
L'economia dell'integrità

Cybersecurity, trust services e architettura
dell'Identità Digitale in Europa.

aruba.it

puise

Per gran parte degli ultimi due decenni, la trasformazione digitale è stata valutata principalmente in termini di velocità e scalabilità.

Le organizzazioni hanno accelerato la migrazione delle infrastrutture verso il cloud, automatizzato i processi operativi e introdotto nuove tecnologie con l'obiettivo di superare i competitor sul piano dell'efficienza. La produttività è diventata il principale indicatore di progresso, mentre l'accelerazione ha rappresentato la cifra distintiva dell'economia digitale. Oggi, tuttavia, questa fase evolutiva sta mostrando i suoi limiti.

In Europa, l'attenzione si sta spostando: non si tratta più soltanto di quanto rapidamente i sistemi possano evolvere, ma di quanto le architetture digitali siano affidabili, governabili e resilienti nel tempo. La velocità, da sola, non genera fiducia. In ecosistemi digitali complessi, può al contrario amplificare vulnerabilità e criticità strutturali.

Diversi fattori stanno favorendo questo cambiamento.

La regolamentazione sta diventando un elemento strutturale dell'architettura digitale. Quadri normativi come **GDPR, NIS2, eIDAS 2.0** e **AI Act** stanno ridefinendo le modalità con cui le organizzazioni progettano sistemi, gestiscono identità digitali e presidiano il rischio tecnologico. A partire dal 2026, la direttiva NIS2 introdurrà una responsabilità diretta a livello di consiglio di amministrazione nella governance della cybersecurity, con sanzioni finanziarie fino al 2% del fatturato globale per le entità critiche che non rispettano gli obblighi di gestione del rischio. **La conformità normativa non è più un passaggio che segue l'implementazione delle soluzioni: diventa un requisito progettuale fin dalle prime fasi di sviluppo.**

Parallelamente, anche il contesto tecnologico è profondamente mutato. Le infrastrutture aziendali sono ormai distribuite per impostazione predefinita. Cloud ibridi, piattaforme SaaS, sistemi di operational technology, API, forza lavoro distribuita e sistemi autonomi hanno progressivamente dissolto i confini tradizionali della rete aziendale. Ogni nuova connessione aumenta le capacità operative, ma estende allo stesso tempo la superficie di esposizione e il perimetro di rischio.

All'interno di questi ecosistemi, la costruzione della fiducia digitale è diventata più complessa. I deepfake mettono in discussione l'autenticità delle informazioni, le frodi d'identità si amplificano grazie all'automazione, mentre i sistemi di intelligenza artificiale opachi sollevano nuove problematiche legate a responsabilità, tracciabilità e trasparenza. Le organizzazioni possono continuare a digitalizzare processi e servizi, ma stakeholder, partner e autorità di vigilanza pongono una domanda sempre più centrale: **i sistemi digitali sono realmente affidabili e verificabili nel tempo?**

In risposta a questo scenario, le fondamenta della competizione digitale stanno progressivamente cambiando.

In molti mercati tecnologici globali, la fiducia viene ancora interpretata come un attributo di brand: un elemento comunicato e dichiarato, più che progettato in modo strutturale.

In Europa sta emergendo un approccio differente, in cui la fiducia viene integrata direttamente nell'architettura dei sistemi digitali attraverso quadri normativi, infrastrutture di identità digitale e piattaforme tecnologiche europee.

In questo modello evolutivo, **la fiducia non è più una leva reputazionale, ma diventa una vera e propria infrastruttura operativa.**

La cybersecurity protegge gli ambienti in cui operano identità e dati; i trust services garantiscono la validazione di azioni, transazioni e comunicazioni digitali; la brand protection tutela la presenza pubblica delle organizzazioni nello spazio digitale. L'integrazione di queste capacità consente di preservare l'integrità di dati e identità lungo ogni interazione digitale, assicurando autenticità, attribuzione e responsabilità nel tempo.

In questo contesto, l'integrità si configura come il livello operativo della fiducia nell'economia digitale: la condizione che permette alle organizzazioni di agire, transare e innovare in modo sicuro in ambienti distribuiti, mantenendo al contempo l'agentività digitale, ovvero la capacità di decidere, operare e innovare su infrastrutture affidabili e identità verificabili.

Questa transizione apre la strada a quella che può essere definita **Integrity Economy**.

In un ecosistema di questo tipo, il vantaggio competitivo non deriva esclusivamente dalla disponibilità di tecnologie avanzate, ma dalla capacità di dimostrare un controllo verificabile su infrastrutture, identità digitali, dati e livelli di esposizione al rischio. La differenziazione si sposta quindi dalla semplice adozione tecnologica alla governance strutturata dell'ambiente digitale.

Operativamente, **l'integrità nasce dalla convergenza di tre ambiti fondamentali**: la **cybersecurity**, che difende sistemi e infrastrutture, i **trust services**, che certificano e validano le operazioni digitali, la **brand protection**, che tutela l'identità pubblica delle organizzazioni nello spazio online.

Questi elementi convergono verso un obiettivo unitario: garantire che le identità digitali — insieme alle transazioni, comunicazioni e decisioni ad esse collegate — rimangano autentiche, attribuibili e verificabili nel tempo.

Per le imprese, questo scenario rappresenta un cambiamento profondo nel modo di concepire la trasformazione digitale. Non si tratta più di una sequenza di aggiornamenti tecnologici o di un semplice percorso di modernizzazione delle piattaforme IT. Diventa una disciplina di progettazione sistemica, che connette l'architettura dei data center alla governance delle identità, a cybersecurity ai framework normativi di fiducia e i domini di esecuzione cloud alle responsabilità giurisdizionali. In questa prospettiva, l'integrità rappresenta la condizione che consente ai sistemi digitali di scalare senza perdere controllo.

La prossima fase della trasformazione digitale non sarà quindi guidata da chi si muove più rapidamente, ma da chi sarà in grado di costruire sistemi capaci di sostenere la fiducia nel lungo periodo. La velocità può generare innovazione, ma senza integrità strutturale può anche amplificare il rischio sistemico.

La velocità senza integrità produce fragilità. L'integrità, al contrario, abilita **l'innovazione che perdura nel tempo**.

Sommario

01 Integrità in un mondo dispersivo e regolamentato	7
02 Operazionalizzare l'integrità	9
03 Integrità dalle fondamenta	12
04 Compliance by design.....	14
05 Identità, nucleo dell'integrità	15
06 Il controllo strategico per garantire sicurezza e compliance	18
07 APPENDIX A - Trust services: validità legale by design	21
08 APPENDIX B - Brand Protection	25
09 APPENDIX C - Cybersecurity	29

PERCHÉ ARUBA È UN PUNTO DI RIFERIMENTO NELL'ECONOMIA DELL'INTEGRITÀ

Aruba è il principale operatore europeo di infrastrutture di fiducia digitale

Il Gruppo Aruba, tramite le due Certification Authorities e QTSPs Aruba PEC e Actalis, gestisce ogni anno 1,6 miliardi di firme elettroniche, oltre 9 milioni di caselle di Posta Elettronica Certificata (PEC), più di 2 milioni di identità digitali gestite e oltre 1 milione di certificati SSL attivi.

Pilastro della fiducia digitale in Italia

L'infrastruttura trust di Aruba dà sostegno a 62,4 milioni di tessere sanitarie italiane e 2,7 milioni di domini in gestione. Aruba opera inoltre come registry del dominio .cloud e come attore di primo piano negli ecosistemi dei domini .it, .eu e di altri ccTLD europei.

