Media Backgrounder
Enterprise and Cyber Security

October 2020

The challenges and opportunities for next generation security

Driven by three-Cs – customers, competition and compliance – organizations globally are reassessing their business processes. Digital transformation is sweeping through all sectors, helping create more efficient ways of working and enabling insights from mountains of data. Utilizing new and innovative tools and technologies, organizations are creating new business processes, disrupting existing ways of doing business and creating new markets. But this new level of interconnectedness also creates new security challenges. Data is everywhere, and as companies increasingly join wider ecosystems and forge direct links to the world around them, they also open up potential new security vulnerabilities.

Considering appropriate security measures and mitigating risks right from the start is essential, as it is no longer a question of "if" a business will be hacked in some way, but "when" and "how". Cyber-attacks are the highest technological risk facing the world, according to the World Economic Forum, with $5.2 trillion in global value in danger up until 2023.

Alongside breaches, organizations are also at risk from other incidents such as distributed denial of service (DDoS) attacks, which can effectively knock a business off the internet – and therefore make it unable to do business. Despite the fact that breaches and DDoS attacks happen almost daily, many organizations are still unaware of the full extent of the risks they face, lack a robust security strategy or do not even have any current security breach readiness. The stakes are high and include damage to brand, reputation and stock value, the loss of competitive advantage through trade secrets being exposed, and fines for regulatory compliance violations. Often the cause of breaches is close to home: with 90% of cybersecurity issues originating from human error[1], organizations need to strengthen the cyber security culture and awareness of cyber threats. The challenge is only getting bigger. Emergency responses to COVID-19 in 2020 meant, from one day to the next, employees had to work from home, posing a different, more complex set of challenges that had to be addressed by cyber security. Scale too just gets bigger all the time. By 2025 there will be 41.6 Bn devices connected IoT (Internet of Things) devices, according to analyst firm IDC. And compounding the threat, there is a critical global shortage of the necessary cyber-skills to stem the tide of data breaches. The scale of the crisis was recently predicted to reach 1.8 million positions in 2022 by *(ISC)*[2], an international, non-profit membership association for information security leaders. "The massive worldwide shortage not only places organizations affected by the shortage at higher risk of cyber-attack," says *(ISC)*[2], "but also affects job satisfaction of current cyber security staff." This is because highly qualified staff are having to perform repetitive routine tasks that are essential for getting the basics right, but this is not satisfying work for them.

Multi-cloud Security: The main vehicle for digital transformation

Until relatively recently, many Chief Information Security Officers (CISOs) believed that the challenge of cyber security would only be intensified by the trend towards hybrid IT and multi-vendor cloud, which has now become the norm for a growing majority of organizations. However, in most cases, experience has contradicted those early concerns about the security of cloud environments. Recent research conducted for Fujitsu by analyst group Pierre Audoin Consultants (PAC) found that seven in 10 organizations operating a mix of on-premises and cloud systems believe their current hybrid environment is actually more secure than the in-house systems they ran previously. Cloud service providers have invested heavily in security controls and features – increasing the level of security in the cloud. In hybrid IT environments the on-premise systems might lag behind and, indeed, most respondents to that research see improved security as a key driver for increasing their use of cloud services.

The challenge is not just about delivering an application or data from a single cloud service. It is also about integrating an array of clouds seamlessly and orchestrating the delivery of business services from a heterogeneous set of clouds – securely and without users perceiving they

are drawing on a network of services. Cloud service providers offer an extensive set of cloud-native security features. The challenge for most organizations is to ensure that their security policies are applied consistently across heterogeneous IT landscapes. This needs a comprehensive understanding of the security requirements, and a thorough assessment of what is already in place or missing. Meeting this challenge requires a combination of cloud-native and cloud-agnostic security skills—a blend that not many organizations yet possess. Indeed, dealing with security concerns in a multi-cloud environment was identified as one of the toughest aspects of managing cloud estates in a recent Fujitsu-sponsored study, cited by 95 percent of respondents. Fortunately, that maturity gap can be closed, which is where the help of an experienced systems integrator such as Fujitsu is often invaluable.

