Fujitsu on Cybersecurity

October 2025

Overview: Securing the Digital Future

- For enterprises, cybersecurity is a defining challenge of the digital era. It is the foundation for business resilience, customer trust and sustainable growth. Chief Information Security Officers (CISOs) face an unenviable reality of rising threats, increasing regulatory demands, and a mandate to do more with less. The pressure is relentless, and the margin for error is thin.
- Fujitsu offers global scale and expertise in defending enterprises, with 1,400 dedicated security professionals and over 500 analysts operating across 12 global Security Operations Centers (SOCs) and five Global Delivery Centers (GDCs).
- Fujitsu's mission is to provide integrated resilience, delivering tailored, end-to-end security solutions that enable businesses to operate with confidence and integrity, allowing them to innovate, grow, and build trust in a digital society.
- Deep integration capabilities differentiate Fujitsu in a crowded field. Fujitsu's security services are woven into the fabric of its IT outsourcing, cloud, workplace and industry solutions. Customers gain the assurance of end-to-end responsibility for securing their entire technology stack. This integrated, intelligence-led approach is the foundation of Fujitsu Cybersecurity.

Industry Trends in Brief

- Multiple factors in today's interconnected world have created a vastly expanded and complex attack surface, including the acceleration of digital transformation, the shift to hybrid workforces and the rapid adoption of cloud services.
- Highly motivated threat actors seeking financial gain or geopolitical advantage are targeting organizations in a landscape defined by escalating compliance demands and a persistent shortage of skilled cybersecurity professionals. A reactive, siloed approach to security is no longer sufficient: A more collaborative, cohesive, and integrated security posture is essential for survival and growth.
- **Key challenges**:
    1. **Platform Consolidation and Simplification:** Enterprises face pressure to streamline complex security stacks and reduce technical debt. Today, many organizations utilize dozens of point tools, which is inefficient and creates gaps. Forward-thinking organizations are moving toward platform consolidation, reducing a sprawl of technologies into integrated solutions that cover enterprise needs. This shift makes integration easier, boosts resilience and cuts costs while providing CISOs with clearer visibility and control over their environments.
    2. **Continuous Threat Exposure Management (CTEM):** Traditional vulnerability management is giving way to a more strategic approach: Continuous Threat Exposure Management. This moves beyond patching lists of vulnerabilities to understanding which exposures matter most to business operations. By continually assessing attack surfaces and prioritizing mitigations, organizations can focus finite

resources on the risks that truly affect resilience, making CTEM an emerging best practice for CISOs worldwide.

3. **Security as a Board-Level Risk:** Cybersecurity has evolved from an IT issue to a boardroom imperative. High-profile breaches, regulatory scrutiny and the financial impact of downtime and data loss have made security inseparable from enterprise risk management. Boards increasingly expect CISOs to articulate risk in business terms, aligning investments with organizational resilience and reputation. This trend reinforces the need for security partners who can bridge technical expertise with strategic business outcomes.
4. **AI-Enhanced Cyber Defense:** The rapid integration of artificial intelligence into security operations is transforming how threats are detected and neutralized. AI can identify patterns and anomalies across massive datasets at speeds that are impossible for human analysts, enabling faster and more accurate detection of sophisticated attacks. From automated playbooks to predictive analytics, AI is helping security teams stay ahead of adversaries, while also alleviating the industry-wide skills shortage.

Fujitsu Cybersecurity: Global Capability and Expertise

Fujitsu is a leading global provider of managed security services, system integration, and security consulting. Its approach is based on extensive expertise, worldwide reach and a strong partner network, aimed at protecting the entire technology stack for Fujitsu clients across multiple critical sectors.

People are a core strength: A passionate and dedicated global team delivers Fujitsu's services, comprising over 1,400 security professionals, including more than 500 analysts, working within a worldwide network of Security Operations Centers (SOCs). This team features a diverse mix of consultants, architects, designers, development engineers and security managers, bringing together the industry's best expertise.

