FUJIFILM
Value from Innovation

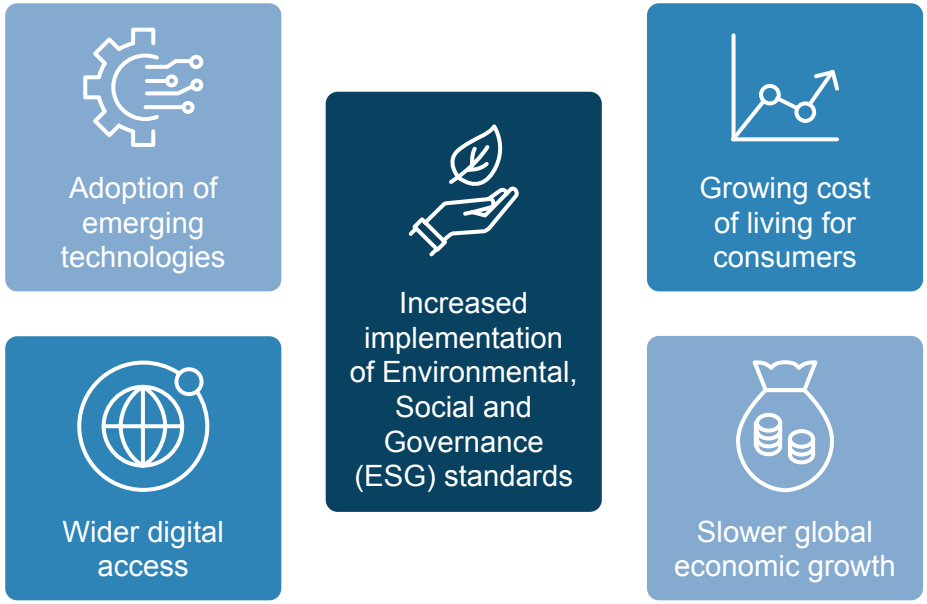
Mitigate the Threat of IT, Data and Print Security Attacks

How Businesses Can Strengthen IT Security Resilience

Transform to Thrive: Digital Transformation for Your Business

In our paper *From Surviving to Thriving: Harness Business Resilience to Build Your Competitive Advantage*, we showed how businesses could remain resilient in a rapidly evolving environment to make their organisations stronger and thrive. Companies with clear and efficient workflow processes and workforce arrangements demonstrated greater resilience through crises.

Businesses worldwide can expect these trends to drive their organisation's transformations from 2023 to 2027.



Businesses that made early strides in embracing digital transformation have witnessed growth rates up to **5 times faster** than their slower-moving counterparts.[1]

Now, it's about being agile.

Resilient and strategic businesses, including large enterprises and small-medium businesses (SMBs), have shown the ability to use digital transformation to empower their hybrid and remote teams, ensure business success and enhance social responsibility.

Many businesses are playing catch-up, some better than others. Today's circumstances provide opportunities for second movers to bridge the gap with industry leaders in technology adoption and innovation culture. They capitalise on lessons from early adopters, accelerating their digitalisation and growth.

As part of building resilience and the right organisational culture mindset, long-term digital transformation means shaping a connected workspace, fostering collaboration in hybrid and remote teams, imagining future jobs through business workflow automation, and enhancing your workforce's skill sets to be innovation-ready.

Discover more insights in this series:

The Workforce of the Future: Streamline Workflows for Smarter Team Productivity

Mitigate the Threat of IT, Data and Print Security Attacks: How Businesses Can Strengthen IT Security Resilience

Transforming Workplaces to Thrive in the Digital Era: Trends and Strategies for Workplace Transformation

Companies that exceeded expectations achieved growth **4 times faster**[2] than those slowest to adopt innovations. This rate is even higher than that of leading companies, demonstrating that you can digitally transform your organisation without sacrificing profitability.

Transform your business in order to thrive – to gain speed and productivity through digital transformation.

FUJIFILM
Value from Innovation

Table of Contents

IT Security: A Growing Concern Among APAC Businesses

Strengthening IT security— ***which involves cybersecurity strategies that safeguard organisational assets, including computers, networks and data, against unauthorised access—*** *is emerging as a top concern for Asia Pacific (APAC) businesses.*

Cyber threats are rapidly evolving, and the consequences of these attacks are intensifying. Beyond just dollars and cents, the actual costs for businesses include data loss, reputational damage and business interruptions.