At the heart of resolving multi-cloud security is an organization's responsibility and obligation to protect any data it puts into the cloud. In a multi-cloud environment, the emphasis shifts from securing the perimeter of the network to securing data wherever it is, at rest or on the move, by fully understanding data flows and protecting them according to their sensitivity and value. Ultimately, it is down to cloud users to carry out due diligence when selecting providers in order to ensure they meet their security and regulatory requirements – especially at the network edge, where there are often fewer or less rigidly-enforced controls.

While enterprises, understandably, are often seeking turnkey approaches to multi-cloud security, it is clear that the legal and technical complexities involved make this a challenging ambition, particularly for in-house departments where relevant skills and experience can be thinly spread. They need to ensure a consistent level of security features to address policy and compliance regulations but this can become complicated when different cloud services are included. This is where the managed services approach from vendors, like Fujitsu, with the necessary depth of expertise and resources globally can accelerate the creation of truly secure multi-cloud environments.

Fujitsu's Enterprise Cyber Security business

Fujitsu's Enterprise Cyber Security business serves 1,400 customers globally and is ranked seventh by analyst group PAC in terms of global security revenue[2]. Services are delivered to highest national government security levels from 13 Global Security Operations Centers (SOCs), seven of which are located in Europe, including in Finland, Germany, Poland and the UK.

Fujitsu has more than 40 years' experience across the entire IT lifecycle in the design, delivery, integration and management of large-scale cyber security services, working in highly secure environments in the public and private sector. The company's global security team is made up of approximately 3,700 cyber security professionals – with hiring plans to grow this number to over 11,000 in the next two years – providing a comprehensive portfolio of consulting services, system integration services and managed services, all aligned to enable organizations to withstand a world of cyber-security threats.

Fujitsu's intelligence-led approach to cyber security

The Fujitsu holistic approach to cyber security works to identify and detect threat to protect our customers. Highly versatile, it gives organizations the ideal response to constantly shifting security challenges. It is intelligence-led, based on a clear awareness of an organization's cyber security posture at any point in time, aided by external intelligence to develop perspectives on the external threat context. Automated, routine scanning for vulnerabilities, together with comprehensive event visibility and analysis enable resources to be brought to bear where there has been or is likely to be a challenge. And robust management of the cyber security platforms underpins the benefits of intelligence-led cyber security.

Fujitsu advocates a tripartite cyber security model, embracing people, technology and processes:

- People: Data vulnerability often derives from people's behavior. Changing corporate culture so that understanding and behavior are correctly aligned to maximize cyber security is a prerequisite for any program. The starting point must be to increase employees' breadth and depth of know-how and diligence when it comes to cyber security.
- Technology: When it comes to the technology of cyber security, cyber-threat intelligence, the capability to pre-empt specific issues, effective measures for the protection of digital identities and overall architecture simplification are important. In increasingly borderless multi-cloud environments, vendor-agnostic defense is critical. But so is the ability to keep pace with evolving threats through the use of Artificial Intelligence (AI), machine learning, automation and orchestration. In particular, the Advanced Threat Protection and SOAR capabilities available from Fujitsu provide customers with constantly evolving approaches as a means of achieving enhanced security, making it one of the only Managed Security Service Providers adopting automation to better protect its customers.
- Processes: These have to be designed from the ground up to be secure – with a focus on operational efficiency, reliability and, of course, security. It is also possible to shorten incident response times with playbook-based responses, using Security Automation and Orchestration tools, to accelerate response and restoration.

Fujitsu's Managed Security Services – Comprehensive security, in one place
Fujitsu is one of the world's leading providers of Managed Security Services (MSS), with continually evolving managed security underpinned by threat intelligence services, providing consistency of understanding through context and situational awareness. Its end-to-end offering addresses organizations' full range of cyber security exposures. In 2020, Fujitsu rated as a Major Player in the IDC Marketscape for Managed Security Services. Fujitsu's intelligence-led, enterprise-grade MSS solutions minimize disruption and maintain business continuity across entire organizations, leaving customers free to focus on other priorities.

Fujitsu's Managed Security Services are provided by intelligence-led Security Operations Centers (SOCs) and two global Advanced Threat Centers (ATCs), which protect customers with 24x7 proactive monitoring and incident response. This includes comprehensive threat protection based on prediction of potential risks to any organization according to threat context and cyber security position, via the latest threat intelligence. Every year, they produce a review of the most significant recent security attacks and offer predictions for the 12 months ahead. The latest predictions can be found at https://www.fujitsu.com/global/services/security/insights/security-prediction-2020/.