Fujitsu is committed to nurturing talent through graduate programs, apprenticeships, and re-skilling initiatives. In addition to dedicated security specialists, thousands of network and cloud architects also incorporate security into their roles, ensuring a security-first mindset is embedded across all Fujitsu services.

Global Delivery, Local Presence: Fujitsu's global security operations are supported by a network of 12 regional SOCs and five Global Delivery Centers (GDCs). Fujitsu provides 24/7 monitoring and response, ensuring constant vigilance for clients. SOCs are strategically located across the Americas (USA, Trinidad), APAC (Australia, New Zealand, Singapore, Thailand), Japan, and Europe (Finland, Portugal, Spain, Sweden, UK), and GDCs in Poland, India, Costa Rica, Portugal and the Philippines offer global support. This structure enables Fujitsu to deliver flexible models – local, blended, or fully offshore –tailored to meet specific customer needs regarding compliance, culture, and operations.

A Legacy of Trust and Experience: Fujitsu Cybersecurity services are supported by over 40 years of security engineering expertise. Fujitsu currently handles more than 100 security projects for leading organizations worldwide, including flagship clients such as the UK Government and major financial institutions like Santander and NatWest. This broad experience gives Fujitsu valuable insights into the complex threat environments and regulatory requirements of sectors facing significant risks, including the public sector, financial services, manufacturing, utilities, and healthcare.

A Comprehensive, Intelligence-Led Portfolio

Fujitsu provides strategic guidance and specialized capabilities at every stage of the cyber resilience journey, built around the core principles of **Identify, Protect, Detect, Respond and Recover**. The value proposition focuses on Fujitsu's ability to safeguard customer data, identify threats and resolve incidents before they affect customers' businesses.

- **Managed Security Services (MSS)**: Fujitsu's flagship managed security services provide continuous, expert-led security operations to defend against evolving threats.

- **Managed Extended Detection and Response (M/XDR)**: A comprehensive and centralized view of security events across an organization's entire IT estate, from endpoints to cloud environments. By correlating intelligence from multiple sources, critical threats do not go undetected. Key benefits include increased visibility, optimized threat intelligence, automated deployment for rapid setup, and swift response capabilities to minimize the impact of an attack.

- **24/7 SOC Services**: SOCs provide round-the-clock services, including Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), vulnerability management, and threat intelligence. Fujitsu's Computer Security Incident Response Teams (CSIRT) effectively manage and remediate incidents.

Regarding strategic security consulting and integration, Fujitsu collaborates closely with clients to establish robust security foundations and refine their security posture over time.

- **Security Consultancy**: Trained experts provide strategic guidance on everything from Governance, Risk, and Compliance (GRC) and security strategy to specialized areas like cloud and Operational Technology (OT) security.

- **Continuous Threat Exposure Management (CTEM)**: Aligning with industry best practices, Fujitsu helps organizations shift from a reactive focus on vulnerabilities to a proactive focus on managing exposure. This approach frees up resources, aligns IT and security teams, and provides clear answers to the question: "Where are we most vulnerable?".

- **Identity and Access Management (IAM) & Data Protection**: Fujitsu implements solutions to protect critical data and ensure that only authorized users have access to sensitive systems and information.

Industry-Aligned Security: Securing Operational Technology (OT)

The convergence of Information Technology and Operational Technology presents a significant challenge, particularly for manufacturing, utilities, and other industrial sectors. These two fields have traditionally functioned with different approaches, goals, and technologies. IT focuses on data confidentiality, while OT emphasizes the safety, availability, and resilience of physical production processes.

Thanks to its manufacturing heritage, Fujitsu has a deep understanding of what production entails and is uniquely positioned to bridge this cultural and technological gap. This allows customers to confidently digitize production, with Fujitsu supporting them throughout their entire OT security journey:

- OT Cyber Assessments provide visibility of OT assets and their vulnerabilities through discovery and risk profiling. A case in point is Fujitsu's work with a primary packaging supplier for Amazon, where an audit revealed that 30% of the customer's OT assets had high-severity vulnerabilities. Consequently, Fujitsu implemented action plans.

