

TOSHIBA

The essential guide to endpoint and network security

 Knowledge
On Demand



A photograph of three IT professionals in a server room. A woman with long dark hair, wearing a red and white patterned jacket, is pointing at a document. A man with a beard, wearing a grey polo shirt, is looking at the document. Another woman with blonde hair in a ponytail, wearing a black jacket, is looking at a computer monitor. The background shows server racks and blue lighting.

Section 1 | Introduction

Introduction

This guide explores the risks, challenges, and solutions associated with endpoint security, providing actionable insights on how Toshiba Tec's security solutions can safeguard your endpoints and network.

It's challenging out there.

It's no secret that securing every endpoint, enforcing security policies and monitoring activity across your network is critical to protecting your organisation from cyber threats. Cyber criminals are often one step ahead with zero day threats that the industry cannot predict, and it's not always possible to prevent the next attack.

So, it's more important than ever to ensure your organisation is as resilient as possible, and you're ready to apprehend all types of attacks. One thing's for sure – no-one is immune and it could happen at any time.

Laptops, mobile devices, the Internet of Things, and all workplace endpoints including print devices, are potential entry points for security breaches.

So, it's clear that security measures go beyond the office, and need to be considered for all working environments. Remote workers, or home-based employees rely on multiple connected devices, increasing the risk of unauthorised access and data leaks.

And compliance with industry standards such as Cyber Essentials requires you to safeguard your entire IT infrastructure—not just individual devices—to prevent data breaches, operational disruptions, and financial penalties.

Toshiba Tec can help

At Toshiba Tec, we believe security is a business-wide priority. We provide end-to-end protection across all connected devices, helping you build a secure and resilient IT environment.





How we help

We help you enforce security policies, monitor activity, and restrict unauthorised applications across all endpoints, whether on-premise or remote.

Additionally, we secure your data in transit through encrypted communication protocols, such as Internet Printing Protocols (IPP) for print workflows, to protect your sensitive business information.

Beyond endpoint security, document management and workflow integration play a crucial role in maintaining data integrity. We provide advanced access controls, secure scanning, and encrypted storage, ensuring your confidential business information remains protected everywhere.

By embedding security across your workflows, you'll enhance compliance, reduce vulnerabilities, and safeguard operational efficiency.



Section 2 | Print Security

Are your printers your weakest link?

Think twice before you hit print.

Printers are no longer just office peripherals- they are network endpoints that process and store vast amounts of sensitive data. Yet, print security is often overlooked, leaving businesses vulnerable to cyber threats, data breaches, and compliance violations.

Everyday millions of confidential files are produced using multifunctional printers (MFPs). They are capable of processing and storing sensitive data – they are essentially sophisticated network endpoints. Yet, while most organisations secure their IT networks, print security often remains an afterthought, leaving businesses vulnerable to cyber threats, data breaches, and compliance violations. An insecure MFP can expose sensitive information to potential attacks and legal risks if your data is not protected properly.



3.4

£3.4 million was the average cost of a data breach in the UK in 2023 according to an IBM Security Report¹.



161

In 2024, business firewalls encountered more than 161 daily attacks targeting applications such as networked printers².



16%

Just 16% of IT decision makers are completely confident in the security of their print infrastructure³.



50%

Half of businesses (50%) and around a third of charities (32%) reported experiencing some form of cyber security breach or attack in the last 12 months⁴.

¹IBM Report: Soaring Data Breach Disruption Drive Costs to Record Levels

²2024 was the worst year on record for commercial cyber-attacks

³Quocirca Global Print Security Landscape 2023 | Press Release

⁴Cyber security breaches survey 2024 - GOV.UK

Do you have:

- A diverse printer fleet that includes multiple brands and a patchwork of software and drivers?
- Hybrid work environments, where feature-rich MFPs are shared between many users, often in co-working spaces or by employees working remotely, outside of company-controlled locations?
- A fragmented approach to cloud printing that could create security risks around access and authentication?
- Older printers with outdated security features that could weaken multi-layered protection?



