure printers and visionary technology, you'll find that productivity and security are at the core of everything we do.

Zebra Products, Solutions, and Services Support for Every Phase of the NIST Cybersecurity Framework

IDENTIFY	Risk Management Monitoring Printer Security Assessment Wizard Professional Services	Supply Chain Risk Management Security Committee
PROTECT	LifeGuard™ for Android Printer Protected Mode Device Control	PrintSecure Updates Auto Wi-Fi Cert Management Risk Management Framework
DETECT	Printer Profile Manager Enterprise Security Monitoring	Real-time Detection
RESPOND	Device Management Threat Detection Counter Measures	Incident Response Customer Alerts
RECOVER	Professional Services Enhancements	Restore to Known State





Securing your performance edge

Security is critical to your business and workflows. That's why Zebra proactively guards against security vulnerabilities, by integrating multiple layers of protection into our solutions. Zebra devices, technology and services are designed with security in mind, without hindering your productivity. You'll find our security is easy to deploy and seamless to your frontline workers. With our smart, configurable technology, you can balance operational objectives with security, in real time, in the real world. Depend on Zebra to provide peace of mind that helps you implement your business and technology strategies at the edge.



See how our security standards improve yours

Visit www.zebra.com/product-security

Sources:

1. Juniper Research, 2018 2. Carbon Black Incident Response Threat Report, Nov. 2018 3. Ponemon Institute, 2018 and 2019 Cost of Data Breach 4. Black Report, Nuix 2017 5. Shape Credential Spill Report 2018 6. Verizon 2019 Data Breach Investigations Report