These trends underline the urgent need for APAC organisations to bolster their IT security capabilities.

Businesses need an effective security strategy. However, building one is a journey, not a destination. It is easy to think of IT security as an initiative that requires large-scale solutions—but even small changes can help strengthen your company's security posture.

In this guide, we will dive into the APAC security threat landscape and highlight top IT security challenges that businesses face. We aim to help companies identify gaps in their existing strategy, so that they can implement the necessary solutions to improve their IT security defences.

The region faces the highest number of cyber threats globally, accounting for **31% of all cybersecurity incidents** remediated worldwide.[3]

In the first quarter of 2023, APAC witnessed the highest year-over-year increase in weekly cyber attacks (1,835 attacks/week).

This figure is **47% higher than the global average** (1,248 attacks/week).[4]

Insights Into the APAC Security Threat Landscape

Backdoors deployment is the top action by cyber attackers, followed by ransomware and MalDocs.[5]

Businesses in Malaysia and the Philippines suffered the most security incidents in the region.[6]

Businesses in Australia were the least likely to have an incident response plan in place, while Hong Kong was the most likely.[7]

Businesses in Singapore were primarily concerned with business interruption.[8]

Top Five Measures Implemented by Businesses in Response to an IT Security Incident[9]

68% Conducting regular training or tabletop exercises

64% Implementing an incident response playbook, plan or policies

62% Having a compromise recovery plan

62% Appointing a data protection officer

62% Engaging cybersecurity specialists on a retainer

Top IT Security Challenges for APAC Businesses

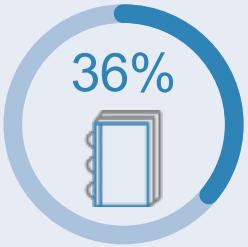
Understanding IT security challenges can save your business from operational disruption, lost revenue and stolen data.

Companies should invest in a comprehensive organisational strategy to cover all aspects of IT security.

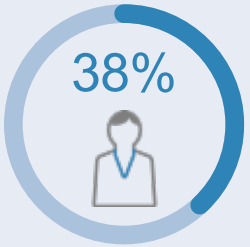
Gain a deeper understanding of critical challenges, so you can identify and plug gaps in your IT security processes.

Overcoming the Misalignment Between Business and IT Security Priorities

When CIOs and business executives don't align on business objectives, it can hinder the implementation of effective security measures. This misalignment has led to insufficient IT security investments.



of APAC organisations did not have an incident response playbook, plan or policies in place in 2022.



did not have an appointed data security officer, or access to cybersecurity specialists on a retainer.[10]

were unsure if their IT security defences are strong enough to combat cyber attackers' new strategies.[11]

Educating Employees in Data Protection

Human error is the number one cause of cloud data breaches.[12] Various factors contribute to human error, primarily opportunity, environment and lack of awareness.[13]

Examples of human errors that result in data breaches include downloading infected software, using weak passwords or compromising IP addresses.

Factors contributing to human error:

Opportunity

The greater the number of opportunities for errors, the more likely mistakes will occur.

Environment

The workplace's physical environment and office culture influence human error. Sometimes, employees know the correct action to take but fail to follow through.

Lack of awareness

Users may simply not know the right actions to take.

Addressing the IT Security Talent Shortage

The global shortage of cybersecurity workers widened by 26.2% to 3.42 million in 2022.[14]

APAC faces the largest talent shortage, reaching a gap of 2.16 million cybersecurity workers.[15]

This shortage can be attributed to factors such as the lack of tertiary education programmes focusing on IT security,[16] misunderstandings about the security industry and the rapid pace at which technology is evolving.[17]

The talent shortage also highlights the importance of finding better ways to protect sensitive data and digital assets.

Addressing Security Challenges in Cloud Adoption

Cloud adoption in APAC is growing rapidly as companies turn to the cloud for their IT needs.

However, shifting to cloud computing is a complex process, and it is crucial to incorporate security right from the beginning. Without an effective strategy for cloud migration, you can be at risk of data breaches, data loss and cloud misconfiguration.

