Protecting UK Telecom Networks through the Vendor Assessment:

Microsoft cloud service offerings and security engineering practices
to strengthen telecom security and enhance resiliency

Introduction

Microsoft welcomes the new and robust Telecoms Security Framework developed for the UK telecoms sector and appreciates the opportunity to highlight Microsoft's existing and ongoing commitment to compliance with the Telecoms Security Requirements (TSRs) and the vendor security assessment guidance. We recognize that while no system can be 100% secure or available, we applaud the realistic standards set forth in the TSRs and used to assess the security of vendor equipment for the protection of the UK's telecoms networks. The robust and practical controls outlined will help the UK achieve its goals by making it harder for UK networks to be compromised, while also providing ways in which threats can be detected and mitigated quickly.

The proposed issuance of the TSRs is timely. Advances associated with broader technological trends and changes happening around virtualization and 5G allow operators to deploy tailored environments offering more granular control over asset and data security. The combination of resilient, cloud-based infrastructure with the virtualization of network functions enables the deployment of customized secure networks with enhanced flexibility to effectuate network replacement and remedy security threats. New technologies create new security challenges, especially in the context of communication networks as the overall security level will ultimately be influenced by the weakest link in the entire ecosystem. Therefore, it is even more important to establish a sufficiently high baseline level of security from the beginning, including automating security and compliance when and where possible.

Microsoft has long supported and promoted risk-based approaches to security as advocated in the overview and subsequent sections of the TSRs. Such approaches are responsive to government agencies and telecoms security goals, and to business needs to efficiently adopt and integrate new technology to address the modern threat landscape. In response to the 2020 report released by the UK National Cyber Security Centre's (NCSC) on the state of telecom security,[1] Microsoft has highlighted below an overview of our standard practices aligned across the telecom vendor requirements. Our approach to telecom and security more broadly is based on two core principles: 1.) secure engineering practices underpinning Microsoft Azure and 2.) our services and innovative security and network operational tooling for operators.

With that context, we respectfully wish to share our perspective and security approach as a major Cloud Service Provider (CSP) based our hybrid cloud solutions and in alignment with the UK's existing cloud security principles[2]. In the CSP role, Microsoft works with a variety of customers and partners

[1] NCSC's Security Analysis for the UK Telecoms Sector Report
[2] https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

that deploy and build on top of our products and services. Our services enable partners in the telecommunication sector to use Microsoft cloud services and infrastructure to support their core networks and other products while meeting compliance requirements.[3]

Microsoft's Security Practices Alignment with the Vendor Requirements

Microsoft Azure is compliant with more than 90 certifications across the globe and follows a comprehensive set of industry leading security and reliability practices across our products and services.[4,5] We also continually mature our practices and regularly share guidance for our customers and other companies to follow, freely sharing best practices throughout the industry and promoting responsible behaviours. Below is a high-level summary of Microsoft Azure's compliance along with cross-references to the vendor security assessment criteria.

Vendor Assessment A.) Product Lifecycle Management

The below section outlines how Microsoft integrates our security practices across the software security development lifecycle (SDL). Back in 2002, Microsoft launched its Trustworthy Computing initiative to help ensure Microsoft products and services were built inherently highly secure, available, reliable, and with business integrity. Almost two decades later, the Microsoft SDL is an outcome of our software development groups continually implementing a security framework that's easy for developers to understand and incorporate into their product lifecycle and development activities. The SDL includes security considerations throughout all phases of the development process, helping developers build highly secure software and simultaneously addressing security compliance requirements. Since first publicly shared in 2008, we have updated the practices as a result of our growing experience with new scenarios, like the cloud, IoT, and AI.[6] All of Microsoft products follow the Microsoft SDL, including Azure. The Microsoft SDL meets or exceeds the guidance published in ISO/IEC 27034-1[7].

