
Cybersecurity come controllo strutturale

Un approccio europeo alla resilienza, all'accountability e all'indipendenza operativa.

aruba.it

pruise

Sommario

01	La cybersecurity nell'era del controllo distribuito	3
02	La crisi di governance della sicurezza distribuita	6
03	Cybersecurity come controllo strutturale	7
04	Crescita sicura per grandi imprese e PMI	9
05	Dai principi alle capacità operative	11
06	Il futuro della cybersecurity	15
07	CONCLUSIONI	17

CAPITOLO 01

La cybersecurity nell'era del controllo distribuito

Dall'opportunità digitale all'esposizione digitale

Nelle prime fasi della Digital Transformation, le tecnologie digitali hanno moltiplicato le opportunità e aperto nuovi modi di vivere e lavorare. Allo stesso tempo, anche i rischi sono diventati digitali: la sicurezza si è spostata dal mondo fisico al dominio digitale, concentrandosi sulla protezione di perimetri ben definiti. La pandemia da COVID-19 e la crescita del lavoro da remoto hanno progressivamente reso quei perimetri più sfumati. Oggi la cybersecurity sta evolvendo per riflettere il modo in cui le organizzazioni stesse sono diventate organizzazioni digitali.

La cybersecurity è passata da ambito tecnico specialistico a una delle priorità di investimento della digital economy.

Questa crescita riflette un cambiamento manageriale più ampio: i budget cyber aumentano perché le organizzazioni non investono più soltanto in strumenti di difesa, ma anche in resilienza, capacità di risposta, protezione dei dati, governance del cloud e fiducia a livello di board. Le stesse tecnologie che guidano la trasformazione digitale stanno ridefinendo anche il panorama delle minacce.

Il perimetro si è dissolto

Per anni **la sicurezza è stata considerata una funzione specialistica**: importante, tecnica e spesso complessa, ma comunque separata dall'architettura centrale del business. Questa separazione non regge più. **Oggi l'infrastruttura è distribuita tra piattaforme cloud, ambienti SaaS, API, utenti remoti, sistemi operativi, provider terzi e processi sempre più automatizzati**. L'organizzazione non è più contenuta entro un perimetro chiaramente definito. Opera attraverso una rete di dipendenze in continuo movimento.

Il rischio si muove attraverso le dipendenze

Questa evoluzione ha creato enorme flessibilità. Ha però cambiato anche la natura del rischio. Una vulnerabilità non colpisce più soltanto un singolo sistema: può propagarsi tra identità, workload, fornitori, applicazioni e servizi rivolti ai clienti.

Un problema in un livello può trasformarsi rapidamente in una questione operativa, regolatoria e reputazionale. In questo contesto, la cybersecurity non riguarda solo la prevenzione degli attacchi o la capacità di recuperare rapidamente dopo un incidente. Riguarda la capacità di governare sistemi digitali sempre connessi, sempre esposti e sempre più interdipendenti.

La sicurezza deve essere progettata fin dall'inizio

La cybersecurity deve diventare parte integrante del modo in cui gli ambienti digitali vengono progettati, gestiti e governati fin dall'inizio. Con l'evoluzione delle minacce cyber e il cambiamento delle regole di accountability, la cybersecurity deve diventare strutturale lungo l'intero stack tecnologico, abilitando integrità digitale, residenza dei dati in UE, controllo operativo e indipendenza tecnologica.

La pressione europea verso un'accountability continua

Per le organizzazioni europee, un'ulteriore pressione arriva dalle istituzioni dell'Unione Europea, sempre più orientate a costruire un'Europa digitale resiliente e sicura.

Normative come NIS2, GDPR, DORA e AI Act stanno spostando la cybersecurity da una logica di compliance episodica a una logica di accountability continua.

I board sono chiamati a supervisionare il rischio cyber. Le supply chain devono essere governate. La resilienza operativa deve essere dimostrata. La compliance non è più un controllo finale: sta diventando un requisito architetturale.

Resilienza, residenza dei dati in UE e controllo strategico sono oggi priorità critiche e si collocano stabilmente al centro delle decisioni di cybersecurity.

Il controllo strategico è centrale

Mantenere il controllo strategico su infrastruttura, dati, giurisdizione e responsabilità operative è la nuova frontiera.

Dove vengono eseguiti i sistemi, chi li governa, come si muovono i dati e chi controlla in ultima istanza le dipendenze critiche sono ormai domande strategiche.

