LogTag Recorders

LogTag Online:

System Security, Compliance, And Reliability/Resiliency

December 2019

Security

Overview

LogTag Online is committed to providing you with a trusted set of cloud services. We have leveraged our decades-long industry experience building enterprise to create a robust set of LogTag Online security technologies and practices. These work to help reduce the cost, complexity, and risk associated with security in the cloud.

Our mission is to deliver the highest levels of security, privacy, compliance, and availability to private and public sector organizations and help you protect your business assets while reducing security costs. Toward that end, our partner Microsoft invests over $1 billion annually in cybersecurity, including the LogTag Online platform, and employs over 3500 dedicated cybersecurity professionals.

LogTag Online helps you strengthen your security posture, streamline your compliance efforts, and enable digital transformation.

LogTag takes a defense-in-depth approach to security in LogTag Online.

Physical Security

The LogTag Online datacenters are operated in a way that strictly controls physical access to the areas where your data is stored. The LogTag Online cloud service can make use of datacenters in 54 regions (as of 2019), and each of these has extensive multilayered protections to ensure unauthorized users cannot gain physical access to your customer data. Layered physical security measures at LogTag datacenters include access approval:

- At the facility's perimeter.
- At the building's perimeter.
- Inside the building.
- On the datacenter floor.

Physical security reviews of the facilities are conducted periodically to ensure the datacenters properly address LogTag Online security requirements.

Security Design and Operations

Secure cloud solutions are the result of comprehensive planning, innovative design, and efficient operations. LogTag makes security a priority at every step, and operational security best practices are integrated into every aspect of LogTag Online. This includes implementing controls that restrict unauthorized access from personnel and contractors.

LogTag provides multilayered security across physical datacenters, infrastructure, and operations. LogTag Online employs operations and security professionals work to protect your data from unauthorized access.

Infrastructure Protection

Infrastructure security is a key component of the secure foundation on which LogTag cloud services are built. LogTag Online addresses security risks across its infrastructure, which includes hardware, software, networks, administrative and operations staff, and the physical datacenters that house it all.

Physical security

LogTag Online runs in a highly secured facility, sharing space and utilities with other Services. Physical access is strictly controlled on a “need to” basis and limited in both area and time.

The facility is designed to run 24 hours a day, 365 days a year, and employs multiple layers of security measures to help protect operations from power failure, physical intrusion, and network outages:

- Perimeter: Security staff around the clock, facility setback requirements, fencing and other barriers, and continuous surveillance camera monitoring
- Buildings: Alarms, seismic bracing, and security cameras, routine patrol of the datacenter by well-vetted and highly trained security personnel
- Server facilities: Multifactor-authentication-based access controls that use biometrics and card readers, cameras, and backup power supplies
- Datacenter floor: Full body metal detection screening and additional security scan, video monitoring, and restriction on allowed devices

LogTag datacenters comply with industry standards (such as ISO/IEC 27001) for physical security and availability. They are managed, monitored, and administered by trained operations personnel. Periodic physical security reviews of the facilities are conducted to ensure the datacenters properly address the security requirements.

Monitoring and Logging

Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the LogTag Online environment, providing continuous visibility and timely alerts to the teams that manage the service.

Identity and user-access management and control

Identity is a crucial boundary layer for security. Many consider it to be the primary perimeter for security. This is a shift from the traditional focus on network security, as network perimeters keep getting more porous.

LogTag has strict controls that restrict access to LogTag Online by LogTag personnel. LogTag personnel do not have default access to cloud customer data. Instead, they are granted access, under management oversight, only when necessary.

LogTag Online server compliance offerings

LogTag in conjunction with our key partners, offers a comprehensive set of compliance offerings for the cloud server to help you comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data.

These include compliance offerings that are: globally applicable, US government regulations, other region- or country-specific regulations, and industry-specific requirements. Below is a list of our compliance offerings as of October 2019.

Globally applicable offerings

Compliance offerings covered in this section have global applicability across regulated industries and markets. They can often be relied upon by customers when addressing specific industry and regional compliance obligations.

- **CIS Benchmark.** The Center for Internet Security Microsoft Azure Foundations Benchmark.
- **CSA STAR Attestation.** The Cloud Security Alliance audit of a cloud provider's security posture.
- **CSA STAR Certification.** The Cloud Security Alliance certification that involves an independent third-party assessment of a cloud provider's security posture.
- **CSA STAR Self Assessment.** The Cloud Security Alliance level 1 offering that is free and open to all cloud services providers.
- **ISO/IEC 20000-1:2011.** International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) certification in Information Technology Service Management.
- **ISO 22301.** International Organization for Standardization (ISO) Business Continuity Management Standard.
- **ISO/IEC 27001.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Information Security Management Standards.
- **ISO/IEC 27017.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Code of Practice for Information Security Controls.
- **ISO/IEC 27018.** International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Code of Practice for Protecting Personal Data in the Cloud.
- **ISO 9001.** International Organization for Standardization Quality Management Systems Standards.
- **SOC 1, 2, and 3.** Service Organization Controls standards for operational security.
- **WCAG 2.0.** Web Content Accessibility Guidelines 2.0.