Microsoft integrates security practices across the entire product lifecycle, from planning to sunsetting, for program managers, developers, and testers alike. Several key areas of our SDL for our telecom customers include defining metrics and compliance reporting, regularly performing threat modelling[8], the use of cryptography standards (including security protocol, algorithm, and key length recommendations for SSL/TLS versions), and especially critical in today's deployment model of 5G capabilities is managing the risk of using third-party components[9].

Equally important, our approach enables flexible practices and activities at every stage of development using either the classic waterfall, agile development methodology or DevOps. DevOps[10]

---

[3] Azure for Operators
[4] Microsoft Security Engineering Portal
[5] Compliance in the trusted cloud | Microsoft Azure
[6] Microsoft's Security Development Lifecycle
[7] Microsoft SDL Conforms to ISO/IEC 27034-1:2011 - Microsoft Security
[8] https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
[9] https://safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf
[10] What is DevOps? DevOps Explained | Microsoft Azure

is a compound of development (Dev) and operations (Ops) that merges people, processes, and technology to continually provide value to customers. Microsoft follows a Secure DevOps (DevSecOps) approach so that security, development, and operations are tightly integrated.[11] Security and compliance controls (which are baked into the DevOps process and pipeline) ensure the operational configuration conforms to the security baseline, which takes into account real-world threats such as the Open Web Application Security Project (OWASP) Top 10[12] or SANS Institute Top 25[13], and industry and regulatory requirements. DevOps automation minimizes or eliminates issues that could be introduced by human error.

Vendor Assessment B.) Product Security Management

Azure also manages change automation so that all code and configuration updates go through well-defined stages to catch regressions and bugs before they reach customers.[14] We test requirements prior to changes and code is released to the public under safe deployment processes. Significant changes are released to our Early Updates Access Program (also known as "canary regions"), which allows for public trial of the change prior to release into Azure's General Availability regions[15]. Lastly, new offerings go through the Product Launch Readiness process that validates the offering has attained the relevant compliance and security validations.

For secure management capabilities we offer Azure Sentinel for our customers to deploy secure capabilities across TLS, role-based access controls (RBAC) authentication policies and more.[16] Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. In particular our Sentinel capabilities allow for our customers to deploy security automation and orchestration, unlock investigative tools, leverage threat hunting, and collect and analyse data.

Vendor Assessment C.) Protected Development and Build Environments

Microsoft deploys strict hardware-enforced separation of tenant resources.[17] We deploy hardware-enforced type 1 hypervisor separation and network segregation offboard from the host software. We also integrate the concept of least privilege within our Microsoft SDL practices and implement this into secure build configurations and give the tenant strict controls on their data via Customer Lockbox[18] and Key Vault[19] services. In addition, we can also offer dedicated hosts if preferred by the tenant, in both mainline Azure regions and private edge zones, and our commitment to confidential

---

[11] Enable DevSecOps with Azure and GitHub - DevSecOps | Microsoft Docs
[12] OWASP Top Ten
[13] CWE/SANS TOP 25 Software Errors
[14] Azure Automation Change Tracking and Inventory overview
[15] Advancing safe deployment practices | Azure Blog and Updates | Microsoft Azure
[16] What is Azure Sentinel? | Microsoft Docs
[17] Isolation in the Azure Public Cloud
[18] Customer Lockbox for Microsoft Azure
[19] Azure Key Vault Overview - Azure Key Vault

computing enables us to protect sensitive data-in-use through isolating computations to a hardware-based trusted execution environment.

For Azure, Microsoft deploys continuous integration and continuous deployment (CI/CD) through faster release cycles across different microservice architectures. This capability is also something we offer our customers through Azure DevOps documentation and Azure Pipelines.[20] This enables our customers to deploy a suite of technologies which deliver software more securely and quickly. From code to cloud, our customers are able to automate each part of the DevOps process with continuous integration and continuous deployment.