- OT Transformation implements foundational controls, including IT/OT network segregation, secure remote access and the establishment of a cyber policy.

- OT Managed Monitoring provides 24/7 monitoring of the OT network, delivering contextualized alerts on relevant security events.

Fujitsu OT security services are a key enabler of wider digital transformation, helping clients achieve business objectives such as improved Overall Equipment Effectiveness (OEE), compliance, and competitiveness. For example, for a large water and sewerage company, Fujitsu's security and edge services are projected to deliver 25% cost savings compared to traditional solutions, while ensuring regulatory compliance.

The Critical Difference: Why Partner with Fujitsu?

Fujitsu is distinguished by its approach to delivering services and the unique value it brings to partnerships.

- **Integrated End-to-End Capability**: Instead of being an add-on, security is integrated into all infrastructure, workplace, and application services. This provides clients with a seamless, end-to-end capability and a single point of accountability for their entire technology stack, offering a key advantage over pure-play security vendors.

- **Intelligence-Led Approach**: Combines top intelligence tools, deep customer insights, and industry-leading expertise to recommend and implement solutions precisely tailored to clients' needs.

- **Powerful Partner Ecosystem**: Fujitsu maintains strong strategic partnerships with leading technology companies, including Microsoft, ServiceNow and Palo Alto Networks. Fujitsu's role goes beyond reselling technology to serve as an integration and management partner. Fujitsu develops the necessary processes, personnel and organizational structures around the tools that customers have already invested in, ensuring they gain maximum value.

- **Customized and adaptable solutions**: Security is not a one-size-fits-all approach. Fujitsu services are tailored to meet the evolving needs of customers, offering flexible consumption models and delivery options that cater to their specific requirements.

The Fujitsu approach focuses on delivering tangible business results: reducing risk, ensuring compliance, and enabling secure innovation and growth. By integrating security from the ground up, Fujitsu helps its customers build trust, allowing them to pursue their strategic goals with confidence.

Fujitsu quotes – John Swanson, Global Security Portfolio Lead, Uvance, at Fujitsu

- "For enterprises, cybersecurity is a defining challenge of the digital era. It is the foundation for business resilience, customer trust and sustainable growth."

- "A reactive, siloed approach to security is no longer sufficient. A more collaborative, cohesive, and integrated security posture is essential for survival and growth."

- "Fujitsu's mission is to provide integrated resilience, delivering tailored, end-to-end security solutions that enable businesses to operate with confidence and integrity, allowing them to innovate, grow, and build trust in a digital society."

Reference customers

- **Public sector (City of Helsinki)**: Fujitsu is enabling transformation for the City of Helsinki in Finland in transitioning from a reactive to a proactive digital city by centralizing ICT infrastructure and services, enhancing cybersecurity, and enabling predictive and personalized digital services for residents and employees.
- **Energy & Utilities**: Fujitsu's security and edge services are projected to deliver 25% cost savings compared to traditional solutions to a large water company, while ensuring regulatory compliance.
- **Financial services**: Fujitsu provides cybersecurity consulting to a large bank, focusing on standardized oversight of security controls to deliver unified assurance, regulatory compliance and continuous resilience improvement for one of Europe's largest banks.
- **Manufacturing**: Fujitsu's comprehensive transformation services for a globally recognized automotive manufacturer include alert optimization, strategic advisory, SOAR automation, RBVM methodology, centralized CISO reporting, benchmarking and scalable security solutions.
- **Construction (RPM International)**: For this global leader in specialty coatings, sealants and building materials, Fujitsu implemented improved visibility to secure digital operations, protect business and customer data, maximize uptime, support regulatory compliance and help avoid supply chain disruptions as IT and OT systems converged. **Mark Rankin, Vice President of Global Systems at RPM International Inc.,** says: "We chose Fujitsu to do an OT assessment for RPM because of their experience within our industry. Their service is based on a proven methodology supported by OT discovery and analysis technology, to give deep and actionable insights."