Impegno fondativo verso la compliance europea

Aruba è membro del Consiglio di Amministrazione di Gaia-X e parte attiva del Digital Clearing House. È inoltre membro fondatore di CISPE e aderisce al relativo Codice di Condotta, integrando i principi europei di protezione dei dati e di conformità al cloud federato all'interno del proprio modello operativo.

1,6MLD

FIRME ELETTRONICHE
GESTITE OGNI ANNO

+9MLN

CASELLE DI POSTA ELETTRONICA
CERTIFICATA (PEC)

+2MLN

IDENTITÀ DIGITALI
GESTITE

+1MLN

CERTIFICATI SSL
ATTIVI

62,4MLN

TESSERE SANITARIE
GESTITE

2,7MLN

DOMINI
IN GESTIONE

evidence box

CAPITOLO 01

Integrità in un mondo dispersivo e regolamentato

L'ambiente digitale in cui operano oggi le organizzazioni è profondamente diverso rispetto alle architetture IT centralizzate del passato.

I sistemi aziendali sono diventati intrinsecamente distribuiti, estendendosi tra infrastrutture cloud ibride, piattaforme SaaS, operational technology, forza lavoro distribuita e processi sempre più automatizzati. Quello che un tempo era un perimetro di rete ben definito si è trasformato in un ecosistema dinamico di servizi interconnessi, in continua evoluzione.

Questa dispersione aumenta le capacità operative, ma modifica radicalmente anche la natura del rischio digitale.

Ogni nuova integrazione, che si tratti di integrazioni API, di dipendenze SaaS, di un dispositivo connesso o di un flusso automatizzato, introduce nuovi canali attraverso cui interruzioni, vulnerabilità o incidenti possono inserirsi. Parallelamente, automazione e intelligenza artificiale comprimono i cicli decisionali, consentendo ai sistemi di operare a una velocità e su una scala che i modelli tradizionali di governance non erano stati progettati per controllare. Il risultato è un contesto in cui complessità operativa ed esposizione sistemica crescono simultaneamente, rendendo più difficile mantenere visibilità e controllo.

In queste condizioni, la gestione del rischio non può più essere considerata una funzione amministrativa o un esercizio periodico di conformità normativa. Diventa un requisito strutturale per garantire resilienza organizzativa, continuità operativa e sicurezza delle infrastrutture digitali.

La regolamentazione europea riflette sempre più chiaramente questa evoluzione. La direttiva NIS2 introduce un modello di governance in cui cybersecurity e continuità operativa non sono più responsabilità limitate ai team tecnici. Le organizzazioni devono dimostrare pratiche di risk management estese all'intera catena del valore, includendo supply chain, fornitori terzi e dipendenze digitali critiche. I consigli di amministrazione sono chiamati a esercitare una supervisione diretta e l'assenza di misure adeguate può comportare sanzioni economiche rilevanti e responsabilità manageriali. La compliance, di conseguenza, non può più essere un processo di verifica a posteriori. Deve essere integrata fin dalla progettazione e incorporata nel funzionamento quotidiano dei sistemi digitali, diventando parte integrante dell'architettura tecnologica e dei modelli operativi.

Molte organizzazioni, tuttavia, incontrano difficoltà nel rendere operativo questo cambiamento. In assenza di una definizione chiara di integrità digitale all'interno del proprio contesto, che comprenda infrastrutture, dati, identità e dipendenze esterne,

gli investimenti in sicurezza tendono a essere pianificati su base reattiva. I controlli vengono introdotti in risposta a incidenti o richieste regolatorie, invece di essere integrati in un modello architetturale coerente e proattivo, capace di allineare governance, cybersecurity e continuità operativa in un'unica visione sistemica.

Questo approccio reattivo è sempre più difficile da sostenere. Gli analisti evidenziano con continuità una carenza strutturale di competenze in cybersecurity, con un gap di talenti che interessa una quota significativa delle imprese europee. In questo scenario, strategie di sicurezza frammentate generano inevitabilmente pressioni economiche e operative.

Diventa quindi necessario passare da controlli di sicurezza isolati a framework di progettazione coerenti, in grado di governare ambienti digitali. In un contesto di questo tipo, **l'integrità smette di essere solo un principio di buona governance e assume una funzione più profonda: diventa la proprietà strutturale che determina la capacità dei sistemi digitali di rimanere governabili mentre crescono in complessità.**

Le organizzazioni che incorporano l'integrità nell'architettura delle infrastrutture, nella gestione delle identità digitali e nei processi operativi sviluppano una maggiore capacità di assorbire shock operativi, adattarsi ai cambiamenti normativi e mantenere il controllo su ecosistemi tecnologici sempre più articolati.

Al contrario, le imprese che non adottano questo approccio tendono a rimanere intrappolate in cicli continui di remediation, interventi correttivi e gestione emergenziale degli incidenti.

La distinzione tra questi due modelli sta diventando sempre più netta e rappresenta, in modo crescente, la differenza tra resilienza digitale duratura e vulnerabilità sistemica persistente.

CAPITOLO 02

Operazionalizzare l'integrità

Perché l'integrità possa diventare una proprietà concreta dei sistemi digitali, e non soltanto un obiettivo strategico, deve tradursi in pratiche operative efficaci e integrate.

In molte organizzazioni, tuttavia, l'architettura della sicurezza riflette ancora l'evoluzione frammentata dell'ambiente digitale stesso. Le infrastrutture possono essere distribuite su più provider cloud, gli strumenti di cybersecurity acquisiti da vendor specializzati, le piattaforme di gestione delle identità gestite separatamente, mentre i framework di governance vengono applicati in maniera successiva per cercare di armonizzare la complessità risultante.

Ogni componente può funzionare efficacemente in isolamento, ma il sistema nel suo complesso spesso manca di un chiaro centro di responsabilità.

Quando si verificano incidenti, la tracciabilità della responsabilità può diventare sfidante. Il compito di gestire rischi e conseguenze è disperso tra provider, piattaforme e domini operativi, pur rimanendo l'organizzazione responsabile delle ricadute operative, legali e reputazionali.

Le evoluzioni regolamentari a livello europeo stanno mettendo in discussione questo modello frammentato.

Quadri normativi come NIS2 enfatizzano la necessità di una governance end-to-end dimostrabile, imponendo alle organizzazioni di comprendere e gestire i rischi lungo l'intero ecosistema digitale. I consigli di amministrazione devono mantenere visibilità sulle esposizioni della supply chain, gli auditor richiedono tracciabilità completa su infrastrutture

ibride, e gli obblighi di reporting degli incidenti si applicano indipendentemente dal fatto che gli incidenti derivino da sistemi interni o servizi esternalizzati. In queste condizioni, l'integrità non può rimanere un principio dichiarativo: deve essere integrata direttamente nel modo in cui i sistemi vengono progettati, gestiti e governati.

Si delineano così due approcci principali per tradurre l'integrità in pratica operativa.

Il primo approccio considera l'integrità soprattutto come una sfida di perimetro. Le organizzazioni aggiungono controlli di sicurezza, ampliano le capacità di monitoraggio e introducono ulteriori procedure di compliance per compensare la frammentazione architetturale. Sebbene queste misure possano migliorare la visibilità, spesso restano sovrapposte alla complessità esistente e dipendono fortemente dalla coordinazione tra molteplici provider esterni.

Il secondo approccio affronta il problema a un livello più strutturale e integrato. Invece di limitarsi a compensare la frammentazione, punta a ridurla attraverso l'allineamento di ownership infrastrutturale, sicurezza operativa, connettività e trust framework all'interno di un'architettura coerente.

In questo modello, l'integrità non viene aggiunta come layer di controllo esterno, ma diventa una proprietà intrinseca del sistema stesso.

Il modello operativo di Aruba si è sviluppato seguendo questa seconda logica.