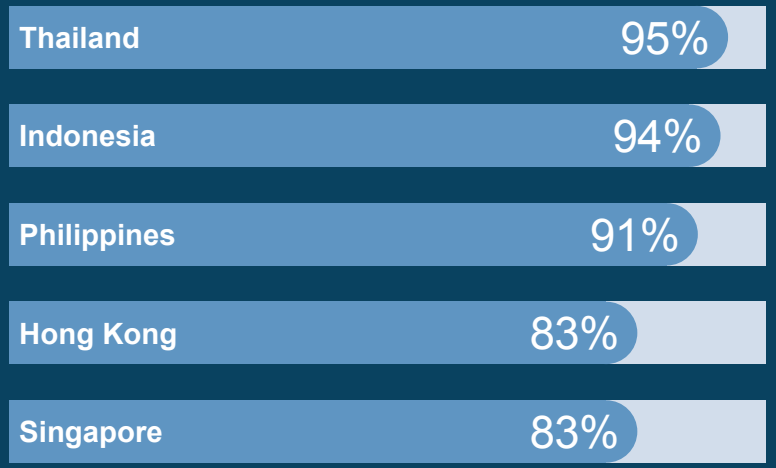
APAC Cloud Adoption Updates

Cloud spending among APAC businesses will reach USD 200 billion by 2024.[18]

Organisations already utilising cloud services are also expected to increase their cloud investment.

Four in five businesses in Asia (84%) are planning a full cloud migration by 2024.

The increase in cloud investment will most likely come from[19]:



Equipping Against Network Decryption

With businesses moving their data and computing to the cloud, security teams must safeguard businesses' digital footprint by using encrypted traffic.

However, cyber attackers can decrypt or expose encrypted messages, passwords and keys, revealing sensitive information and jeopardising systems. With quantum computing in development, this—in the hands of the wrong people—poses a significant threat to companies.

One of the top network security challenges for APAC companies in 2023 is the quantum computing security threat of network decryption.

About 60% of APAC organisations identify network decryption as the greatest concern for quantum computing security threats.[20]

Protecting the Digital Space

The number of connected devices will continue to grow, and as a result, businesses are finding it increasingly challenging to protect them against threats. This is due to:

1. Workforces today have **more connected devices than ever before**, with employees typically using an array of connected devices—including desktops, laptops, smartphones, tablets and multifunction printers—to carry out their day-to-day responsibilities.

2. Connected device adoption amplifies the amount of **data gathered and transmitted among connected devices.** This widens the attack surface available to cyber attackers.

3. **Most connected devices are not designed with security in mind.** They do not have adequate security controls to prevent cyber attacks, such as regular software updates or security patches from manufacturers or vendors.

Mobile security threats:

- Phishing attacks, malicious applications, vulnerable networks, man-in-the-middle (MiTM) attacks[21]

Print security threats:

- **Internal threats:** Unauthorised operations by other users, data breaches arising from careless mistakes
- **External threats:** Software tampering, breach of document data stored on devices, audit log tampering, eavesdropping and tampering of communication data, unauthorised access to admin functions

Securing Your Organisation from IT Threats

Businesses must develop a strong security plan that addresses the identified IT security challenges.

Here are recommendations to protect your organisation from security threats.

Challenges	Recommendations
Overcoming the misalignment between business and IT security priorities	**Establishing cyber resilience in your organisation**
Educating employees in data protection	**Promoting cyber awareness in the workplace**
Addressing the IT security talent shortage	
Addressing security challenges in cloud adoption	**Supporting IT departments by engaging external IT expert services**
Equipping against network decryption	
Protecting the digital space	**Having a security plan for your devices**

Establishing Cyber Resilience in Your Organisation

Cyber resilience refers to an organisation's ability to anticipate, react to and rebound from a cyber attack when it occurs.

You must prioritise cyber resilience due to increasingly sophisticated cyber attacks. While it once took days to hack into systems, malicious activities today can happen within hours. Building integrated and modernised IT security plans and systems that enable businesses to deflect attacks quickly is crucial.[22]

Elements to Establish Cyber Resilience[23]

1

Anticipate

Understand your organisation's assets, vulnerabilities and potential threats.

2

Withstand

Implement systems, processes and tools to protect your data and connected devices.

3

Recover

Timely recovery is important—so ensure you have an incident response plan to minimise the impacts of a security incident.

4

Evolve

Learn from past incidents, and implement the insights you have gained to plug potential gaps in your organisation's IT security measures.