If you answered yes to any of these questions, you'll need to include printers as integral parts of your overall IT security framework.

- Invest in modern, secure MFPs with built-in encryption and authentication.
- Consolidate vendors - a single-vendor print fleet ensures consistent security updates and patches.
- Opt for Managed Print Services (MPS) to optimise, secure, and maintain print environments.
- Embrace the cloud - cloud-based printing solutions enhance centralised security enforcement across multiple locations.
- Invest in security solutions that require authentication before printing and enable secure print release.
- Implement role-based access to limit who can print.

We're ready to make it happen.



Secure Managed Print service

Need support? Our Managed Print Service streamlines and secures your entire print environment. By integrating advanced security features—such as remote firmware updates, secure print release, and robust device management—with proactive maintenance and supply management, this service ensures your printing infrastructure is both efficient and secure.

Tailored to meet the specific needs of your organisation, it helps reduce downtime, lower overall costs, and maintain compliance with industry standards, all while providing expert support to keep your print operations running smoothly.

By adopting a Software as a Service (SaaS) print management solution, you can control the entire printing process from the first click to the final output—all within a secure cloud environment.

Cloud Printing

Take printing to the cloud, safely and efficiently.

Transition to a secure, modern, and efficient print environment while ensuring end-to-end encryption across all communication channels. User, billing, and print data remain fully protected, with customer credentials and information strictly separated to prevent unauthorised access.

Need to integrate printers with cloud services like OneDrive and SharePoint? Without proper safeguards, these integrations can expose scanned documents to unauthorised access. However,

Toshiba's Secure Print Release ensures that sensitive documents are printed only when the authorised user is present, eliminating the risk of data leaks. Additionally, tracking and auditing features provide visibility into cloud integrations, helping you maintain compliance and security.

Toshiba offers two robust cloud print solutions, one for cloud enablement and one for cloud print management: **e-BRIDGE Global Print** and **e-FOLLOW.cloud**.





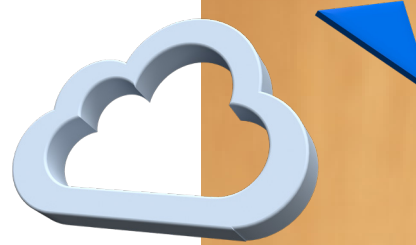
Bridge the gap with e-BRIDGE Global Print

Toshiba's e-BRIDGE Global Print makes it easy to work from anywhere. Employees can send their print jobs directly to your cloud-connected Toshiba MFPs, from any remote location, and then release them directly from any MFP touch panel.

e-BRIDGE Global Print is a completely cloud-native application, so users don't need to know the IP address of a particular printer or whether they're on the same network as the printer they want to use.

All print jobs are encrypted from a user's workstation to the MFP where the job is released and printed. Integration with Google Workspace™ and Microsoft 365® accounts allows for seamless and secure user authentication, protecting sensitive documents from unauthorised access.

Hosted on Microsoft® Azure® and Amazon Web Services™, e-BRIDGE® Global Print offers a reliable and scalable platform for businesses of all sizes and is ideal for organisations with distributed workforces.



Feature-rich cloud print management for flexible working with e-FOLLOW.cloud

Toshiba's e-FOLLOW.cloud is a secure, serverless print management solution designed to support modern, flexible workplaces. It enables users to submit print jobs from anywhere—whether in the office, at home, or on the go—and release them securely at any connected Toshiba multifunction printer. As a cloud-native system, it eliminates the need for local print servers, reducing IT complexity and costs. With end-to-end encryption, it safeguards sensitive information while ensuring compliance with data protection standards.

The solution is scalable for organisations of all sizes and supports mobile and hybrid working environments, allowing seamless integration across multiple locations. Its direct connection with Toshiba MFPs simplifies setup and maintenance, offering a user-friendly and efficient way to manage printing across distributed teams.

e-FOLLOW.cloud not only enhances productivity but also supports sustainability goals by reducing unnecessary print waste through controlled access and pull-print functionality.