Molto prima che concetti come la sovranità digitale diventassero centrali nelle politiche tecnologiche europee, Aruba ha investito nello sviluppo e nella gestione

diretta delle proprie infrastrutture. Strutture di data center, ambienti cloud europei e operazioni di sicurezza interne sono state progettate per supportare servizi mission-critical su scala nazionale. **Caratteristiche come resilienza energetica, segregazione logica, auditabilità e governance delle identità non sono state introdotte come elementi di marketing, ma come requisiti operativi essenziali per garantire continuità e fiducia.**

Con il tempo, queste discipline operative si sono evolute in un portafoglio integrato di Trust & Security.

La differenza tra questo approccio e ecosistemi più frammentati è strutturale.

Le pratiche di sicurezza sviluppate per proteggere infrastrutture critiche sotto responsabilità operativa diretta, incluse procedure di Security Operations Center, cicli di gestione delle vulnerabilità, framework di audit, governance del ciclo di vita delle identità e modelli di continuità testati, derivano da un'esposizione operativa continua. Esse riflettono sistemi progettati per funzionare in modo affidabile in condizioni reali, piuttosto che architetture assemblate prevalentemente attraverso integrazioni contrattuali.

Questa coerenza verticale modifica il modo in cui il rischio viene distribuito.

Quando infrastrutture, ambienti cloud, operazioni di cybersecurity, connettività e servizi di trust operano all'interno di una catena di responsabilità unificata, la governance diventa più trasparente. Il controllo architetturale si allinea con la responsabilità operativa, riducendo la probabilità che il rischio venga disperso su più livelli esterni e frammentati. Per le organizzazioni che operano in settori regolamentati, questa coerenza ha implicazioni operative concrete. Piuttosto che costruire architetture di compliance complesse in modo

indipendente, spesso sotto pressione normativa e con carenze di talenti in cybersecurity, le imprese possono fare affidamento su modelli operativi già sviluppati in contesti di governance stringente.

In questo senso, l'integrità diventa una disciplina operativa trasferibile.

Un approccio di questo tipo non elimina completamente la complessità, ma introduce punti di riferimento architetturali che riducono la frammentazione e chiariscono i confini giurisdizionali.

All'interno di un'economia digitale dispersiva, la domanda che le organizzazioni si trovano sempre più spesso a porsi non riguarda solo la sicurezza dei singoli sistemi, ma se l'integrità sia strutturalmente incorporata in tutto lo stack digitale: dall'infrastruttura fisica su cui operano i servizi alle identità attraverso cui le azioni vengono autorizzate.

Operazionalizzare l'integrità richiede quindi più della semplice aggiunta di strumenti di sicurezza. È necessario allineare ownership infrastrutturale, governance delle identità, operazioni di cybersecurity e legal trust framework all'interno di una logica di progettazione coerente.

Quando questi elementi operano in sinergia, l'integrità cessa di essere un mero obiettivo di conformità e diventa un principio organizzativo, fulcro centrale del modello operativo digitale stesso.



CAPITOLO 03

Integrità dalle fondamenta

L'integrità digitale non può essere raggiunta attraverso l'aggiunta di un layer di sicurezza a sistemi esistenti. In ambienti digitali complessi, la fiducia deve essere costruita direttamente nell'architettura, partendo dalle fondamenta fisiche su cui poggia l'infrastruttura digitale.

Alla base si trova il substrato fisico. La progettazione dei data center, la ridondanza energetica, le misure di salvaguardia ambientale e la collocazione geografica determinano la resilienza di base delle operazioni digitali.

La disponibilità non è un semplice obiettivo astratto di livello di servizio, ma il risultato di una continuità ingegnerizzata che integra energia, cooling e controllo infrastrutturale. È anche a questo livello che emergono questioni di giurisdizione e localizzazione dei

dati, poiché l'infrastruttura fisica definisce l'ambiente legale in cui i sistemi digitali operano realmente.

Sopra questa base poggia il dominio di esecuzione, dove operano dati e applicazioni. Gli ambienti cloud europei operanti sotto giurisdizione europea forniscono le condizioni per un'esecuzione dei carichi di lavoro controllata, garantendo separazione logica, operazioni auditabili e governance coerente su architetture ibride o multi-cloud.

In questo contesto, **la sovranità non è un semplice impegno contrattuale, ma una proprietà architeturale concreta, modellata dalla proprietà dell'infrastruttura, dal controllo operativo e dall'allineamento normativo.**

Al di sopra del dominio di esecuzione si colloca il perimetro dinamico di sicurezza. Gli ambienti digitali moderni sono costantemente esposti a minacce in evoluzione che interessano reti, applicazioni e asset digitali esterni. Le capacità di cybersecurity gestita, tra cui rilevamento e risposta continua, gestione delle vulnerabilità, monitoraggio della superficie di attacco e protezione della presenza digitale, contribuiscono a garantire la continuità operativa in un contesto caratterizzato da esposizione costante ai rischi.

Sempre più, questo perimetro si estende anche alla tutela dell'identità digitale e al brand. Domini, configurazioni DNS e asset di identità online rappresentano componenti critiche della fiducia organizzativa. Domini fraudolenti, campagne di impersonificazione e manipolazione di asset digitali possono compromettere la credibilità in poche ore, rendendo essenziali il monitoraggio proattivo e la risposta rapida per mantenere l'integrità della presenza digitale dell'organizzazione.

Al livello più alto si colloca l'infrastruttura formale di fiducia. I servizi trust qualificati, come firme digitali, sigilli elettronici, marcature temporali, infrastrutture a chiave pubblica e framework di identità conformi a eIDAS 2.0, traducono i meccanismi tecnici di sicurezza in azioni digitali legalmente riconosciute.

Questi servizi collegano transazioni, documenti e comunicazioni a identità responsabili, operanti all'interno di framework regolatori certificati.

L'emergere dei wallet di identità digitale europei, sia per cittadini che per organizzazioni, evidenzia l'evoluzione di questo livello di trust. Questi strumenti, oltre a svolgere funzioni di autenticazione, supportano individui e organizzazioni nel gestire identità, autorizzazioni e deleghe all'interno di ecosistemi verificabili.

Considerati nel loro insieme, questi livelli costituiscono un sistema interdipendente.

La resilienza fisica supporta gli ambienti di esecuzione europei; l'infrastruttura europea facilita la conformità normativa; le capacità di cybersecurity mantengono la continuità operativa; i servizi fiduciari assicurano la validità legale delle azioni digitali.

In questo contesto, l'integrità non rappresenta una singola capacità, ma una proprietà sistemica dell'intero stack digitale.

Essa emerge quando infrastruttura, sicurezza, gestione delle identità e meccanismi di trust legale sono progettati per operare in modo coerente, dalla base fisica fino ai livelli più alti delle interazioni digitali.

CAPITOLO 04

Compliance by design

Diffusamente, la compliance rimane ancora episodica. Spesso si manifesta come un processo guidato da audit, che mette in luce le debolezze strutturali nel momento in cui l'attenzione regolatoria vi si focalizza.

Sebbene questo approccio fosse gestibile in contesti tecnologici più stabili, oggi risulta sempre più difficile da sostenere.

Negli ecosistemi digitali caratterizzati da automazione, intelligenza artificiale e normative complesse, la compliance non può essere considerata un semplice passaggio di verifica finale da aggiungere dopo la costruzione dei sistemi. Deve invece essere integrata nella progettazione dell'architettura digitale fin dalle fasi iniziali.

Raggiungere questo obiettivo richiede un cambiamento di approccio verso il “compliance by design”, in cui governance, gestione delle identità e controlli di cybersecurity sono incorporati in modo strutturale lungo l'intero stack tecnologico.