Non si tratta di rifiutare ecosistemi esterni o partnership globali, che restano forti e strutturali. Si tratta piuttosto di garantire che le organizzazioni mantengano visibilità, autorità e accountability significative sui sistemi da cui dipendono.

Il gap di controllo è anche un gap di competenze

La domanda di cybersecurity cresce più rapidamente della capacità di molte organizzazioni di dotarsi internamente delle competenze necessarie. La forza lavoro globale nel settore cyber continua ad aumentare, ma la carenza di professionisti qualificati resta significativa, soprattutto in Europa.

Questo rafforza il valore strategico di modelli operativi integrati, capacità di sicurezza gestita, automazione e governance chiara: le imprese hanno bisogno di resilienza anche quando le competenze specialistiche restano scarse.

Dalla crescita del mercato al controllo strutturale

Il mercato si espande perché il rischio si diffonde **attraverso piattaforme cloud, ambienti SaaS, identità, supply chain, workflow abilitati dall'AI e servizi business critical**. Maggiore spesa non significa automaticamente maggiore controllo.

Per le imprese, la vera sfida è **capire se gli investimenti in sicurezza possano essere tradotti in un modello operativo coerente: un modello che colleghi infrastruttura, dati, identità, compliance, detection, response e recovery**.

È in questo contesto che la cybersecurity diventa controllo strutturale.

CAPITOLO 02

La crisi di governance della sicurezza distribuita

La complessità cresce più rapidamente dell'accountability

Il controllo diventa più difficile quando ogni nuovo rischio genera un nuovo strumento, ogni nuova piattaforma introduce un nuovo provider e ogni nuovo requisito regolatorio aggiunge un ulteriore livello di governance.

Nel tempo, le organizzazioni possono accumulare tecnologie e perfino capacità, ma non necessariamente coerenza. Singolarmente, questi elementi possono funzionare bene. Nel loro insieme, però, possono creare un modello operativo frammentato, in cui infrastruttura, cloud, identità, compliance e security operations sono gestiti attraverso team, contratti e strutture di accountability differenti.

La visibilità può aumentare, ma la responsabilità diventa più difficile da tracciare.

CAPITOLO 03

Cybersecurity come controllo strutturale

Il controllo strutturale parte dall'architettura

È da qui che parte l'approccio di Aruba: la risposta non può essere semplicemente aggiungere altri livelli di sicurezza. Se il problema è la frammentazione, **la risposta deve essere architetturale. È questa la logica che eleva la cybersecurity a controllo strutturale.**

La sicurezza non viene trattata come un livello separato, posto sopra l'infrastruttura o le piattaforme cloud. È parte dell'architettura che permette alle organizzazioni di governare i propri ambienti digitali, preservando l'integrità digitale tra data center, piattaforme cloud, connettività, identità, compliance e servizi fiduciari.

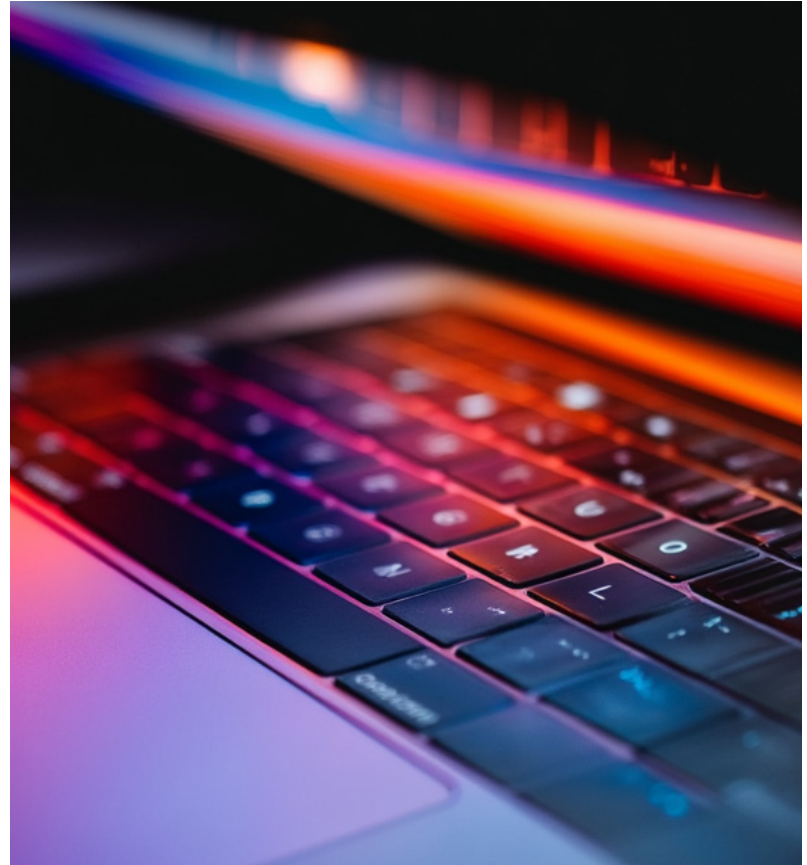
La resilienza dipende dal sapere chi controlla cosa, dove operano i sistemi, come sono distribuite le responsabilità e quanto rapidamente l'organizzazione può agire quando accade qualcosa.