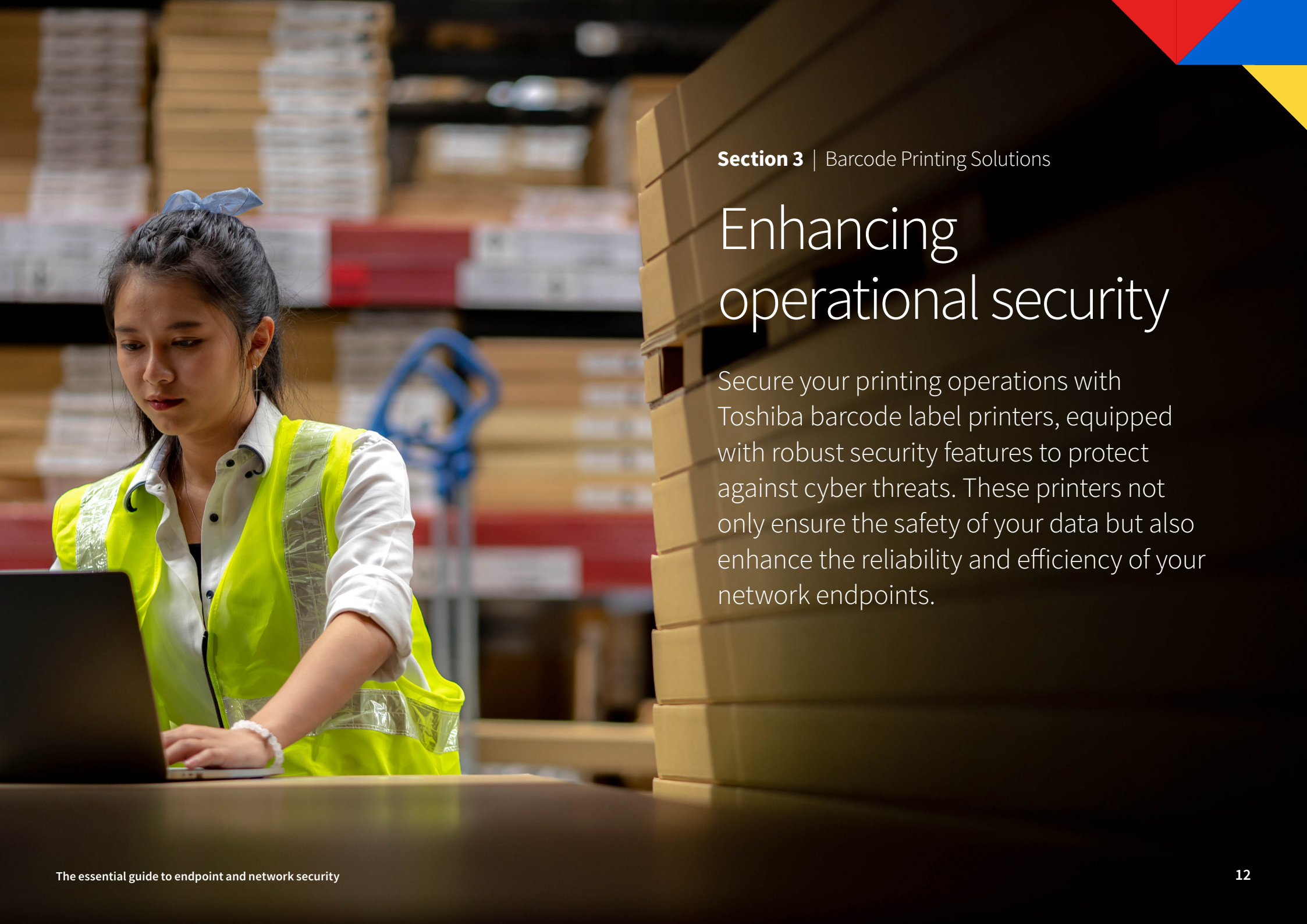


**Virgin Active uses e-FOLLOW.
cloud print management
software for security, efficiency
and data intelligence.**



“Toshiba pulled out all the stops to upgrade our print management solution within a very tight schedule. What we now have is a future-proofed, secure platform, which is easy for staff to use and has allowed us to take the next steps into digitisation. The Toshiba team has been professional and accommodating at every stage in the process.”