Concretamente, significa che molti elementi tradizionalmente associati alla compliance diventano componenti fondamentali dell'architettura del sistema. Meccanismi di logging, separazione dei ruoli, gestione robusta delle identità, servizi trust integrati, soluzioni di business continuity e workflow operativi auditabili vengono progettati all'interno dei sistemi, anziché essere aggiunti successivamente come layer separati.

All'interno di un'architettura di questo tipo, i requisiti normativi derivanti da framework come NIS2, GDPR, DORA, eIDAS 2.0 e AI Act non vengono percepiti come requisiti esterni. Al contrario, essi si riflettono direttamente nel funzionamento dei sistemi digitali, nella gestione degli accessi e nella generazione delle evidenze operative.

Di conseguenza, la governance cessa di essere un'attività occasionale legata ad audit periodici e si trasforma in una disciplina operativa continua, integrata nel ciclo di vita dei sistemi digitali.

Le implicazioni di questa transizione non sono soltanto regolatorie, ma anche economiche. Quando la compliance è strutturalmente incorporata nei sistemi digitali, le organizzazioni riducono i costi a lungo termine legati a interventi reattivi, strumenti frammentati e ripetuti ridisegni architetturali. Allo stesso tempo, possono innovare all'interno di confini di governance chiaramente definiti, accelerando l'adozione di nuove tecnologie senza compromettere il controllo sull'esposizione al rischio.

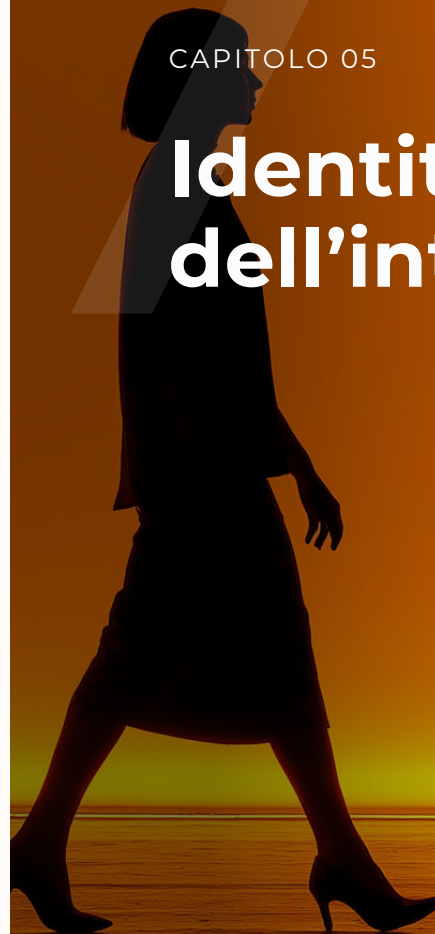
Ancora più importante, **la compliance assume una dimensione culturale.**

Quando responsabili della sicurezza, data protection officer, team tecnologici e leadership operano secondo principi architetturali condivisi, la governance si allinea alla strategia organizzativa, invece di essere percepita come un vincolo esterno. La compliance smette di essere vista esclusivamente come un obbligo difensivo e diventa un meccanismo attraverso cui l'organizzazione mantiene chiarezza operativa e responsabilità verificabile.

Negli ecosistemi digitali maturi, la governance non è più una fonte di attrito. Si integra nella logica di progettazione, consentendo ai sistemi complessi di funzionare in modo affidabile e scalabile.

CAPITOLO 05

Identità, nucleo dell'integrità



L'integrità digitale converge sui temi di identità.

Ogni sistema digitale, che sia cloud-native, automatizzato o basato su Intelligenza Artificiale, dipende dalla capacità di attribuire le azioni a soggetti identificabili, operanti sotto autorità definite. In assenza di meccanismi affidabili di attribuzione, diventa difficile stabilire responsabilità e i framework di governance perdono efficacia. L'identità, quindi, agisce come meccanismo attraverso cui vengono garantite responsabilità, autorità e tracciabilità all'interno degli ambienti digitali.

Per il fattore umano coinvolto — dipendenti, clienti e cittadini — la governance delle identità richiede una gestione completa del ciclo di vita.

Procedure sicure di onboarding, meccanismi di autenticazione robusti, controlli di autorizzazione granulari, tracciabilità delle azioni e revoca tempestiva dei privilegi contribuiscono a mantenere interazioni digitali affidabili e verificabili. In questo senso, la gestione delle identità va ben oltre la semplice autenticazione: costituisce un framework di governance che definisce come gli individui interagiscono con i sistemi e tra loro, garantendo sicurezza, trasparenza e responsabilità operativa.

Parallelamente, le architetture digitali moderne introducono un numero crescente di **identità non umane**. Applicazioni, API, servizi, tenant e workload cloud necessitano di meccanismi che ne consentano l'autenticazione e l'interazione sicura.

Certificati, chiavi crittografiche e politiche di accesso basate sui ruoli devono quindi riflettere le responsabilità effettive e i confini operativi entro cui queste entità operano. Nei sistemi distribuiti, l'autenticazione servizio-servizio diventa altrettanto critica quanto quella degli utenti tradizionali.

L'emergere delle **machine identities** amplia ulteriormente questo scenario. Dispositivi, sensori, container, workflow automatizzati e AI-agent eseguono ora azioni in autonomia e su larga scala. Ciascuna di queste entità necessita di un'identità verificabile, attraverso la quale la propria attività possa essere autenticata, autorizzata e monitorata. Senza infrastrutture a chiave pubblica strutturate e gestione robusta del ciclo di vita, il numero di interazioni automatizzate può crescere più rapidamente dei meccanismi di governance progettati per controllarle, aumentando il rischio di esposizione e perdita di controllo.

All'interno di questo contesto in evoluzione, AI-agent rappresentano un caso particolarmente rilevante. Piuttosto che configurarsi come nuovi attori giuridici, questi sistemi operano come estensioni delegate di identità e responsabilità esistenti.

La loro autorità deriva da meccanismi espliciti di delega, tra cui identity wallet, attestazioni crittografiche e framework normativi definiti, attraverso i quali le organizzazioni specificano quali azioni un agente automatizzato può eseguire e in quali condizioni.

Questo approccio garantisce che l'automazione rimanga ancorata a strutture di governance responsabili e verificabili. L'autonomia può aumentare l'efficienza operativa, ma deve sempre operare all'interno di limiti di autorità verificabili.

I framework europei di identità assumono un ruolo chiave nel rafforzare questo allineamento tra autenticazione tecnica e responsabilità legale. I servizi trust qualificati e i meccanismi di identità definiti da **eIDAS 2.0**, tra cui firme digitali, sigilli elettronici, marcature temporali e i modelli emergenti basati su wallet digitali, collegano le azioni digitali a attori identificabili all'interno di quadri giurisdizionali riconosciuti.

Con il crescente coinvolgimento dei sistemi di intelligenza artificiale nei processi operativi e decisionali, la governance delle identità diventa un pilastro fondamentale della responsabilità digitale.

L'automazione che opera senza strutture identitarie chiare rischia di generare opacità anziché efficienza.

Le organizzazioni che sviluppano framework identitari coerenti mantengono la capacità di governare ecosistemi digitali complessi, mentre chi trascura questa dimensione spesso si trova a dover affrontare una situazione in cui la capacità tecnologica cresce più rapidamente della supervisione possibile.

Un solido tessuto identitario diventa quindi essenziale per sostenere il controllo strategico: la capacità delle organizzazioni di adottare nuove tecnologie, scalare processi automatizzati e integrare sistemi di AI pur mantenendo controllo su autorità e responsabilità.

