Security That Empowers the Adaptive Workplace

Reimagine your adaptive workplace security strategy with solutions from Fujitsu

shaping tomorrow with you

Microsoft | FUJITSU

Reimagine a Way Forward with Peace-Of-Mind Security

One of the biggest challenges facing forward-thinking organizations during the recent pandemic has been finding digital alternatives to physical processes, as fast as possible. The adaptive workplace, with employees staying connected and productive whether they work in the office, at home, or while mobile is a perfect example of this.

Strong cyber security is essential for anywhere work. Today's security solutions use automation, artificial intelligence, and machine learning technologies to process the massive and growing amount of security alerts, then identify risks and respond to threats. These solutions protect applications and data wherever they are hosted, and secure digital identities and devices wherever they are used.

Your organization needs a strong, effective security operation to support an adaptive workplace and keep up with more sophisticated threats. Technology can help streamline security operations, but the requirements of designing, implementing, and managing cloud applications and security measures can be overwhelming. That's when a partner can bring clarity and guidance for the needed improvements and technology opportunities unique to your organization.

Fujitsu can help transform your cyber security program to give your business the resilience it needs during these uncertain times, when it's hard to predict what disruptions lie ahead. Read on to see how we can help you solve five pressing security challenges.

Challenge 1:
Knowing Your Risks

"Fujitsu was the clear choice based on service and digital transformation capabilities that played a central role in its approach. Working in competitive markets, every pound we spend needs to deliver cost efficiency and value for money."

Darren Miles
VP Global Infrastructure & Operations
Centrica

Needing to future-proof themselves in these uncertain times, most organizations are looking to become more flexible and secure going forward. Traditional security focused on protecting the network perimeter, but with more remote workers, the network edge is now everywhere. This brings a new focus on protecting digital identities and managing access by users and devices.

As security threats become pervasive and harder to detect by traditional solutions, it's essential to maintain an up-to-date understanding of your risk exposure. Fujitsu helps you identify, assess, and address these risks from the perspectives of business, technical, and compliance requirements.

Fujitsu Security Consulting Services bring expert insight to the unique security challenges, needs, and opportunities of your organization. A consulting engagement can also identify requirements and gaps in your infrastructure, configurations, and operational practices that create security risks or limit your ability to comply with regulatory requirements.

Using the agreed business requirements as a starting point, technical experts from **Fujitsu Security Professional Services** will assess security gaps and develop an improvement plan. Solutions recommended in this plan may include **Microsoft Security Center** and **Microsoft Compliance Center** for managing infrastructure resources and **Microsoft Azure Active Directory** conditional access features to better secure device connections.

Fujitsu Advantages:

- Independent advice that delivers unrivaled expertise, proven methodologies, and extensive industry experience.

- Embracing the new flexible ways of working, we provide insights for managing risk and compliance demands effectively

- Expert technical services for design, installation, testing, and integration of security controls that put Fujitsu consulting advice into action.

Microsoft Solutions Spotlight

Microsoft 365 Security Center
Designed to help security teams better manage and protect their organization, Microsoft 365 Security Center is a specialized security workspace. It provides a view of security health; tools to configure devices, user identities, and applications; and alerts for suspicious activity.

Microsoft Compliance Manager
Included in a Microsoft 365 subscription, Microsoft Compliance Manager helps you manage regulatory compliance activities for Microsoft cloud services.

Microsoft Azure Active Directory
The conditional access capabilities in Microsoft Azure Active Directory apply a zero-trust model to control access by employees, partners, and customers. This tool verifies user identity, device configuration, and other risk signals before allowing access to your apps and data.

Challenge 2:
Staying ahead of the next threat

"Fujitsu has put robust security controls in place to ensure Libraries NI is protected from cyber threats which have become more prevalent and malicious. This multi-layered approach includes endpoint protection, configuration management, firewall security, traffic flow and data segregation, web and email security, certificate services and operational security management. All of this plays a fundamental role, with security by default and privacy by design underpinning the Libraries NI solution."

Desi Curry
Head of ICU and ICT
Libraries NI

Organizations want to feel more secure, more united and more prepared to deal with whatever disruption comes next. Keeping up with new threats is an essential defense for business revenues and operations.