L'approccio di Aruba ad ambienti digitali coerenti

Il posizionamento di Aruba riflette questa visione. **In qualità di provider europeo fondato su infrastruttura proprietaria, Aruba collega data center, cloud e servizi fiduciari all'interno di un modello più ampio di controllo.** L'obiettivo non è costruire ecosistemi chiusi. L'obiettivo è ridurre i rischi di dipendenza nascosta, preservando al tempo stesso la capacità di evolvere. Il valore non risiede soltanto nei singoli servizi, ma nella coerenza dell'ambiente che contribuiscono a costruire. Il nostro impegno verso standard aperti e architetture trasparenti garantisce che **il controllo resti nelle mani dell'organizzazione, evitando forme di lock-in proprietario.**

La compliance europea come disciplina operativa

Questo cambia anche il significato della compliance. La sicurezza non può essere solo uno stack di funzionalità e livelli tecnologici, e la compliance non può essere ridotta a una checklist o a un esercizio di reporting. **In un contesto regolatorio modellato da NIS2, GDPR, DORA, AI Act e Cyber Resilience Act,** soprattutto mentre prodotti connessi e componenti digitali diventano parte di ambienti business critical, le organizzazioni hanno bisogno di sistemi che rendano oversight, tracciabilità e resilienza parte integrante del modello operativo. L'obiettivo strategico non è quindi semplicemente una protezione più forte. È la creazione di ambienti digitali in cui sicurezza, resilienza e governance si rafforzano a vicenda. **Il controllo non nasce dall'aggiungere complessità. Nasce dal ridurre la frammentazione.**



CAPITOLO 04

Crescita sicura per grandi imprese e PMI

La cybersecurity si estende agli ecosistemi di business

Il suo perimetro include oggi piattaforme cliente, supply chain, ecosistemi di partner e transazioni digitali.

Per grandi imprese e PMI, la cybersecurity sta quindi diventando una decisione di business. Protegge l'integrità della trasformazione digitale aiutando le organizzazioni a tutelare persone, dati, servizi, clienti, reputazione del brand e continuità operativa. In questo senso, la cybersecurity non riguarda solo la riduzione dell'esposizione al rischio: riguarda la creazione della fiducia necessaria per crescere in modo sicuro e sostenibile.

La protezione end-to-end resta essenziale, ma i clienti hanno sempre più bisogno che la cybersecurity supporti fiducia nei fornitori, accountability contrattuale, auditabilità e fiducia dei clienti finali.

Un'infrastruttura sicura non è soltanto un asset tecnico: diventa una piattaforma di business attraverso cui le organizzazioni possono scambiare dati, erogare servizi, dimostrare compliance e preservare credibilità operativa.

Ogni stakeholder aziendale ha una diversa domanda di controllo

Questo cambia anche il modo in cui la cybersecurity viene valutata. I **CISO** devono ridurre il rischio e migliorare la risposta. **CIO** e **CTO** hanno bisogno di fondamenta sicure e interoperabili. I **responsabili risk e compliance** hanno bisogno di evidenze e tracciabilità. **Procurement e legal team** hanno bisogno di chiarezza su responsabilità dei vendor, residenza dei dati e dipendenze da terze parti. I **board** hanno bisogno di fiducia nel fatto che il rischio cyber sia gestito in modo da proteggere continuità, reputazione e crescita.