Quando la governance delle identità è incorporata strutturalmente, l'innovazione rimane governabile e trasparente, anziché opaca.

Con l'evoluzione degli ecosistemi digitali, diverse discipline tradizionalmente considerate domini separati, operazioni di cybersecurity, servizi fiduciari e protezione del brand, convergono sempre più verso un obiettivo comune: preservare l'integrità dell'identità digitale e delle azioni ad essa associate.

La cybersecurity protegge sistemi e infrastrutture attraverso cui le identità operano, i trust services vincolano transazioni, comunicazioni e documenti a identità legalmente riconosciute, preservandone autenticità, intenzionalità e tracciabilità temporale, la brand protection tutela l'espressione pubblica dell'identità organizzativa attraverso domini, comunicazioni e asset digitali.

L'integrazione di queste capacità costituisce livelli complementari di Digital Integrity, garantendo che identità, transazioni e comunicazioni rimangano **autentiche, attribuibili e verificabili** all'interno di ecosistemi digitali complessi.

CAPITOLO 06

Il controllo strategico per garantire sicurezza e compliance

L'obiettivo di una trasformazione digitale matura non consiste nell'accumulare tecnologie, ma nello sviluppo del controllo strategico: la capacità delle organizzazioni di scegliere, comporre e governare infrastrutture, dati, Artificial Intelligence e identità all'interno di confini architetturali e giurisdizionali chiari.

Negli ecosistemi digitali sempre più complessi, la capacità di mantenere questo controllo sta diventando una competenza strategica distintiva.

I sistemi che scalano rapidamente ma restano opachi o dipendenti da attori esterni possono generare efficienza a breve termine, ma spesso indeboliscono la capacità dell'organizzazione di gestire il rischio, rispettare regolamenti in evoluzione e adattare nel tempo la propria traiettoria tecnologica.

In Europa, iniziative emergenti legate a ecosistemi cloud federati e framework di sovranità digitale dimostrano che scala e governance non sono necessariamente incompatibili. Ambienti digitali su larga scala possono rimanere interoperabili, conformi e resilienti senza che le organizzazioni debbano rinunciare al controllo su infrastrutture, identità o dati. Quando l'integrità è progettata all'interno dell'architettura di base, performance e localizzazione dei dati possono coesistere.

Guardando al futuro, diversi sviluppi strutturali sono destinati a influenzare l'evoluzione della Digital Integrity.

Uno degli ambiti critici riguarda la **resilienza crittografica**. L'emergere delle capacità di computing quantistico è destinato a mettere alla prova i modelli di crittografia



attuali, trasformando la preparazione a lungo termine in materia di sicurezza digitale da aggiornamento tecnico a questione di pianificazione strategica. Le organizzazioni che iniziano oggi a predisporre ambienti crittografici post-quantum saranno meglio posizionate per preservare la durata dei propri framework di fiducia digitale.

Un secondo vettore riguarda la **crescita rapida delle machine identities**. Agenti AI, workflow automatizzati e sistemi autonomi eseguono sempre più attività operative su infrastrutture digitali distribuite. Governare questi sistemi richiede modelli chiari di delega, gestione del ciclo di vita e strutture di autorità verificabili, capaci di garantire che l'attività automatizzata resti attribuibile e responsabile.

Un terzo cambiamento riguarda la **gestione continua della postura di sicurezza in ambienti ibridi e multi-cloud**. Con l'aumento della distribuzione delle infrastrutture, la resilienza non può più basarsi solo su valutazioni periodiche. La supervisione della sicurezza deve evolvere in un processo continuo, in grado di monitorare l'esposizione, adattarsi alle minacce emergenti e mantenere l'integrità operativa su sistemi interconnessi.

Le organizzazioni che integrano l'integrità strutturalmente fin dall'inizio conservano un grado di opzionalità tecnologica: possono far evolvere architetture, integrare nuove tecnologie e adottare capacità basate su AI senza accumulare rischi strutturali nascosti.

Al contrario, i sistemi in cui la sicurezza resta uno strato esterno sovrapposto possono apparire innovativi a breve termine, ma aumentano gradualmente la fragilità complessiva.

In questo contesto, la sicurezza non deve essere interpretata come un semplice strato difensivo. Quando è integrata correttamente, diventa il meccanismo attraverso cui le organizzazioni proteggono le condizioni necessarie all'innovazione digitale.

Dall'infrastruttura fisica agli ambienti di esecuzione cloud, dalle operazioni di cybersecurity alla brand protection e alla legal trust validation, tutti questi meccanismi convergono nella protezione dell'identità digitale stessa, garantendo che le azioni eseguite nel mondo digitale rimangano autentiche, attribuibili e durature nel tempo.

Con la maturazione dell'ecosistema digitale europeo, **la fiducia sta progressivamente evolvendo da attributo reputazionale a componente strutturale dell'infrastruttura**. Le organizzazioni in grado di ingegnerizzare questa integrità all'interno dei propri sistemi saranno le meglio posizionate per sostenere l'innovazione pur mantenendo il controllo sugli ambienti in cui operano.



APPENDIX / A

Trust services: validità legale by design

All'interno del framework di Digital Integrity descritto in questo documento, i Trust Services rappresentano il livello di validazione legale che collega le azioni digitali a identità responsabili e verificabili.

Validità legale by Design

I Trust Services costituiscono l'apice della Digital Integrity, trasformando azioni tecniche in realtà legalmente vincolante e verificabile. In un contesto regolatorio definito da eIDAS 2.0, NIS2, GDPR, AI Act e framework digitali nazionali, autenticità e non ripudiabilità non sono più dettagli procedurali, ma requisiti strutturali.

L'integrità richiede che identità, intenzione, tempo e consegna possano essere dimostrati e verificati.

Come Qualified Trust Service Provider e una delle principali Certification Authority europee, con Actalis come prima CA dell'UE, Aruba opera su scala continentale.

Oltre 1,6 miliardi di firme digitali all'anno e più di 10 milioni di caselle PEC testimoniano non solo l'adozione di mercato, ma la rilevanza sistemica. La fiducia a questa scala non è una funzione opzionale: è infrastruttura. I Trust Services rappresentano il livello di validazione legale dell'intero stack digitale.

Strumenti operativi per l'Integrity Economy

All'interno della Integrity Economy, i Trust Services qualificati non sono accessori di compliance, ma strumenti operativi. Actalis e Aruba PEC, come Qualified Trust Service Provider, costituiscono un'infrastruttura fiduciaria legalmente riconosciuta, che garantisce autenticità, integrità e non ripudiabilità nelle interazioni digitali.

Firme digitali, certificati qualificati (QWAC e QSEALC), crittografia SSL/TLS e sistemi di posta elettronica certificata (PEC) assicurano immutabilità e tracciabilità, requisiti sempre più stringenti in ottica NIS2. In ambienti regolamentati, la possibilità di dimostrare che una transazione è autentica, marcata temporalmente e inalterata non è più opzionale: è esigibile.

Dalla sicurezza tecnica alla certezza legale

I sistemi digitali possono essere sicuri senza essere legalmente vincolanti. I Trust Services colmano questo gap. La Certified Platform di Aruba integra firme digitali, marcature temporali, PEC, identità digitale, conservazione digitale e fatturazione elettronica conforme in un'architettura unificata.

Ospitata su infrastruttura europea e integrata in controlli di sicurezza end-to-end, la piattaforma garantisce che ogni interazione sia:

- autenticata;
- marcata temporalmente;
- tracciabile;
- legalmente valida;
- conforme alla normativa.