**European Head of IT Service Delivery
Virgin Active**



Section 3 | Barcode Printing Solutions

Enhancing operational security

Secure your printing operations with Toshiba barcode label printers, equipped with robust security features to protect against cyber threats. These printers not only ensure the safety of your data but also enhance the reliability and efficiency of your network endpoints.

Ensuring safe and efficient barcode printing solutions

As cyber threats continue to evolve, security is of paramount importance, and every endpoint on a network has the potential to be a vulnerable entry point. Toshiba barcode label printers are built with security in mind and have the latest security standards integrated to ensure secure printing across networks, protecting both data and the printer. These features not only safeguard your operations but also enhance overall efficiency and reliability.



Data Protection:

- Data transmitted between the printer and the server is encrypted using Secure Socket Layer (SSL) / Transport Layer Security (TLS), making it difficult for attackers to intercept and read the information.
- Secure Shell (SSH) allows secure remote access to network devices, ensuring that communications are encrypted and protected from interception.
- Internet Protocol Security (IPsec) encrypts data packets transmitted over the network, ensuring confidentiality.
- Internet Printing Protocol (IPP) offers several security advantages for network printing, including encryption, authentication, access control, and data integrity.
- The IEEE 802.x standard utilises robust encryption methods like WPA3 to secure data transmitted over the network, ensuring confidentiality and protection against eavesdropping. Strong authentication methods, such as 802.1X, require users to authenticate before gaining access to the network.
- SNMPv3 provides robust security features, including encryption, authentication, data integrity, access controls, support for more sophisticated network management tools and remote configuration options and protection against eavesdropping. By providing strong security features SNMPv3 helps comply with various regulatory requirements, such as GDPR, and others, which mandate the protection of sensitive information.

Hardware Protection:

- Several label printers in the range can be PIN/password protected, restricting unauthorised access to the printer's menu and configuration systems.
- For printers on Toshiba's A-BRID platform, embedded apps are whitelisted, preventing unauthorised and non-certified applications from being installed.
- Connection to Toshiba's e-BRIDGE CloudConnect ensures the latest firmware is always installed. When a vulnerability is identified, a software patch can be sent to the printer to fix the issue, reducing the risk of exposure and keeping the hardware secure.





Section 4 | Device Management

Comprehensive security and management

Secure, reliable device management will help you to stay ahead of cyber threats. But how do you ensure the safety of your data while enhancing the efficiency of your networked MFPs, printers, and barcode label printers? Toshiba's cloud-based service is designed to meet these challenges head-on, providing robust security features that protect your operations and streamline your workflow.