Promoting Cyber Awareness in the Workplace

Even with cutting-edge technology, employees are often the weakest link in an organisation when it comes to IT security.

Implementing cyber awareness training programmes can help you counter this problem. These programmes equip your teams with knowledge of the latest security threats, best practices and industry-specific regulations and compliance requirements.

This minimises the risk of security incidents and promotes adherence to relevant industry regulations—both of which help to boost your security defences.

Workplace Cyber Awareness Best Practices

Make cyber awareness training an organisation-wide effort.

Customise training content to meet the needs of executives and employees.

Avoid a one-and-done approach.

Conduct training regularly to update your teams on the latest threats and attack techniques.

Schedule phishing simulations and testing.

Identify vulnerable areas in your security strategy and help employees recognise and avoid phishes during simulations.

Supporting IT Departments by Engaging External IT Expert Services

In light of new challenges that most business security teams are incapable of handling—such as preparing for wide-scale network decryptions, or ensuring a smooth cloud migration process—equipping IT teams with support from trusted and capable IT expert services will ensure you are steps ahead of cyber attackers.

For example, to combat network decryptions, IT experts can help companies:

- Determine if sensitive data can be easily decrypted
- Constantly update encryption technologies

For cloud migration, IT experts can monitor and guide companies through the migration process. Proper procedures to meet regulations, incident response plans and periodic drills and simulations can be guaranteed.

Your business can eliminate potential issues and breaches with external IT expert services. IT experts conduct frequent assessments and timely upgrades. This allows you to stay compliant with regulations and be proactive instead of reactive when problems arise.

Why APAC Companies Partner with Managed and Professional Security Service Providers[24]:

Increasing data breach incidents within APAC

Increasing cloud deployments due to digital transformation efforts

Overcoming the shortage of IT security professionals

Growing need for external security expertise and insights into compliance

Reducing expenditure on hiring in-house security specialists, while receiving effective security management

Having a Security Plan for Your Devices

Businesses must adopt IT security solutions that offer protection across endpoints—including desktops, laptops, tablets, servers, smartphones and other connected devices.

Additionally, secure your print devices from cyber attacks. Printing is a common and frequent activity across organisations; vast amounts of business information pass through printers.

To build a secure print strategy, you need to:

- Ensure that all devices connected to the organisation's network are secured.
- Ensure that all connected devices within the organisation are held to the same security standards and policies.
- Protect your printer output using solutions offering a secure print release function.
- Utilise managed print services that offer the latest protection against increasingly sophisticated cyber threats. This is ideal for businesses that regularly rely on printing and have a distributed print environment.

Printer Security: Key Features to Implement

Secure Print Release

Secure print release enables print jobs to be held in a secure virtual queue until a final print command is delivered, with the user physically present at the printer. Before a print job is released, employees must authenticate themselves through various methods like using a PIN code, ID card, mobile app or scanning a QR code.

This feature helps you minimise common printer user errors—such as uncollected print jobs, having confidential printouts left unattended at the printer, or incidents where individuals mistakenly collect sensitive documents that do not belong to them.

Secure Mobile Printing

Secure mobile printing enables employees to submit print jobs securely using connected devices and typically includes features like authentication, encryption, user authorisation, logging and auditing.

Secure mobile printing is crucial in certain work environments, such as when an organisation has implemented a hybrid work arrangement, and employees must print from their devices when working offsite.

It is also an essential feature for organisations in the healthcare and finance sectors, as these companies need to meet compliance requirements on document security.

360° Data Security

360° data security encompasses robust measures to ensure protection, which ranges from secure scanning to ceasing unauthorised access, as well as audit trails to monitor devices in real-time.

Key features include one-touch user authentication (which lets you effectively manage your user and print environment), enhanced audit capabilities and end-to-end data encryption via a secure network.

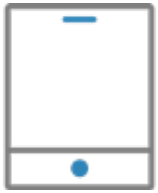
A Checklist to Building Your IT Strategy

Here are our recommendations to building your IT strategy:

Assess your organisation's IT security capabilities

- ☐ Evaluate the skills and expertise of each team member.
- ☐ Evaluate the allocation of resources to the IT security team. Assess whether the budget aligns with the organisation's security needs.
- ☐ Create a plan to address areas of improvement and skill gaps in the team.
- ☐ Look into solutions that can help bolster your organisation's capabilities, such as engaging external IT expert services.