Si tratta di compliance by design, non basata su strumenti aggiuntivi. I Trust Services incorporano i requisiti normativi nei pattern architetturali: logging nativo, verifica robusta delle identità, separazione dei ruoli, governance del ciclo di vita e audit trail non ripudiabili. La responsabilità a livello di board, formalizzata sempre più sotto NIS2, diventa dimostrabile operativamente. L'integrità diventa verificabile.

Le cinque dimensioni dell'integrità legale

I Trust Services di Aruba si articolano in cinque garanzie complementari:

1 / PROOF OF IDENTITY

Framework di identità digitale, certificati qualificati (QWAC, QSEALC) e sistemi wallet-based assicurano che attori, individui, organizzazioni e agenti delegati, siano verificabilmente autenticati. La governance dell'identità copre lifecycle management, revoca e tracciabilità.

In contesti AI, questa dimensione è fondamentale: un agente AI non è un nuovo soggetto legale, ma una proiezione delegata di un'identità responsabile. I Trust Services garantiscono che la delega resti esplicita, delimitata e auditabile.

2 / PROOF OF INTENT

Firme elettroniche qualificate e sigilli vincolano l'intenzione all'identità, eliminando ambiguità in contratti, approvazioni, autorizzazioni e dichiarazioni formali. Applicate su larga scala, sostituiscono l'attrito con certezza verificabile.

3 / PROOF OF TIME

Marcature temporali qualificate ancorano le azioni digitali a quadri temporali riconosciuti. Nei settori regolamentati, questo non è un dettaglio procedurale, ma integrità probatoria.

4 / PROOF OF DELIVERY

La posta elettronica certificata (PEC e sistemi e-delivery conformi) garantisce trasmissione legalmente riconosciuta e non ripudiabile. Con oltre 10 milioni di caselle PEC gestite, Aruba opera una delle infrastrutture centrali della fiducia digitale italiana ed europea.

5 / PROOF OF PRESERVATION

La conservazione digitale conforme assicura che documenti fiscali, contrattuali e amministrativi rimangano autentici, accessibili e legalmente validi nel tempo. La conservazione non è semplice storage: è continuità regolata e garantita.

Queste garanzie integrate inseriscono la fiducia digitale in ogni interazione, assicurando integrità, conformità e resilienza.

L'Identità Digitale come ancora di autenticità

In un panorama fiduciario frammentato, meccanismi di identità come SPID, CIE e i futuri European Digital Identity Wallet forniscono governance strutturata delle identità su scala continentale. Questi framework garantiscono che firme digitali, controlli di accesso e comunicazioni certificate siano legate a identità verificabili e riconosciute dallo Stato.

Con l'evoluzione verso wallet digitali interoperabili sotto eIDAS 2.0, l'identità diventa programmabile, portatile e legalmente vincolante. I Trust Services operano quindi non solo come strumenti di validazione, ma come ancore identitarie in un'economia digitale sempre più decentralizzata.

Scala, integrazione e sovranità

I Trust Services non sono strumenti isolati. Essi sono integrati nell'architettura end-to-end di Aruba.

Ospitati in data center Tier IV sotto normativa europea, integrati con ambienti cloud europei e servizi di cybersecurity gestita, i Trust Services operano all'interno di una catena di responsabilità unificata. Proprietà dell'infrastruttura, sicurezza operativa e validazione legale convergono.

Questa coerenza verticale riduce la frammentazione, allinea l'esecuzione tecnica con la chiarezza giurisdizionale e trasforma la compliance in vantaggio competitivo.

Su questa scala, il modello supporta:

- trasformazione digitale nella Pubblica Amministrazione;
- workflow in settori regolamentati;
- interoperabilità identitaria transfrontaliera;
- automazione aziendale e governance AI.

Milioni di utenti e partner si affidano quotidianamente a questa infrastruttura. La fiducia, qui, è misurabile.

La compliance come vantaggio competitivo

In molte organizzazioni, la compliance è episodica e reattiva. I Trust Services invertiscono questo paradigma. Integrando meccanismi fiduciari qualificati fin dal "Day Zero", le imprese riducono il friction audit, accelerano l'accesso al mercato e rafforzano la fiducia di assicuratori e investitori.

Le firme digitali eliminano i colli di bottiglia cartacei, la posta certificata riduce l'ambiguità legale e la governance identitaria chiarisce le catene di responsabilità. La sicurezza abilita l'evoluzione digitale. Quando la fiducia è incorporata strutturalmente, l'innovazione non accumula debito di rischio, ma opera all'interno di confini verificabili.

In un'economia dell'integrità europea, questa distinzione è cruciale: i mercati premiano chi può dimostrare controllo su identità, documenti e validità legale, non solo semplicemente affermarlo.

Un percorso componibile verso l'integrità

I Trust Services sono modulari by design. Le organizzazioni possono partire da un singolo componente, firma elettronica, PEC, identità digitale o conservazione digitale a norma, e integrare progressivamente capacità più ampie lungo i workflow. Con la maturazione dei sistemi, la fiducia diventa sistemica, non solo transazionale.

Questo modello componibile supporta la capacità di avere controllo strategico, quindi scegliere, orchestrare ed evolvere l'architettura digitale senza rinunciare alla governance. In questo contesto, l'integrità non è un principio astratto, ma una disciplina operativa.

Validità legale come infrastruttura

Dalla verifica delle identità alla marcatura temporale, dalla consegna certificata alla conservazione, i Trust Services di Aruba trasformano la regolamentazione in architettura e l'architettura in fiducia verificabile.

Essi costituiscono il motore di validazione legale dell'intero stack digitale. Nell'era digitale matura europea, la fiducia non è più un attributo, è infrastruttura.

E l'infrastruttura, quando progettata con integrità, diventa la base della crescita sicura.

APPENDIX / B

Brand Protection

All'interno del framework Digital Integrity, la Brand Protection tutela l'espressione esterna dell'identità organizzativa su domini, comunicazioni e asset digitali.

Integrità al confine digitale

Se i Trust Services rappresentano il layer di validazione legale, la Brand Protection protegge il fronte più esposto: il digital edge.

Oggi la reputazione viaggia alla velocità della rete. Un dominio fraudolento, un'email contraffatta, un sito clonato o un'identità impersonata possono compromettere la fiducia in poche ore. In contesti modellati da phishing AI-enabled, impersonazioni automatizzate e social engineering sofisticato, il brand stesso diventa superficie di attacco.

La Digital Integrity si estende quindi oltre infrastruttura e governance identitaria, proteggendo il perimetro visibile dove gli utenti incontrano l'organizzazione. La Brand Protection tutela l'identità laddove è più visibile: al confine digitale.

La nuova superficie di attacco: la reputazione

Il perimetro digitale non è più definito solo dai firewall, esso comprende:

- domini e sottodomini;
- configurazioni DNS;
- marchi e loghi;
- servizi pubblici online;
- infrastrutture email;
- asset di identità digitale.

Ogni dominio registrato a scopo fraudolento, ogni estensione typo-squatted e ogni campagna di impersonation non è un semplice fastidio tecnico, ma un attacco diretto al capitale reputazionale. In quella che molti analisti definiscono una “recessione della fiducia”, le organizzazioni non possono permettersi protezione reattiva. Visibilità, monitoraggio e recupero rapido diventano attività continue.

Gestione dei domini come controllo strategico

La governance dei domini spesso è percepita come attività amministrativa, ma in realtà è infrastruttura strategica.

Aruba gestisce oltre 2,7 milioni di domini ed è registry operator ufficiale per l'estensione .cloud. Questa scala riflette capacità operativa, autorità giurisdizionale e tecnica.

La gestione dei domini include:

- registrazione e rinnovo su estensioni globali;
- procedure sicure di trasferimento;
- razionalizzazione del portafoglio;
- governance della configurazione DNS;
- supervisione del ciclo di vita.