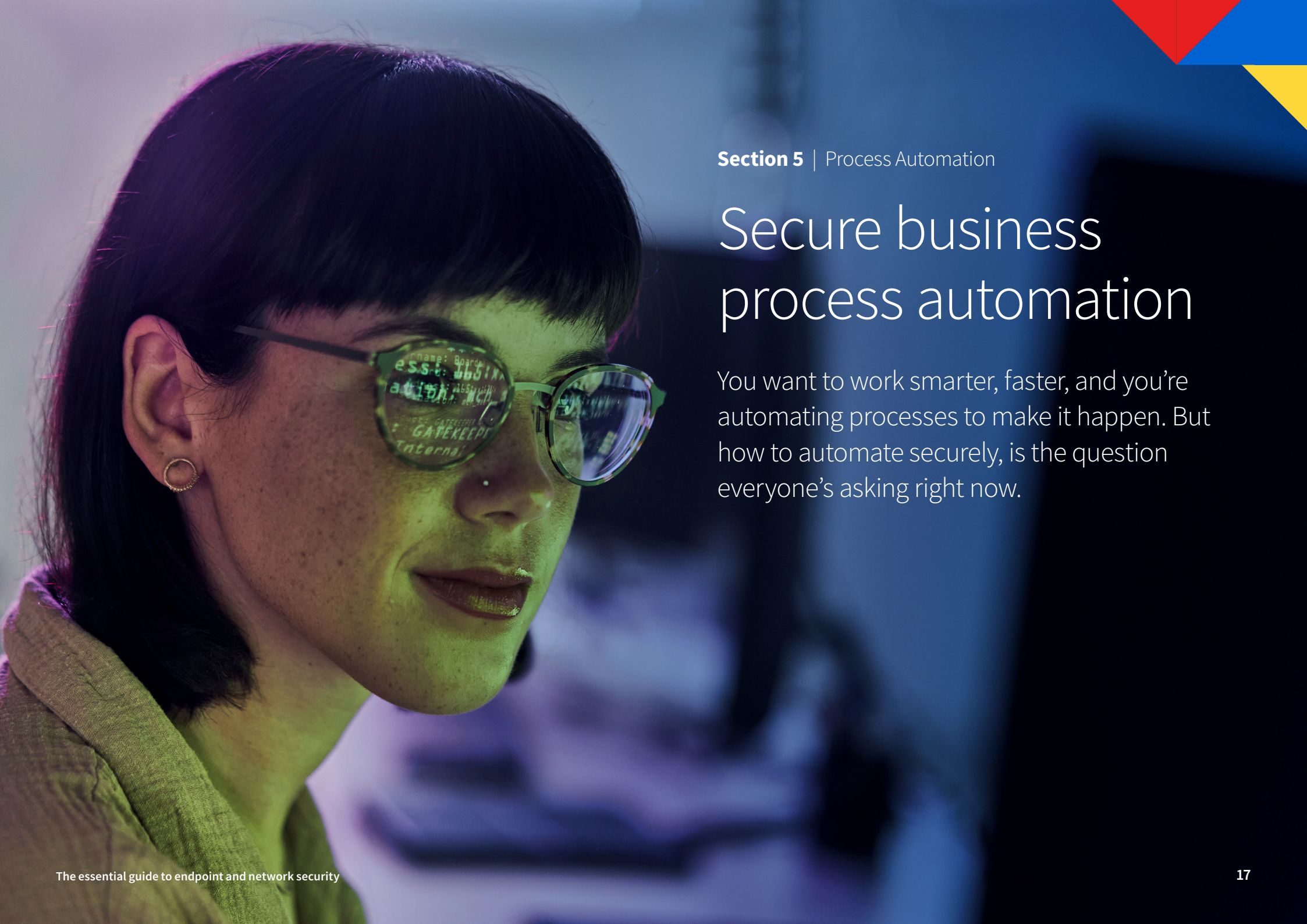
Optimising device management with e-BRIDGE CloudConnect

In today's interconnected world, managing and securing networked devices is crucial for maintaining operational efficiency and protecting sensitive data. Toshiba's e-BRIDGE CloudConnect provides a cloud-based support service that offers comprehensive

security and management for networked MFPs, printers, and barcode label printers. This service securely collects operation data transmitted from your devices over HTTPS/SSL connections, ensuring that only authorised parties can view the data. By leveraging e-BRIDGE CloudConnect, businesses can enhance device uptime, streamline maintenance processes, and ensure the latest firmware updates are always installed.