Vendor Assessment D.) Exploit Mitigations

Microsoft deploys a wide variety of physical, infrastructure, and operational controls to help secure Azure for us and our customers. We also enable exploit protection for our customers through our Azure Security Center, including Microsoft 365 Defender and Azure Defender to protect hybrid cloud workloads against threats.[21] These capabilities enable our customers to use the Azure Secure Score dashboard to track their security posture, including simplifying their compliance. These capabilities also enable our customers to meet TSRs through the use of AI and automation to quickly detect false alarms, identify real threats and streamline investigations.

For our Azure datacentres we use several approaches to ensure the security of our underlying fabric. Azure's security approach is concerned with three types of threats: 1.) external threats, such as malicious or compromised customers, 2.) insider threats, such as compromised entities with logical or physical access to the hardware, 3.) and supply chain threats. Azure deploys multiple layers of security to address these various threats in our datacentres, using both hardware and software. Five measures that apply directly to the fabric itself are:

1. Secure boot: All early boot firmware measurements are stored in a signed manifest. Unified Extensible Firmware Interface[22] (UEFI) components are signed. Upon bootup, servers in our fleet check the signature of their firmware before running it. UEFI Secure Boot policy is enforced in the UEFI environment. Should component or UEFI Secure Boot verification fail, the server does not boot and instead it is remedied by the underlying fabric with the correct firmware and UEFI images. (See section F for additional details).
2. Secure firmware: Firmware is patched to eliminate any vulnerability disclosed publicly or otherwise identified. Servers in our fleet receive the new freshly patched firmware and apply it.
3. Secure compliance reviews: New server designs deployed in our fleet receive a rigorous set of security compliance reviews to meet Azure hardware/firmware security requirements.
4. Supply chain security and resiliency: Azure has a hardware supply chain security program in which security requirements are published and enforced with Azure hardware suppliers.
5. Hardware/Firmware Inventory & Lifecycle Management: Azure enforces component inventory as a single source of truth for Azure fabric. Each Azure node has its software measured (fingerprinted) and monitored using a hardware monitoring service. Azure hardware uses

[20] CI/CD for Azure VMs - Azure Solution Ideas | Microsoft Docs
[21] Azure Security Center | Microsoft Azure
[22] Specifications | Unified Extensible Firmware Interface Forum (uefi.org)

solutions centred around Project Cerberus. (See section F for additional details on Project Cerberus)

We also leverage Microsoft's security operations, including Microsoft's Cyber Defense Operations Center (CDOC)[23], to protect, detect and respond to over 8 trillion threat signals daily to protect Microsoft cloud infrastructure, services, and customers from evolving threats.[24] Our approach is built upon four core tenants: protecting our infrastructure, strengthening our products and services through secure engineering procedures, protecting customers through a comprehensive suite of security solutions, and our detection and response services.[25] We regularly integrate these detect and protect capabilities for both our own and our customer's infrastructure and services.[26]

Vendor Assessment E.) Secure Updates and Software Signing

All components in the software stack that are installed in the Azure environment are custom built following the Microsoft SDL. All software components and configuration, including operating system images and databases, are deployed as part of change management and release management processes. Microsoft integrates our product lifecycle practices into the development of source code. In addition to software signing, signature verification and secure updates, we also incorporate mandatory virus scans plus other security scans with logging in all Azure software component builds. The Hypervisor enforces user and kernel mode code integrity, preventing any unsigned code from being loaded into memory pages that can be used to execute code for the host operating system.