Fujitsu offers a unique combination of Advanced Threat capabilities, based on contextual threat intelligence, a much broader set of primary threat research, and market-leading security automation, all delivered from its Advanced Threat Centers. Automation of first- and second-line tasks, allows analysts to focus on higher value tasks such as threat hunting. Techniques include playbook-led incident response orchestration, which reduces alert fatigue, and accelerated detection and response using new technologies such as artificial intelligence (AI) and machine learning.

Fujitsu's Advanced Threat services provide organizations with a comprehensive array of information, helping to respond to threats before they can seriously damage the business. This unique pairing enables faster detection and a suite of new as-a-Service offerings for Fujitsu's customers, at a time when the scale and sophistication of threats is growing exponentially.

Highly-qualified and experienced experts at the Fujitsu Global Advanced Threat Center utilize enhanced threat intelligence capabilities, threat research insight and automated management and response to security events, an area coming increasingly into focus for enterprises using so-called Security Orchestration, Automation and Response (SOAR) tooling.

Advanced Threat Services available from Fujitsu include:

- Advanced Threat Protection
- Cyber Threat Intelligence
- Endpoint Detection and Response (EDR)
- Enhanced Analytics & Threat Analytics
- Security Information and Event Management (SIEM and SIEMaaS)
- Threat Response

The MSS portfolio offers comprehensive protection across the enterprise, including Identity and Access Management, Infrastructure Protection, Data Protection, and Threat and Vulnerability Management. Within these services, specific technology offerings include: Firewall Management, End Point Security & Encryption, IDS/IPS, SIEM and SIEM as a Service, Web and Email Security, Multi-Cloud Security services, Data Loss Prevention, Vulnerability Management and advanced threat detection, orchestration and analytics, all underpinned by Fujitsu's Cyber Threat Intelligence Services.

Fujitsu Security Consulting Services
As a comprehensive, independent service delivering unrivalled expertise, proven methodology and extensive industry experience, Fujitsu Security Consulting provides invaluable insight tailored to particular organizational needs, taking into consideration the specific requirements of the various industry segments.

Fujitsu's Security Consulting Services portfolio addresses the four core areas of governance, risk and compliance; strategy architecture; continuity and resilience; and transformation and integration. It includes a broad set of IT Consultancy and Technical Professional Services. This includes all aspects of Cloud Assessment, Multi-Cloud Security consulting, Information Assurance, Information Risk Consultancy, Security Consultancy, Continuity and Disaster Recovery Consultancy, Data Loss Prevention Office 365 assessment, Identity and Access Management, Training and Awareness and Technical Design. Using Fujitsu Security Consulting Services, customers benefit from independent information security consultant expertise and advice related to business needs, plus the design, implementation and integration of security controls needed to put this insight into action.

Selected highlights from Fujitsu's security portfolio

Security, Orchestration, Automation and Response (SOAR)
Security professionals have an incredibly powerful AI tool at their disposal to assess and prioritize cyber threats: Security, Orchestration, Automation and Response (SOAR) technologies that are designed to simplify the incident response process. In particular, the Advanced Threat Protection and SOAR capabilities available from Fujitsu provide customers with constantly evolving approaches as a means of achieving enhanced security, making it one of the only Managed Security Service Providers adopting automation to better protect its customers.

SOAR technologies are designed to simplify the incident response process. Thanks to machine learning, SOAR can appropriately prioritize the most critical threats that human analysts should deal with. This automated incident handling reduces alert fatigue and frees up Security Operations Center staff to deal with more complex and rewarding analytical work. Notably, the mean time to respond is decreased, ensuring that a business can reduce the impact of cyber-attacks.

SOAR is a new technology but it does not replace completely all other security processes and services. Fujitsu also advocates a holistic, intelligence-led approach to cyber security, based on a clear awareness of an organization's cyber security posture at any point in time, aided by external intelligence to develop perspectives on the external threat context.