Key features and benefits:

- **Secure data collection** – Operation data is transmitted securely over HTTPS/SSL connections, ensuring confidentiality and protection against data leaks.
- **Remote diagnostics** – Increases device uptime with proactive status alerts and remote diagnostics, allowing issues to be identified and resolved quickly.
- **Automated maintenance** – Reduces workload with scheduled meter readings, automated supplies delivery, and remote firmware updates.
- **ISO 27001 compliance** – Operates in accordance with the ISO 27001 international standard for information security management, ensuring robust security measures.
- **Server authentication** – Prevents server spoofing and ensures data is transmitted to the correct server, maintaining data integrity and security.
- **Flexible support** – Supports various configurations and authentications, providing adaptable security policies for different business needs.
- **No document data handling** – Handles device operation status information only, ensuring that document data is never leaked.
- **Device security** – Implements and manages device security policies to ensure compliance and protection, while regularly updating installed apps to mitigate vulnerabilities and enhance security.



Section 5 | Process Automation

Secure business process automation

You want to work smarter, faster, and you're automating processes to make it happen. But how to automate securely, is the question everyone's asking right now.

Robust security with smarter business process automation

The challenge is balancing efficiency and security. You want seamless, automated workflows to boost productivity and reduce manual work, but at the same time, you can't compromise security. And as you digitise, you become a bigger target for cyber threats, data breaches, and compliance risks.

It's why we're making business process automation smarter and more secure, so you can work faster, more efficiently, and with total peace of mind.

Whether it's digitising documents, automating workflows, or keeping sensitive data under lock and key, security is built into everything we do. With data encryption, strict user authentication, and real-time monitoring, we can help you stay protected from cyber threats without slowing you down.

Lion Hudson streamline their operations with a complete document management solution.



“We had incredible buy-in from the whole company, as everyone could see that there would be no more time wasted on searching for documents in filing cabinets, lever arch files or in-trays. In addition, we no longer have to think about storing documents in our office, and our data security has improved enormously.”

**Finance Director
Lion Hudson**



How can process automation help?

Toshiba offers a suite of software solutions designed to boost productivity, enhance operational efficiency, improve accuracy, and strengthen security across your organisation.

- Implement robust security measures, including encryption, access controls, two-factor authentication, and detailed audit logs to safeguard data.
- Automate document capture, processing, and distribution using AI to minimise human error and reduce security vulnerabilities.
- Create customisable, rule-based workflows with built-in security features such as time stamps, watermarks, sign-off limits, and structured approval processes.
- Seamlessly integrate with user management systems to ensure only authorised personnel can access and handle documents.
- Centrally monitor directories, email mailboxes, and data streams to maintain secure and efficient data flows.
- Provide real-time visibility into document workflows to support transparency, accountability, and regulatory compliance.
- Tailor security settings to meet organisational needs, including OCR recognition and document format conversion.
- Integrate with existing systems to maintain secure data handling across platforms.
- Offer robust disaster recovery options for reliable data backup and restoration in emergencies.



Data security is a top priority for us

Our devices and services mitigate the risk of complex and evolving threats, meet security requirements, and prevent unauthorised access to protect your data.

Not only do we ensure a high level of protection for your organisation, but we also help you comply with stringent data security requirements and standards, while boosting efficiency.

Plus, our ISO/IEC 27001 certification and regular security audits mean we're always ahead of compliance requirements.

And with our cloud-based solutions like e-BRIDGE CloudConnect, plus AI and IoT-powered automation, you can streamline operations while keeping data safe and sound.

It's all about working smarter, faster, and more securely - without the headaches.

We'll ensure that what's yours stays yours.





Ready for a multi-layered security approach that protects workflows, network integrity, endpoints and sensitive data?

Whether it's through remote updates, encryption, user authentication, or secure disposal solutions, Toshiba Tec helps you prevent threats and stay compliant at every touchpoint.

Don't take chances with your business data. Secure everything, today.

If you're ready to find out more – we're here to help.

Toshiba Tec Germany Imaging Systems GmbH

Carl-Schurz-Str. 7, 41460 Neuss, Germany

+49 2131-1245-0

www.toshibatec.eu