Vendor Assessment F.) Hardware Roots of Trust and Secure Boot

Azure Servers use two roots of trust to verify the integrity of platform firmware.[27] The first, called Cerberus[28], authenticates the integrity of all platform firmware as it is loaded and compares it to the expected value in a platform firmware manifest. If there is a mismatch, the code is not executed, and a remediation process is started. The second root of trust is a Trusted Platform Module (TPM) 2.0. The TPM is a tamper-resistant, cryptographically secure auditing component with firmware supplied by a trusted third party. Measurements of host components, firmware and configuration settings are recorded during boot in the TPM. The boot measurements are cryptographically signed by the TPM and sent to the Azure Host Attestation Service for validation. Before the platform can join the Azure fleet and host customer workloads it must pass validation. Potential hosts with a downgraded manifest or firmware are rejected. If invalid, servers are taken offline to bring them back into a compliant state. Azure Servers also implement UEFI Secure Boot which checks the signature of any component loaded in the UEFI stage of the boot process against security policies defined in the UEFI standard. The UEFI policy settings in use during boot are recorded in the TPM and are part of the information sent to the Azure Host Attestation Service.

---

[23] https://www.microsoft.com/en-us/msrc/cdoc
[24] Trust your cloud | Microsoft Azure
[25] Microsoft Security Business Operations
[26] Turn on exploit protection to help mitigate against attacks
[27] Platform integrity and security overview
[28] Firmware integrity - Azure Security

Vendor Assessment G.) Security Testing

Testing is a critical component of our security engineering practices and our testing capabilities meet the robust testing requirements outlined in the TSRs. Microsoft performs tests through the development and deployment phases and regularly performs tests during the operations and maintenance phases of our products and services. The three main testing practices we integrate are: Static Analysis Security Testing (SAST), Dynamic Analysis Security Testing (DAST) and penetration testing.[29] SAST provides a highly scalable method of security code review by analysing source code before compilation to validate the use of secure coding policies. DAST enables us to perform run-time verification of fully compiled or packaged software, checking end-to-end security functionality and consistency that is only apparent when all components are integrated and running. This is typically achieved using a tool or suite of prebuilt attacks or tools that specifically monitor application behaviour for memory corruption, user privilege issues, and other critical security problems.

We also employ an "Assume Breach" strategy and leverage highly specialized groups of security experts, known as Red Teams to perform offensive activities and Blue Teams to improve defenses. The teams strengthen threat detection, response and defense for enterprise cloud services. While these practices have been in place for many years, most customers are unaware of the work being done behind the scenes to harden the Microsoft enterprise cloud.[30] We run Red Team penetration testing to uncover potential vulnerabilities resulting from coding errors, system configuration faults, or other operational deployment weaknesses by skilled security professionals simulating the actions of a hacker. These are often performed in conjunction with automated and manual code reviews to provide a greater level of analysis than would ordinarily be possible.

Vendor Assessment H.) Secure Management and Configuration

Our Operational Security Assurance (OSA) consists of a set of practices that aim to improve operational security in cloud-based infrastructure. Through the combination of the OSA, DevSecOps, and safe deployment practices (see section B for more details) Microsoft demonstrates our commitment to maintaining comprehensive in-depth understanding and audit control of our cloud services to the TSRs and oversight functions. These practices, in addition to SDL, follow a number of principles we deploy across our cloud infrastructure including: multi-factor authentication, enforcing least privilege, encrypting data in transit and at rest, implementing security monitoring, and regularly assessing and updating our security strategy.[31] Monitoring automatically and continuously checks that services' assets are compliant to the defined security baseline and all privileged accounts (including administrative) are linked to an individual user account, which undergo periodic review.

Vendor Assessment J.) Vulnerability and Issue Management

Through decades of experience with developing and managing software and working with the security community to improve products and services, Microsoft has learned that Coordinated

---

[29] Develop secure applications on Microsoft Azure

[30] https://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf

[31] Microsoft's Operational Security Assurance

Vulnerability Disclosure (CVD) most effectively minimizes risk to our technology users. We are committed not only to internal research and testing to identify and address issues but also to partnership with external researchers that find and report potential issues. Under our CVD policy, Microsoft receives vulnerability reports directly from finders and through third party coordinators. We both respond promptly to vulnerability reports and communicate with reporters throughout the vulnerability investigation, remediation, and public disclosure process, requesting further information as helpful and providing updates as progress is made. However, if there is evidence of a vulnerability in the public domain while Microsoft is developing or testing a remediation, then we work closely with vulnerability reporters to provide customers and the broader public with early disclosure and a comprehensive set of existing mitigations. This proactive threat hunting, combining our internal CDOC expertise and external resources provides comprehensive Red Team/Blue Team security threat assessment, monitoring and defense capabilities for Azure cloud and services.