Nei settori regolamentati, la cattiva gestione dei domini può comportare esposizione normativa sotto NIS2.

Il board deve avere visibilità sugli asset digitali oltre l'infrastruttura centrale. Il controllo dei domini, quindi, è strutturale, non formale.

Monitoraggio continuo dei domini

In ecosistemi digitali dispersivi, le minacce emergono spesso fuori dai confini organizzativi diretti. I servizi di Domain Monitoring identificano proattivamente:

- typo-squatting e domini simili;
- registrazioni fraudolente;
- tentativi di impersonation del brand;
- attività DNS sospette.



Alert automatici e workflow investigativi riducendo i tempi di risposta e limitano il danno reputazionale. La visibilità precoce supporta i principi di compliance by design.

Sotto NIS2 e framework correlati, la consapevolezza e la segnalazione degli incidenti sono obbligatorie, trasformando la protezione del brand da remediation reattiva a resilienza operativa.

Recupero e intermediazione: ripristinare il controllo

Quando gli asset digitali sfuggono al controllo legittimo, per scadenza, registrazione ostile o frammentazione legacy, il recupero diventa strategico.

Aruba fornisce negoziazione, intermediazione e processi strutturati per domini contestati o scaduti. Questa capacità non è meramente transazionale: ripristina il controllo su componenti identitarie digitali che altrimenti comprometterebbero la strategia di brand a lungo termine.

Marchi e autorità legale

La protezione del brand si estende oltre i domini alla riconoscibilità legale.

Verifica, registrazione, monitoraggio e rinnovo di marchi a livello nazionale, europeo e internazionale garantiscono che gli asset del brand siano non solo gestiti tecnicamente, ma difendibili legalmente.

Integrazione sull'intero stack digitale

La Brand Protection si integra con:

- servizi gestiti di cybersecurity (SOC, threat intelligence, mitigazione DDoS);
- framework di governance identitaria;
- trust Services (per comunicazioni e consegne verificate);
- infrastruttura europea e controllo DNS.

Quando il monitoraggio domini si connette alla telemetria SOC, la risposta è coordinata. Quando i meccanismi di posta certificata convalidano le comunicazioni ufficiali, il rischio di impersonation diminuisce. Quando la governance identitaria allinea asset di brand, la responsabilità si rafforza.

Sovranità dell'infrastruttura come fondamento dell'integrità del brand

La Brand Protection si rafforza quando gli asset digitali operano su infrastruttura europea.

Gli ambienti Private Cloud e Bare Metal di Aruba Enterprise forniscono infrastruttura controllata e giurisdizionalmente ancorata per workload ad alta intensità di dati, iniziative Private AI e applicazioni mission-critical.

In un modello di sicurezza senza perimetro tradizionale, dove dati e applicazioni operano in ambienti ibridi, la sovranità infrastrutturale garantisce il controllo su DNS, domini e sistemi identitari.

Da protezione a vantaggio competitivo

Nei mercati digitali maturi, la fiducia è misurabile.

Gli investitori valutano l'esposizione al rischio, gli assicuratori analizzano la postura cyber, gli organi regolatori effettuano controlli sulla supply chain, i clienti richiedono autenticità

La Brand Protection riduce l'incertezza su tutti questi fronti. Integrando governance proattiva dei domini, monitoraggio continuo e allineamento legale, nei modelli operativi le organizzazioni:

- riducono la volatilità reputazionale
- rispondono agli incidenti in tempi più rapidi
- provano diligenza regolatoria
- rafforzano la fiducia degli stakeholder

La compliance diventa vantaggio competitivo. La sicurezza abilita l'evoluzione digitale.

Un modello componibile per una fiducia sostenibile

I servizi di Brand Protection sono progettati in modo modulare.

Le organizzazioni possono iniziare con il consolidamento o il monitoraggio dei domini ed evolvere progressivamente verso una governance integrata degli asset digitali.

Con la crescita degli ecosistemi, l'identità del brand diventa sempre più distribuita tra piattaforme, geografie e partner. L'integrità al digital edge garantisce che l'espansione non generi esposizioni non gestite.

La protezione del brand deve quindi funzionare come una disciplina di governance, non come una misura di sicurezza reattiva.

Integrità al digital edge

La Digital Integrity non è confinata ai data center o ai certificati di identità. Si estende a ogni punto in cui l'organizzazione è visibile, ricercabile e contattabile.

A questo confine, la fiducia è fragile.

La Brand Protection protegge questa frontiera, preservando l'autenticità, prevenendo le impersonificazioni e garantendo che la presenza digitale rimanga allineata con identità legale e responsabilità operativa.

Dall'infrastruttura fisica fino alla registrazione dell'ultimo dominio, l'integrità deve essere continua. Nell'economia europea dell'integrità, il brand non è solo un asset.

È una responsabilità.

APPENDIX / C

Cybersecurity

All'interno del framework Digital Integrity, la Cybersecurity protegge i sistemi e le infrastrutture attraverso cui operano le identità digitali.

Resilienza continua su larga scala

Se i Trust Services garantiscono la validità legale e la Brand Protection protegge il digital edge, la Cybersecurity operazionalizza l'integrità lungo il perimetro dinamico. In ecosistemi distribuiti, ibridi e guidati dall'AI, la sicurezza non è più una funzione di confine, ma una disciplina continua.

Forza lavoro remota, ambienti multi-cloud, dipendenze SaaS, tecnologie operative, integrazioni API e sistemi autonomi hanno dissolto il perimetro tradizionale. Ogni connessione diventa un potenziale punto di ingresso, ogni integrazione introduce nuove interdipendenze. In questo contesto, la resilienza non può basarsi su controlli statici.

La sicurezza deve essere progettata by design e governata by default.

Dai controlli alla resilienza coerente

Molte organizzazioni costruiscono la cybersecurity come una raccolta di strumenti: firewall, protezione degli endpoint, dashboard di monitoraggio.

Pur essendo necessari, questi controlli restano spesso frammentati, generando visibilità senza una responsabilità unificata. Il modello di cybersecurity di Aruba è strutturato in modo diverso.

Allineato al NIST Cybersecurity Framework, integra prevenzione, rilevamento, risposta e recupero in una disciplina operativa coerente. La sicurezza non è un overlay, ma è incorporata nell'infrastruttura, nella governance delle identità e nei processi operativi. L'integrità dell'intero stack digitale richiede continuità della protezione, dalle strutture fisiche ai workload cloud, dalle applicazioni alle identità degli utenti.

La cybersecurity garantisce la continuità di questa protezione.

Il perimetro dinamico

Le superfici di attacco moderne sono fluide e comprendono:

- cloud-native applications;
- web services and APIs;
- hybrid e multi-cloud architectures;
- industrial e IoT systems;
- user endpoints e remote access environments.

Gestire questa complessità richiede sorveglianza continua, non valutazioni periodiche.

Il portafoglio di cybersecurity di Aruba combina diverse capacità operative progettate per proteggere ambienti digitali distribuiti.

Vulnerability Assessment & Penetration Testing (VAPT)

Scansioni strutturate delle vulnerabilità e test di intrusione simulati consentono di identificare le debolezze prima degli attaccanti.

Queste attività non rappresentano solo diagnosi tecniche, ma supportano direttamente la prontezza alla compliance rispetto a NIS2 e alle normative settoriali, trasformando la sicurezza in uno strumento di governance preventiva.

Web Application Protection (WAP)

I meccanismi di protezione delle applicazioni web difendono da tentativi di sfruttamento, attacchi di injection e traffico malevolo.