Cyber Threat Intelligence (CTI)
As cybercrime grows increasingly strategic, traditional security solutions are no longer sufficient. Enterprise organizations require advanced threat protection that uses cyber intelligence to prepare organizations so that they can keep attackers out - preventing them from exploiting vulnerabilities using tactics such as social engineering and spear-phishing. Fujitsu's Cyber Threat Intelligence capability underpins their proactive managed security service that prevents unwanted parties from accessing an organization's IT infrastructure. Using the latest market-leading insights, gathered from a wide variety of reputable sources, then correlated and analyzed by Fujitsu security experts, it identifies, monitors and mitigates threats throughout their lifecycle and enables customers to proactively act against them.

Unified Endpoint Security Managed Service
Endpoint devices on the edge of a network are the easiest place for attackers to gain entry, creating the danger of multiple cyber security weak spots for companies with operations in more than one location. Fujitsu's Unified Endpoint Security (UES) Managed Service provides complete visibility and enhanced security of endpoint devices by detecting and neutralizing cyber threats before they cause data loss, unplanned downtime or loss of reputation. In addition to saving time in managing and monitoring these devices, Fujitsu is taking complexity away from the customer and increasing visibility of threats by using the most effective tools to monitor, predict and detect threats, and to protect different endpoint devices across the business – a particular area of concern with the rapid expansion in remote working in 2020.

Fujitsu Identity and Access Management
Fujitsu's Identity as a Service (IDaaS) solution provides the freedom to manage users' access to relevant systems, applications, data and resources, all in one place. Passwords and IDs stay safe and in control, while compliance requirements are always met. Employees are able to conveniently access the resources they need in heterogeneous IT environments, with single sign-on and self-service features, e.g. password reset, for cost-effective management. Meanwhile, IT managers can easily keep user credentials safe, controlled and in line with existing corporate security policies – even if they're using cloud services. By storing access information in a central directory, customers can manage it easily using convenient, standardized interfaces. This results in complete, end-to-end identity management for an entire organization.

Fujitsu Privileged Access Management (PAM)
Certain employees in an organization have specialist usage rights to access sensitive information. For example, business administrators and developers can install software, create new users and accounts, and other actions. These high-level access rights are extremely attractive to cyber criminals. If breached, this can cause substantial disruption and even long-term damage.

Fujitsu's Privileged Access Management (PAM) Offering is designed specifically to keep these users' profiles safe. Featuring a higher level of security, with enhanced controls and traceability features, PAM integrates easily with customers' existing operations and access infrastructure, to create a cost-effective, compliant solution, where customers only pay for what they use, scaling as needed – on-premises or in the cloud.

Notes to editors

[1] Source: Cybintsolutions.com

[2] Pierre Audoin Consultants, *IT Security Vendor Rankings Worldwide*, 23 September 2020

Online resources

- Fujitsu Enterprise and Cyber Security: https://www.fujitsu.com/emeia/themes/security/
- UES newsflash / announcement: https://www.fujitsu.com/emeia/about/resources/news/press-releases/2019/emeai-20190509-fujitsu-delivers-greater-threat-visibility.html
- Brief video about Intelligence-Led Security https://www.youtube.com/watch?v=CzJgU3ucsIl
- Read the Fujitsu blog: https://blog.global.fujitsu.com/category/cyber-security/
- Follow Fujitsu Security on Twitter: https://twitter.com/FujitsuSecurity
- Follow us on LinkedIn: https://www.linkedin.com/showcase/fujitsu-security/
- Find Fujitsu on Facebook: http://www.facebook.com/FujitsuICT
- Fujitsu pictures and media server: http://mediaportal.ts.fujitsu.com/pages/portal.php
- For regular news updates, bookmark the Fujitsu newsroom: http://ts.fujitsu.com/ps2/nr/index.aspx

Media contact
Public Relations
International Corporate Communications
E-Mail: public.relations@ts.fujitsu.com

About Fujitsu
Fujitsu is the leading Japanese information and communication technology (ICT) company offering a full range of technology products, solutions and services. Approximately 130,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers. Fujitsu Limited (TSE:6702) reported consolidated revenues of 3.9 trillion yen (US$35 billion) for the fiscal year ended March 31, 2020. For more information, please see www.fujitsu.com.