US Government

The following compliance offerings are focused primarily on addressing the needs of US Government.

- **CJIS**. Criminal Justice Information Services Security Policy.
- **DFARS.** Defense Federal Acquisition Regulation Supplement for defense contractors.
- **DoD DISA L2, L4, L5.** US Department of Defense Provisional Authorization.
- **DoE 10 CFR Part 810.** Department of Energy Code of Federal Regulations.
- **EAR.** US Export Administration Regulations.
- **FDA CFR Title 21 Part 11.** Food and Drug Administration Code of Federal Regulations.

- **FedRAMP.** Federal Risk and Authorization Management Program.
- **FERPA.** Family Educational Rights and Privacy Act.
- **FIPS 140-2.** Federal Information Processing Standard.
- **IRS 1075.** US Internal Revenue Service Publication.
- **ITAR.** International Traffic in Arms Regulations.
- **NIST 800-171.** National Institute of Standards and Technology Special Publication on Protecting Unclassified Information in Nonfederal Information Systems and Organizations.
- **NIST Cybersecurity Framework (CSF).** National Institute of Standards and Technology Cybersecurity Framework.

Other region and country-specific regulations

The following compliance offerings are specific to various regional and national laws and regulations. Some of these offerings are based on independent third-party certifications and attestations; others provide contract amendments and guidance documentation to help customers meet their own compliance obligations.

- **Argentina PDPA.** Personal Data Protection Act 25,326.
- **Australia IRAP Unclassified.** Information Security Registered Assessors Program.
- **Australia IRAP PROTECTED.** Information Security Registered Assessors Program highly sensitive data security level.
- **Canada Privacy Laws.** Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta Personal Information Protection Act (PIPA), and British Columbia Freedom of Information and Protection of Privacy Act (BC FIPPA).
- **China GB 18030:2005.** Chinese Coded Character Set standard set by the China Electronics Standardization Institute (CESI).
- **China DJCP (MLPS) Level 3.** Information Security Technology—Basic Requirements for Classified Protection of Information System Security (multilevel protection scheme).
- **China TRUCS / CCCPPF.** Trusted Cloud Service Certification.
- **EU EN 301 549.** European Union Accessibility Requirements Suitable for Public Procurement of ICT Products and Services.
- **EU ENISA IAF.** The European Union Agency for Network and Information Security Information Assurance Framework.
- **EU GDPR.** European Union General Data Protection Regulation.
- **EU Model Clauses.** European Union data protection law Standard Contractual Clauses.
- **EU-US Privacy Shield.** Designed by the U.S. Department of Commerce, and the European Commission.
- **Germany C5.** Cloud Computing Compliance Controls Catalog.
- **Germany IT-Grundschutz workbook.** IT-Grundschutz workbook for Internet and cloud usage.
- **India MeitY.** Ministry of Electronics and Information Technology accreditation for public cloud, government virtual private cloud, and government community cloud.
- **Japan CS Mark Gold.** Cloud Security Gold Mark for IaaS and PaaS.
- **Japan My Number Act.** Social Benefits and Tax Number resident identification number system.
- **Netherlands BIR 2012.** Baseline Informatiebeveiliging Rijksdienst standard.
- **New Zealand Gov CC Framework.** New Zealand Government Cloud Computing Security and Privacy Considerations.

- **Singapore MTCS Level 3.** Multi-Tier Cloud Security Standard for Singapore certification for IaaS, PaaS, and SaaS.
- **Spain ENS High.** Spain Esquema Nacional de Seguridad (ENS) High Level Security Measures.
- **Spain DPA.** Spanish Data Protection Agency guidelines.
- **TISAX (Germany).** Trusted Information Security Assessment Exchange.
- **UK Cyber Essentials Plus.** Cyber Essentials PLUS requirements outlined in the Cyber Essentials Scheme Assurance Framework.
- **UK G-Cloud.** United Kingdom Government-Cloud services classification v6.
- **UK PASF.** United Kingdom Police Assured Secure Facility standards.

Resiliency/Reliability

High Availability

A key aspect of a resilient foundation is availability. High availability is all about maintaining acceptable continuous performance despite temporary failures in services, hardware, or datacenters, or fluctuations in load. Highly available systems are consistently operational over long periods of time.

LogTag Online server uptime, expressed as a rolling 12 month average to June 2019, was 99.996%, or approximately 26 minutes of downtime per year. Availability can never be 100% because hardware and software failures happen, and human error occurs.

Data Security

LogTag Online maintains three independent copies of all data in real time. This data is stored in the United States west coast. These copies are real-time duplicates so in the event of failure of one of the copies no data is lost, and the system automatically switches to a back-up version (zero downtime).

The three copies are all held on separate physical servers, though all three servers are housed within the same geographic storage centre.

Additionally a backup of the data is made to a separate Geographic location approximately every 5-10 minutes (1 hour is guaranteed). This data is saved for 35 days, and would be used to recover from a catastrophic local event (fire, earthquake).