Attributes of a Successful Secure Cloud Security Ecosystem

Author: Chris Cracknell, 29/8/2023

Overview

This document describes the attributes required by a Secure Cloud Security Ecosystem that must genuinely protect the secrecy and integrity of its data, even from the owners of the system and state actors

Secrecy and Integrity

Data must be genuinely limited to an authenticated instance of the intended running system and associated meta system.

This explicitly EXCLUDES general access by the system owner, their management, a cloud infrastructure provider, law enforcement and other state and non-state actors.

Meaningful Governance

Governance of the system must be flexible (M of N Quora, various authentication methods, 2FA, OTP, etc.) and must be applied at multiple points in the system, where appropriate.

Governance effort and clarity (transparency) must be meaningful and appropriate to the decisions involved. (Too much effort means the processes are avoided...)

Software Lifecycle

The software lifecycle must have security integrated in it. Including, but not limited to:

- Secure Software Development Process SSDP
- Secure Software Supply Chain SSSC
- Governance in build and deployment
- Secure Revocation

Resilience

The system resilience must be secured, no data, state or service loss y be irrecoverable.

- Provable.
- Governance on Backups and Restores protected from e.g. ransomware corruption.
- Backup must include software state, not just working data.
- High Availability does not replace backup.

Copyright © Chris Cracknell 2023, 2026

- Planned-for disaster scenarios and recovery paths.

Secure Mechanisms

The underlying mechanisms used to implement the system must be secure.

- Industry standards
- Planned to be future-ready (as far as possible)
- Published for peer review
- Upgradeable during the lifetime of the system

Transparency

Everything must be auditable. Proactively (forensic) and monitored.

Ingress and Egress

The points where the system interacts with the wider world must be hardened. Verification at Ingress and Authentication at Egress.

Tool Support

Tooling must be available to support all tasks and roles involved in operating the system. “If it is too much effort to be secure then the users will subvert the process.” - e.g. post-it passwords

Skilled Personnel

All personnel involved in the development and operation of the system must

- be clearly identified as to who is fulfilling what role.
- have the appropriate skills for the roles
- have designated deputies and stand-ins, also possessing appropriate skills.
- have a succession plan in place.

Risk Management

Planned-for and deemed as acceptable levels of risk and risk scenarios must be documented, together with documentation of their acceptance and mitigations.

Copyright © Chris Cracknell 2023, 2026