Implement a plan for building cyber resilience



- ☐ Conduct an assessment to identify your organisation's assets, vulnerabilities and potential threats.
- ☐ Outline systems, processes and tools you need to protect your data and connected devices.
- ☐ Establish a well-defined incident response plan. Regularly test and update your plan through tabletop exercises and simulations.
- ☐ Monitor your IT security infrastructure. Review and update your strategy regularly.

Implement a cyber awareness training programme

- ☐ Identify the objectives of the cyber awareness training programme.
- ☐ Prepare content for the training programme.
- ☐ Schedule employee training sessions, ensuring that training materials and sessions are easily accessible to everyone.
- ☐ Monitor, assess and evaluate the training programme's effectiveness.
- ☐ Update your content and training materials regularly, to ensure that the programme is up-to-date with the latest evolvements in the threat landscape.

Implement a plan for your connected devices

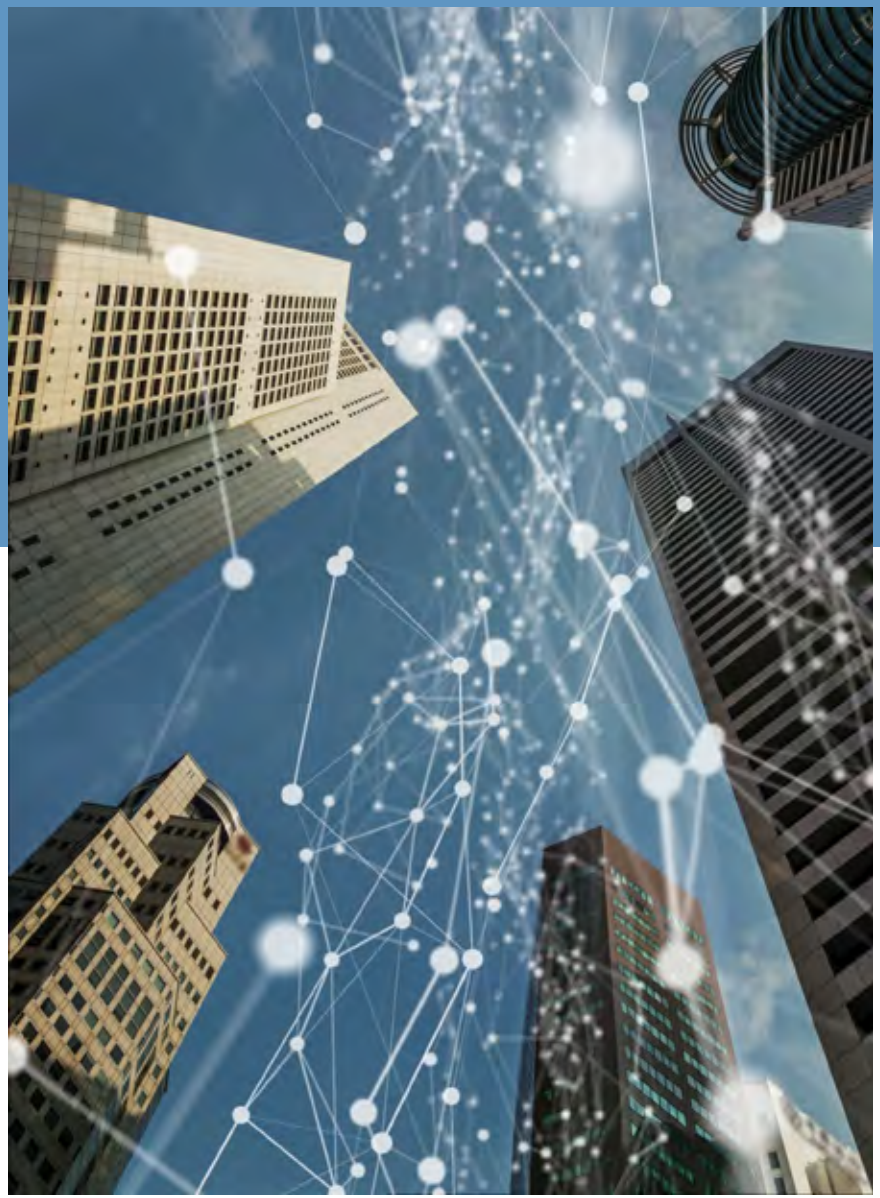
- ☐ Maintain an up-to-date inventory of your organisation's printers and connected devices.
- ☐ Implement user authentication on your print and connected devices to ensure that only authorised persons can access the device.
- ☐ Ensure that the software of all printers and connected devices is up-to-date.
- ☐ Review the security features of each device. Utilise solutions that offer important print security features, like secure print release and secure mobile printing.
- ☐ Leverage managed print services that offer the latest protection against changing print security threats.
- ☐ Ensure that your organisation's cyber awareness training programme covers information on safeguarding your printers and connected devices.