Fujitsu Managed Security Services offer 24/7 real-time monitoring to identify potential security risks, negate their impact, then prevent further attacks. These services are delivered to Fujitsu customers from 9 security operation centers (SOCs) around the world.

Fujitsu also operates two **Advanced Threat Centers** that use primary threat research, enhanced analytics, and contextual intelligence to identify emerging (zero-day) threats specific to an industry or geographic area. These centers apply security orchestration, automation, and response (SOAR) tools for processing and responding to routine security alerts. And for a breach or high-impact threat, an emergency response team works with customers on mitigation and recovery efforts.

Fujitsu security intelligence is enhanced by data generated by the Microsoft Intelligent Security Graph and Microsoft 365 security alerts. Our security teams use **Microsoft Defender ATP** and other Microsoft security technologies to process, analyze, and extract data into useful intelligence. This advanced level of threat intelligence helps our customers move to proactive security management and respond with greater speed and effectiveness to emerging threats.

Fujitsu Advantages:

- Enhanced visibility and capabilities for predictive cyber security monitoring and threat detection.

- Intelligence-led security operations and practices that leverage advanced technologies.

- Comprehensive services for security consulting, design, implementation, and support of a security solution tailored for your business.
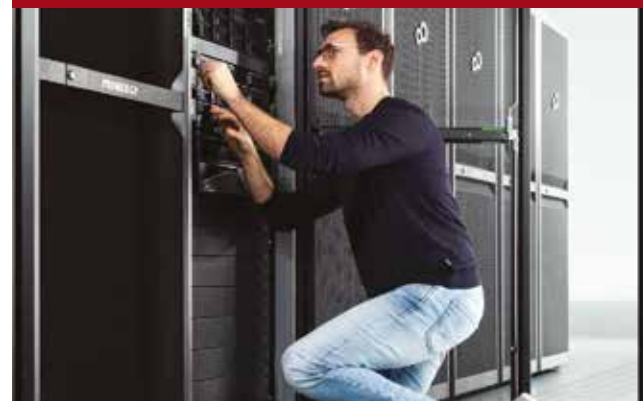
Microsoft Solutions Spotlight

Microsoft Intelligent Security Graph
The Microsoft Intelligent Security Graph collects millions of threat indicators worldwide, then provides them as intelligence for security analytics. Microsoft applications and services use this intelligence to deliver unparalleled threat protection and detection.

Microsoft Defender ATP
In a single platform, Microsoft Defender Advanced Threat Protection (ATP) provides preventative protection, post-breach detection, automated investigation, and response to security threats. The solution is especially useful for detecting zero-day threats.

Challenge 3:
Reimagining your Security Operations

"Fujitsu worked tirelessly to create a robust Azure environment to host the Data Science Workspace, developed by a local Finnish partner, Bitfactor. Given the sensitive and confidential nature of much of the data, **security was a paramount concern**; Fujitsu was able to incorporate the existing on-premise multi-factor authentication and firewalls into the cloud solution to **minimize risk, ensure data privacy and protect corporate IP**

Outi Anttila
Head of Core Services
Orion Corporation

A strong security program requires ongoing investment in operations resources, especially skilled and knowledgeable staff. Yet business leaders will want assurance that you're maximizing investment value, especially for expenditures made to keep up with new technologies and business change.

Automation is a powerful way to streamline internal security operations, increase visibility of security threats and responses, and manage security data for decision-making and audit purposes. Getting the most benefit from automation requires making the best use of technology in your security operations. To help our customers optimize their use of automation, Fujitsu offers custom playbooks that leverage the automation capabilities built into Microsoft solutions.

Given the demands of security today, and the new ways of working that have resulted from the pandemic, your business may be considering whether to outsource all or selected security operations. In this case,

Fujitsu Managed Security Services provide a 24/7 operation tailored to your requirements, helping to ensure business continuity while mitigating threats using the latest cyber intelligence. Our focused services offer protection across core security operations, including identity and access management, infrastructure protection, data protection, and threat and vulnerability management. We also understand that having the right IT is fundamental for businesses looking to meet changing customer and employee expectations.

Fujitsu Advantages:

- Intelligence-led security operations, enabled by advanced tools and in-depth expertise.

- Multiple levels of managed services for outsourcing aligned to your operational needs and preferences.

- Flexible technologies designed to enable the new ways of working

Microsoft Solutions Spotlight

Microsoft Automation Playbooks
Playbooks allow you to launch a predefined response to security alerts. This automation can speed threat identification and response, and simplify enforcement of governance policies.