Un modello pensato per l'adozione

La sfida per molte organizzazioni non è soltanto scegliere tecnologie di sicurezza più robuste. **È adottare la cybersecurity in modo scalabile, ripetibile e allineato al proprio modello operativo.**

Le PMI hanno spesso bisogno di accedere a competenze affidabili senza complessità non necessaria. I clienti enterprise hanno bisogno di servizi che possano integrarsi in ambienti organizzativi, tecnici e di governance più ampi.

L'approccio di Aruba è pensato intorno a questa realtà. **I nostri servizi di cybersecurity sono modulari, ripetibili e accessibili a diversi livelli di maturità,** aiutando i clienti a integrare più facilmente la sicurezza nelle attività quotidiane e nella crescita di lungo periodo.

Esigenze diverse per clienti diversi

Il livello di autonomia operativa varia da cliente a cliente. Alcuni vogliono delegare le operazioni di cybersecurity a un provider affidabile. Altri vogliono mantenere un controllo diretto e integrare i servizi di sicurezza nei propri processi interni.

Per questo Aruba ha strutturato i propri servizi in due modelli complementari. Il modello **Managed/SaaS** è pensato per i clienti che vogliono che Aruba gestisca il servizio per loro conto. Il modello **Self-Managed/PaaS** è pensato per i clienti che vogliono maggiore autonomia all'interno di un ambiente ospitato da Aruba.

Questo approccio a doppio modello permette agli stessi principi strategici di servire profili di cliente diversi. **Le PMI possono accedere a servizi di cybersecurity affidabili in modo più semplice e sostenibile. Le imprese possono adottare servizi che supportano maggiore integrazione, scala e controllo.**

La fiducia come fondamento della crescita

Il controllo strutturale collega sicurezza enterprise e fiducia B2B. Aiuta le organizzazioni a proteggere il proprio business digitale, preservando la capacità di collaborare, integrarsi ed evolvere. Man mano che gli ecosistemi digitali diventano più automatizzati, questa fiducia dipende sempre più da identità verificate, certificati affidabili, contenuti autentici e interazioni tracciabili. Per Aruba, il valore non sta soltanto nella protezione dei singoli livelli dello stack. Sta nel **rendere la cybersecurity più facile da adottare, più semplice da governare e più direttamente collegata alla crescita del business.**

CAPITOLO 05

Dai principi alle capacità operative

Il controllo strutturale deve diventare operativo

Questo principio acquista valore solo quando si traduce in capacità operative concrete, misurabili e già validate sul campo.

In Aruba siamo noi stessi il primo e più esteso banco di prova delle nostre competenze cyber: proteggiamo ogni giorno infrastrutture, servizi e ambienti distribuiti con lo stesso modello che mettiamo a disposizione dei clienti.

Per questo sappiamo che la cybersecurity non può essere progettata in astratto, ma deve nascere dalle esigenze reali delle imprese: governare ecosistemi complessi, mantenere visibilità e continuità, reagire con rapidità quando qualcosa accade. Appliciamo questo approccio in tutti i nostri ambienti, testandolo nelle stesse condizioni operative che affrontano i nostri clienti.

Quali sono queste capacità operative? **Aruba offre soluzioni di cloud security europee, architetture aperte dove applicabile e capacità cyber end-to-end che rafforzano la propria offerta core.**

Resilienza operativa

Il rischio cyber moderno è continuo; per questo anche il monitoraggio e la risposta devono esserlo. **I servizi Managed SOC e MDR, integrati con capacità di security orchestration, supportano questa esigenza aiutando le organizzazioni a rilevare le minacce, coordinare la risposta e mantenere visibilità su ambienti complessi.** L'obiettivo non è solo una detection più rapida. È una continuità più solida.

Identità e fiducia digitale

Man mano che le organizzazioni diventano più automatizzate, l'identità non riguarda più soltanto le persone. **Include certificati, API, macchine, servizi e workflow automatizzati. Le machine identity stanno diventando critiche quanto le identità umane, perché determinano quali sistemi, servizi e processi automatizzati possono agire, scambiare dati e prendere decisioni.** Devono essere governate, rinnovate, autenticate e tracciate. La gestione del ciclo di vita dei certificati e i servizi fiduciari diventano elementi essenziali dell'architettura di sicurezza, perché proteggono l'affidabilità delle interazioni digitali.



Nell'era dell'AI, la fiducia si estende anche ai contenuti: le organizzazioni avranno sempre più bisogno di verificare non solo chi o che cosa ha agito, ma anche se contenuti digitali, dati e output generati dalle macchine possano essere considerati affidabili.