In ecosistemi digitali in cui l'interazione con clienti e partner avviene principalmente tramite interfacce web, la protezione a livello applicativo diventa essenziale per preservare fiducia e continuità operativa.

Managed SOC & Continuous Monitoring

Un Security Operations Center attivo 24/7 monitora ambienti cloud e on-premise, correlando la telemetria, analizzando anomalie e coordinando le attività di risposta agli incidenti. Il rilevamento continuo riduce il dwell time e trasforma la gestione degli

incidenti in una disciplina basata su evidenze, migliorando tempi di reazione, tracciabilità e accountability operativa.

MDR & xMDR

I servizi di Managed Detection and Response (MDR) unificano la visibilità su endpoint, reti, workload cloud e applicazioni. L'extended detection (xMDR) aggrega intelligence e telemetria su più livelli, consentendo una difesa proattiva contro minacce avanzate.

Anti-DDoS

I servizi di mitigazione Anti-DDoS proteggono l'infrastruttura da attacchi di denial-of-service sia volumetrici sia a livello applicativo, preservando disponibilità e continuità operativa.

Gestione dei Certificati SSL/TLS

La gestione automatizzata del ciclo di vita dei certificati SSL/TLS e di code-signing garantisce comunicazioni sicure e distribuzione software autenticata. In un contesto caratterizzato da machine identities e fiducia tra servizi, la governance dei certificati diventa un elemento fondante.

Compliance integrata, non inserita successivamente

Nei framework normativi europei, tra cui NIS2, GDPR, DORA e AI Act, i requisiti di cybersecurity vanno oltre la semplice risposta agli incidenti e comprendono:

- gestione del rischio;
- monitoraggio della supply chain;
- segnalazione degli incidenti;
- continuità operativa;
- tracciabilità e audit.

La telemetria e il logging di sicurezza non sono quindi meri strumenti difensivi, ma costituiscono prove di governance.

Integrando monitoraggio continuo, gestione strutturata delle vulnerabilità e procedure documentate di risposta nei modelli operativi, le organizzazioni riducendo friction audit. La compliance diventa una proprietà emergente dell'architettura, anziché un'attività reattiva.

La compliance by default rafforza la responsabilità esecutiva: i board necessitano di visibilità sul profilo di rischio, i soggetti regolatori richiedono controlli dimostrabili e gli assicuratori richiedono strategie di mitigazione misurabili.

La cybersecurity, se strutturata coerentemente, garantisce questa trasparenza.

Backup e Disaster Recovery come resilienza strutturale

La sorveglianza continua è incompleta senza la capacità di recupero.

I servizi di Backup e Disaster Recovery offrono la garanzia finale di integrità operativa quando i controlli preventivi non sono sufficienti. Replicazione strutturata dei dati, storage geo-ridondante, test automatizzati di recupero, failover orchestrati trasformano la resilienza da assicurazione teorica in continuità misurabile.

Nell'Integrity Economy, la disponibilità non è presunta: è progettata e ingegnerizzata.

Scarsità di talenti e resilienza gestita

I dati di mercato evidenziano costantemente una carenza strutturale di competenze in cybersecurity in tutta Europa. Per molte organizzazioni, sviluppare e mantenere capacità interne 24/7 risulta economicamente insostenibile.

I servizi di cybersecurity gestita rispondono a questo vincolo strutturale. Sfruttando scalabilità, automazione e procedure operative standardizzate in linea con framework internazionali, le organizzazioni ottengono protezione di livello enterprise senza frammentare la responsabilità di governance. La sicurezza diventa così una disciplina trasferibile, non vincolata ai cicli di staffing individuali.

SOC come sorveglianza continua

I servizi di Security Operations Center (SOC) rappresentano il nervo operativo della Digital Integrity.

Attraverso monitoraggio in tempo reale, correlazione di intelligence sulle minacce,

coordinamento della risposta agli incidenti e reportistica documentata, il SOC garantisce sorveglianza continua su infrastrutture cloud, on-premise e ibride.

In un contesto di minacce accelerate dall'IA, la resilienza deve essere dinamica: il SOC istituzionalizza questa dinamicità.

Integrazione Across the Stack

La cybersecurity è più efficace se integrata. All'interno dell'architettura Aruba, i servizi di sicurezza operano in sinergia con:

- ambienti cloud europei;
- infrastrutture data center Tier IV;
- Trust Services e framework di governance delle identità;
- monitoraggio Brand Protection;

Questa coerenza verticale riduce le lacune tra infrastruttura, identità e rilevamento.

La risposta agli incidenti si allinea alla chiarezza normativa, la governance dei certificati si collega ai Trust Services, e il monitoraggio dei domini alimenta l'intelligence del SOC. L'integrità end-to-end non è concettuale: è operativa.

Infrastruttura e cloud come architettura di sicurezza

Le soluzioni Private Cloud e Bare Metal di Aruba Enterprise forniscono il dominio di

esecuzione europeo necessario per workload ad alte prestazioni, ambienti Private AI e operazioni ad alta intensità di dati.

In architetture in cui i perimetri tradizionali si dissolvono, la sicurezza deve essere integrata nei sistemi di compute, storage e network.

L'infrastruttura europea garantisce chiarezza giurisdizionale, isolamento dei workload e controllo architetturale, consentendo una sicurezza senza perimetro senza sacrificare la governance.

Dalla mitigazione del rischio al vantaggio competitivo

Nei mercati digitali maturi, la resilienza influisce sulla valutazione aziendale.

Gli investitori valutano la postura di sicurezza. I clienti osservano l'impegno assunto verso la protezione dei dati. I soggetti regolatori controllano i piani di continuità.

Gli assicuratori adeguano i premi sulla base di controlli dimostrabili.

Quando la sicurezza è incorporata architetturealmente:

- l'innovazione accelera entro limiti di rischio definiti;
- i processi di audit si semplificano;
- i tempi di risposta agli incidenti si riducono;
- la fiducia degli stakeholder si rafforza.

La cybersecurity abilita l'evoluzione digitale.

La cybersecurity non limita la crescita: protegge la Digital Agency, ossia la capacità di scegliere, adottare e orchestrare tecnologie senza accumulare fragilità strutturale.

Integrità in movimento

La cybersecurity non è uno scudo statico: è un processo continuo.

Le minacce evolvono, le tecniche di attacco si adattano e l'automazione scala sia il rischio sia la difesa. In questo contesto, la resilienza deve essere dinamica.

Allineando i processi a framework internazionali, incorporando sorveglianza continua e integrando rilevamento, risposta e governance delle identità su ambienti ibridi, Aruba operazionalizza l'integrità su larga scala.

Dal data center ai certificati, dai workload cloud agli endpoint, la cybersecurity preserva la coerenza su tutto lo stack digitale.

Nell'Integrity Economy europea, la sicurezza non è un semplice strato difensivo.

È l'espressione operativa della fiducia.

**La fiducia, quando
progettata in maniera
sistemica, diventa la
base per una crescita
digitale sostenibile.**

About Aruba

Aruba, fondata nel 1994, è il Cloud Champion italiano e uno dei principali provider europei di infrastrutture e piattaforme digitali basate su asset proprietari. L'azienda progetta e gestisce l'intero stack tecnologico: dalla progettazione e costruzione di data center alle piattaforme cloud, dai servizi di trust e security alla connettività e alle soluzioni software che supportano strategie digitali e applicazioni basate su AI.

Con capitale interamente italiano, Aruba conta 16 milioni di utenti attivi sulle proprie piattaforme provenienti da oltre 100 nazioni e gestisce una infrastruttura distribuita su 8 data center in Europa, che ospita oltre 2,7 milioni di domini, 10 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti.



Copyright © Aruba. All rights reserved.

Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it