IT Network Protection is Your Top Business Priority

APAC businesses must prioritise IT security due to the escalating global security attacks happening in the region. Protecting networks, data and devices, including printers, is a growing concern for businesses amidst the increasing threats.

To address the dynamic threat landscape effectively, you must stay up-to-date with IT security trends and challenges, and have a flexible plan for implementing robust security solutions. This strategic approach allows you to strengthen your security through ongoing processes and strong IT partnerships.

Count on FUJIFILM Business Innovation as your reliable and knowledgeable IT security partner, providing the right solutions and support for your IT team.



Thrive with FUJIFILM Business Innovation

Our robust suite of digital technology and automation solutions can support your digital transformation.

ApeosWare Management Suite 2 is a print management software that aids in seamless device management, integrated authentication, secure print output, log accounting, document distribution and tracking information leak. It simplifies comprehensive document management, providing immense value to businesses.

IT Expert Services is a comprehensive managed IT support service targeting small and medium organisations. Through IT Expert Services, SMEs (Small and Medium Enterprises) gain access to skilled IT professionals allowing them to focus on driving their business forward.

Managed Security Service is a subscription-based AI-powered cybersecurity solution delivered through qualified cybersecurity expertise with 24/7 support. The solution aims to simplify threat hunting while providing faster and actionable responses, along with continuous monitoring, across different attack surfaces and environments.

MFP (Multi-Funtion Printer) Secure is a secure print solution. It offers important print security features like print-on-demand, helping organisations create a secure print environment, minimise the occurrence of common printer user errors, reduce print waste and lower output costs.

MPS (Managed Print Services) Guardia is a new age managed print services provided by FUJIFILM Business Innovation, that protects businesses against cost overruns, data breaches and productivity loss.

PaperCut is a print management software embedded in printers, photocopiers and multifunction devices (MFDs) to monitor and control an organisation's print output. It helps users minimise waste while experiencing easy and secure printing.

Ysoft is a print management software focused on document capture and 3D print management. Its modular print management solutions offer flexibility, enabling organisations to scale quickly and deploy additional features as their needs grow.

FUJIFILM IWpro is an all-in-one secure platform solution for business digitisation, provide workspace for collaboration, workflow optimisation, efficient document management of metadata and documents, and versatile cloud-based printing capabilities.

Empower your Transformation Journey with FUJIFILM Business Innovation

With our solutions and expertise, your organisation can take the next step for lasting transformation. Discover what our valued customers say about their partnership with FUJIFILM Business Innovation.

Through our customer surveys, we've gained some incredible insights:

96%

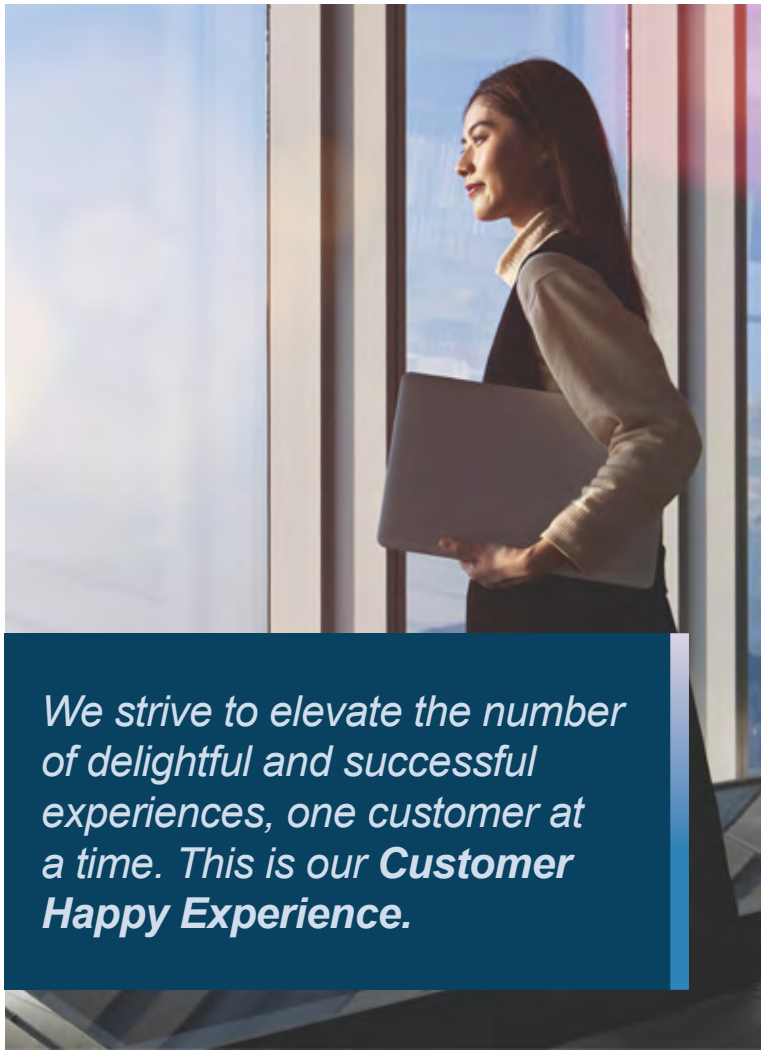
of our customers find doing business with FUJIFILM Business Innovation a breeze

98%

of our customers believe we are the ideal innovative partner to cater to their every need

97%

of our customers would gladly recommend FUJIFILM Business Innovation for all their business requirements



FUJIFILM
Value from Innovation

Let us help you strengthen your IT security.

As cyber threats grow in scale and sophistication, organisations must prioritise IT security. With FUJIFILM Business Innovation, you will be equipped with robust solutions to help you build up your company's cyber defences.

As a customer-centric organisation, we take great pride in creating exceptional experiences for our partners. We engage in close communication with our customers, so that we can implement the right solutions that are set to work for you.

At FUJIFILM Business Innovation, we're here for you: a partner in navigating the rapidly changing IT security landscape. We will help you unlock the full potential of digital transformation while ensuring that your organisation is safeguarded from security threats.

Get ready and stay ready for the future. Contact FUJIFILM Business Innovation.

References

1,2. Accenture, Scaling Enterprise Digital Transformation, August 2021

3. IBM, IBM Security X-Force Threat Intelligence Index 2023, March 2023

4. Check Point Research, Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most, April 2023

5,6,7. Kroll, State of Incident Response: APAC, October 2022

8. IBM, IBM Security X-Force Threat Intelligence Index 2023, March 2023

9,10. Kroll, State of Incident Response: APAC, October 2022

11. EY, Global Information Security Survey, July 2021

12. Thales, 2023 Thales Global Data Threat Report, June 2023

13. Usecure, The Role of Human Error in Successful Cyber Security Breaches, June 2022

14,15. ISC2, Revealing New Opportunities for the Cybersecurity Workforce, October 2022.

16. Deloitte, Finding cybersecurity talent in an altered world, February 2023

17. Advantis Global, The Cybersecurity Talent Shortage: Understanding the Urgency and Impact, July 2023

18. Boston Consulting Group and Cisco, The Future of Cloud in Asia Pacific, August 2021

19. Alibaba Cloud, A Majority of Asia Businesses Expect to Increase Cloud Investment in 2023, March 2023

20. Thales, 2023 Thales Global Data Threat Report, June 2023

21. Tech Target, Top 4 mobile security threats and challenges for businesses, May 2021

22. CNBC, Palo Alto Networks CEO warns companies need modern, integrated cybersecurity: 'The bad actors are moving faster', August 2023

23. IDC, Leadership in a Changing Digital World: Five Mandates, April 2023

24. Frost & Sullivan, Asia-Pacific (APAC) Managed and Professional Security Services Market: The Shortage of Cybersecurity Professionals is Driving MSS and PSS' Future Growth Potential, November 2022