Media Backgrounder
Enterprise and Cyber Security

May 2019

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, and an increasing army of connected things and sensors that deliver constant, real time information. 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 and data breaches are among the top-10 largest threats facing the world, according to the World Economic Forum, which earlier this year reported on evidence that there are four new malware samples created every second. The Breach Live Index, which tracks publicly-disclosed breaches, shows that nearly 15Bn data records have been stolen since 2013, with only four percent of these protected by encryption, rendering the stolen data useless.

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. The impact of infiltration on this scale is massive. In 2017, the Centre for Strategic and International Studies put the total cost of cybercrime at $600Bn – close to 1% of global GDP. 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.

The challenge is only getting bigger: as soon as 2020, there will be over 20Bn devices to secure, according to analyst firm Gartner. 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 quantified at nearly 3 million positions 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."

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. Indeed, most 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. Meeting this challenge requires a different set of security skills – not one that many organizations yet possess – resulting in a huge deficit in skills when it comes to managing cloud security. 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. One area that is coming increasingly into focus for enterprises is the process of automating management and response to security events, using so-called Security Orchestration, Automation and Response (SOAR) tooling.

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. 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 'lift and shift' 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. 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[1]. Services are delivered to highest national government security levels from 13 Global Security Operations Centers (SOCs), three of which are located in Europe (Finland, Germany, 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 2,000 cyber security professionals – with hiring plans to significantly grow this number within two years – providing a comprehensive portfolio of consulting services, system integration services and managed services, plus biometric products under the PalmSecure brand, all aligned to enable organizations to withstand a world of cyber-security threats.

Fujitsu's intelligence-led approach to cyber security

The Fujitsu approach to cyber security 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.
- 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 to accelerate response and restoration. One emerging technology is Security Automation and Orchestration (SAO), which Gartner estimates will have been adopted by 15% of organizations by 2020.

Fujitsu's Managed Security Services – Comprehensive security, in one place

Fujitsu is one of the world's leading providers of Managed Security Services (MSS). Its end-to-end offering addresses organizations' full range of cyber security exposures. In 2019, Fujitsu has once again been included in the Gartner Magic Quadrant for Managed Security Services, which ranks the top global MSS vendors., 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 MSS identifies potential risks, mitigates any

immediate impact and prevents subsequent attacks from happening, offering comprehensive protection across the enterprise, including Identity and Access Management, Infrastructure Protection, Data Protection and Threat and Vulnerability Management.
Fujitsu's Managed Security Services are provided by intelligence-led Security Operations Centers (SOCs), which protect customers with 24x7 proactive monitoring and incident response. 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/predictions-2019.

Comprehensive threat protection includes basing the prediction of potential risks to any organization on an understanding of the threat context and cyber security position, via the latest insights from Fujitsu's SOCs.

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, 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, 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, Technical Design and Third Line Support. 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. Fujitsu also offers Advanced Threat Center capabilities, including automation of first- and second-line tasks, allowing 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.

Selected highlights from Fujitsu's security portfolio

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 keep attackers out - preventing them from exploiting vulnerabilities using tactics such as social engineering, data theft, spear-phishing and zero-day. Fujitsu's Cyber Threat Intelligence provides vigilant and proactive managed security 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.

Threat 360 – Advanced Threat Protection

Fujitsu Threat 360 is an advanced CTI assessment that examines an organization's security posture from an 'inside out' and an 'outside in' perspective to highlight weaknesses in holistic security policies and help protect against malware and ransomware and mitigates data leakage and loss. It includes a Passive Threat Assessment, which looks for threats based on information available on both the clear and dark web and tracks down potentially damaging information that may be publicly available on the web – such as 'internal only' copies of documents and other unstructured data. In addition, Fujitsu Threat 360 provides a Malware Assessment. Based on Cylance technology, this service conducts a thorough analysis of dormant or running threats within an organizations' IT environment.

Fujitsu Identity Access as a Service

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 your 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) is designed specifically to keep this environment safe. Featuring a higher level of security, with enhanced controls and traceability features, PAM integrates easily with your 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] Pierre Audoin Consultants, *IT Security Vendor Rankings Worldwide*, 09 October 2018

Online resources

- Fujitsu Enterprise and Cyber Security: https://www.fujitsu.com/global/themes/security/
- Threat 360 press release: http://www.fujitsu.com/fts/about/resources/news/press-releases/2018/emeai-20180629-fujitsu-announces-new-threat-360-assessment.html
- Inside the Gates - The Banking Trojan Threat (Dridex Case study) https://youtu.be/iRIRG6nJP1E?list=PLi_KjAUQ9e-qtij6G97eLh-rWE1EBNxLl
- 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
Isabell Horvath
Director of PR
Corporate Communications
Tel.: +49 (89) 62060 4419
E-Mail: isabell.horvath@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 140,000 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 4.1 trillion yen (US $39 billion) for the fiscal year ended March 31, 2018. For more information, please see http://www.fujitsu.com.

About Fujitsu EMEIA

Fujitsu promotes a Human Centric Intelligent Society, in which innovation is driven by the integration of people, information and infrastructure. In the Europe, Middle East, India and Africa region (EMEIA), our 27,000-strong workforce is committed to Digital Co-creation, blending business expertise with digital technology and creating new value with ecosystem partners and customers. We enable our customers to digitally transform with connected technology services, focused on Artificial Intelligence, the Internet of Things, and Cloud - all underpinned by Security. For more information, please visit https://www.fujitsu.com/emeia/about/