To provide transparency into our policies and processes, we share information about our commitments to working with the security community and to leveraging best practices, such as ISO/IEC 29147[32]. We also publish a list of vulnerabilities and patches that impact Microsoft products and services, enabling customers to search by impacted product family and our severity rating (and describing the vulnerabilities by using the industry standard Common Vulnerability Scoring System), and we highlight critical vulnerabilities, security updates, and attack activity in Microsoft Security Response Center (MSRC) blog posts.[33] In addition, to foster partnerships with others in the security community, we seek researcher collaboration through substantial bug bounty programs and give credit to vulnerability reporters.

Unlock Cloud Security Innovation for Telecom Operators

While secure development is integral to Microsoft's own cloud and service offerings, we also provide comprehensive tooling and advice to assist all our customers in adopting security best practices, including access to real-time AI-driven cyber operations previously unavailable to telecoms. In addition to the breakout above where we highlighted our own security capabilities for our infrastructure and services, the below highlights a few key takeaways for telecoms to consider when selecting a vendor.

Microsoft encourages our Azure tenants to deploy systems with Azure's automated DevSecOps and security policy enforcement and, to that end, makes available for tenant use similar tooling as we utilize for the management of our cloud itself. In particular, Azure Arc[34], Azure Active Directory[35], Customer Lockbox, Key Vault and Azure Monitor[36] enable tenants to define and impose consistent security policies, user access controls, key and certificate management and rotation, and multi-factor

[32] ISO - ISO/IEC 29147:2018 - Information technology — Security techniques — Vulnerability disclosure
[33] Microsoft Security Response Center
[34] Azure Arc – Azure Management | Microsoft Azure
[35] Azure Active Directory | Microsoft Azure
[36] Azure Monitor | Microsoft Azure

authentication across both resources in Azure and edge[37] locations. We strongly recommend that customers implement Privileged Access Workstation (PAW) systems[38] as a best practice. As envisaged in the TSRs, we use a similar approach for our own internal administration of our cloud services, the **Secure Access Workstation**[39], which is customised for our operating requirements to secure administrative access to our clouds and other critical functions.

Service reliability is of critical importance to operators, driven by both customer expectations and regulatory oversight.[40] Cloud offers novel network architecture options for operators beyond traditional deployment models. Familiar patterns such as deploying services across multiple regions to assure 5-nines availability can be combined with edge-based services such as campus 5G, and hybrid combinations such as operator on-premises datacentres with cloud bursting[41] to utilize cloud resources on demand to handle peak loads. Microsoft supports all these deployment models, providing both the underlying technical resources and extensive advice for operators on how to exploit the increased flexibility for best service availability and data security.[42]

Cloud also enables telecoms to rapidly deploy infrastructure and services that integrates Microsoft's leading security practices and standards into their development lifecycles to address on-going operator requirements, integrate a zero-trust architecture and use cloud services as a catalyst to further security innovation, leveraging IoT, big data, and AI. These concepts enable a more scalable and dynamic approach than the traditionally long cycles needed to develop, test, deploy, and configure telecom networks. Operators stand to inherit unique capabilities unlocked by cloud computing as they migrate their infrastructure and take advantage of cloud security and compliance capabilities.

[37] Microsoft Edge security for your business | Microsoft Docs
[38] Developing a privileged access strategy | Microsoft Docs
[39] Protecting high-risk environments with secure admin workstations (microsoft.com)
[40] Azure Reliability
[41] What Is Cloud Bursting - Definition | Microsoft Azure
[42] Multicloud and Hybrid Cloud Solutions