Challenge 4:
Using the Cloud Securely

Cloud applications and data sharing have become essential tools for supporting employees working from home during the COVID-19 pandemic. But the move to cloud by many businesses was already well underway and it will only increase in the future.

Greater use of cloud brings security concerns and potential risk in two areas. The first is maintaining compliance with the growing number and reach of regulations for data storage and protection. To help your compliance posture, Fujitsu offers consulting with **Microsoft Compliance Center** as well as **customized security and compliance workshops** based on Microsoft curriculum.

Second is preventing data loss through shadow IT, especially the unauthorized use of cloud services and applications. The challenge is to detect shadow IT and prevent data from inappropriate storage and sharing. Our **Security Professional Services** use the **Microsoft Cloud Application Security** solution to identify all cloud applications used by your

employees. The solution can also apply risk ratings to cloud applications in use and verify that enterprise data has appropriate protections when stored in the cloud.

Fujitsu Advantages:

- Confidence and insights to manage risk and compliance demands effectively.

- Improvements in overall protection levels and minimized risk of cyber attack.

- Access to the latest industry-specific security insights, controls, and technologies.

- Support provided to help make resilience a reality, despite the uncertain future.

Microsoft Solutions Spotlight

Microsoft Cloud Application Security (MCAS)
MCAS provides rich visibility, control over data travel, real-time access policies, and sophisticated analytics to identify and combat cyber threats across your cloud services.

Challenge 5:
Security prepared for anything

To achieve higher levels of security maturity and protection, **Van Oord** selected Fujitsu to build enhanced security measures into its global business, enabling the company to unlock their potential through compliancy. Fujitsu implemented a comprehensive portfolio of security solutions including security consulting, managed security solutions, continuous vulnerability management, and Security Information and Event Management as a Service (SIEMaaS).

The sheer volume of security incidents means that indicators of compromise (IOC) can go undetected resulting in prolonged unauthorized system access and the potential for further damaging activities. This experience points to a common challenge: You can't secure what you can't see.

Fujitsu offers options to help your organization avoid this security gap. Our **Professional Security Services** can map Microsoft 365 capabilities to your defined requirements, then ensure that you have a clear view of the security controls being used through the use of a requirements traceability matrix. If you are utilizing our **Managed Security Services**, Fujitsu staff will use tools such as **Microsoft Azure Sentinel** to monitor your security posture as well as detect and respond to risks.

Choosing the right security solutions and keeping them up-to-date is an ongoing effort. And it's an effort that becomes more complex as business activity becomes more digital and security threats grow in velocity and sophistication.

To help our customers stay ahead, Fujitsu operates a **Security Center of Excellence** that receives early exposure to new Microsoft security capabilities. The center advises customers on how to use new Microsoft features and technologies to best advantage.

Fujitsu Advantages:

- Expert services that accelerate and maximize the value gained from your security investments.

- Optimized security spending with expert insights about new technologies.

- A single partner to manage infrastructure and cloud services for both Microsoft 365 and security solutions.

- Technology that helps to make employees and customers feel more comfortable in the 'new world'.

Microsoft Solutions Spotlight

Microsoft Azure Sentinel
Microsoft Azure Sentinel provides a cloud-native solution for security information and event management (SIEM). It collects and logs security data across all users, devices, applications and infrastructure, both on-premises and in multiple clouds.

The Strength of
Fujitsu and Microsoft

Fujitsu is a **Microsoft Gold Azure Managed Service Provider** (MSP) partner and works with customers to design, implement, and manage security solutions based on Microsoft technologies. Our employees hold Microsoft and security certifications for multiple capabilities, including over 100 security engineers certified on Azure (AZ500) and Microsoft 365 (MS500).

These strengths allow us to bring intelligence-led security solutions and services to business and public sector organizations worldwide. This is particularly important at the current time as we explore new ways of working and look for increased resilience to instil a fresh sense of confidence in our people and our customers.

About Microsoft
Microsoft (Nasdaq "MSFT" @microsoft) enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more. www.microsoft.com

Learn how Fujitsu can help your business gain value from advanced security services and Microsoft solutions: https://www.fujitsu.com/global/themes/security/

■ Microsoft | FUJITSU