Sicurezza dell'infrastruttura e del cloud

Con lo spostamento dei workload su ambienti ibridi, l'infrastruttura diventa inseparabile dalla strategia di cybersecurity. Le organizzazioni hanno bisogno di fondamenta sicure, interoperabili, scalabili e allineate ai propri requisiti di governance.

È qui che l'ecosistema più ampio di Aruba diventa strategicamente rilevante: la sicurezza è connessa al livello infrastrutturale, non separata da esso.

Compliance e accountability

Le imprese devono dimostrare resilienza, tracciabilità e controllo in modo continuativo. Questo richiede che monitoraggio, identità, visibilità infrastrutturale e governance lavorino insieme. **La compliance by design è preziosa perché trasforma la pressione regolatoria in una disciplina architetturale.**

Sicurezza nell'era dell'AI

L'AI sta cambiando sia l'attacco sia la difesa. **Attacchi automatizzati, identità sintetiche, deception generata da macchine e operazioni guidate dall'AI aumentano la velocità e la complessità del rischio.** Creano anche una nuova sfida di fiducia: le organizzazioni avranno bisogno di verificare origine, integrità e affidabilità di contenuti, decisioni e interazioni generati da macchine. Allo stesso tempo, l'AI può rafforzare detection, analisi e risposta.

Da strumenti isolati a un modello operativo di sicurezza

Insieme, queste capacità supportano una proposta semplice. Le imprese non hanno bisogno di altri strumenti isolati. Hanno bisogno di integrità garantita attraverso infrastruttura, identità, resilienza, compliance e risposta, e di capacità connesse che trasformino la sicurezza in un modello operativo.

La cybersecurity diventa l'architettura che permette alla trasformazione digitale di restare governabile.

EVIDENZE DELLA CAPACITÀ OPERATIVA DI ARUBA IN AMBITO CYBERSECURITY

SOC e managed detection su larga scala

Aruba gestisce un Security Operations Centre attivo 24x7 con servizi di Managed Detection and Response (MDR) ed Extended Detection and Response (xMDR), proteggendo oltre 5,4 milioni di clienti in Europa.

Allineamento al NIST CSF e certificazioni

La postura di sicurezza di Aruba è allineata al NIST Cybersecurity Framework, con certificazione ISO 27001, qualifica ACN QC3 e capacità dedicate per vulnerability assessment, penetration testing (VAPT), protezione delle applicazioni web (WAP) e anti-DDoS.

La cybersecurity come primo prodotto interno di Aruba

Le stesse operazioni di sicurezza che proteggono i clienti enterprise di Aruba sono quelle che Aruba utilizza per proteggere se stessa: 1,6 miliardi di firme, 9 milioni di caselle PEC e l'infrastruttura nazionale italiana di trust dipendono ogni giorno da questa maturità operativa.

+5,4MLN

CLIENTI PROTETTI
IN EUROPA

1,6MLD

FIRME PROTETTE
PER CLIENTI ENTERPRISE

+16MLN

UTENTI

9MLN

CASELLE PEC ENTERPRISE
PROTETTE

evidence box

CAPITOLO 06

Il futuro della cybersecurity

Governance e indipendenza definiranno la prossima fase

Stiamo entrando in una nuova era della trasformazione digitale: governance e indipendenza tecnologica conterranno sempre di più.

Il futuro della cybersecurity non sarà definito soltanto da una difesa più forte. Sarà definito dalla capacità di preservare il controllo strategico mentre gli ambienti digitali diventano più automatizzati, distribuiti e interdipendenti.

Il nostro futuro digitale non riguarda solo la difesa, ma anche la capacità di recupero. Il modo in cui difendiamo, proteggiamo e recuperiamo sarà **centrale nella prossima fase della cybersecurity europea.**

L'AI ridefinirà sia l'attacco sia la difesa

Con l'AI, gli attacchi diventeranno più rapidi, più adattivi e più difficili da attribuire. **La difesa diventerà più predittiva, automatizzata e dipendente dall'analisi in tempo reale.** Allo stesso tempo, anche i sistemi di AI dovranno essere monitorati, autenticati e governati, con una chiara accountability sulle identità, sulle fonti dati e sulle decisioni automatizzate su cui si basano.

L'identità diventerà il piano di controllo

Con la moltiplicazione di machine identity, API, agenti delegati e workload autonomi, le organizzazioni avranno bisogno di modalità più solide per verificare l'autorità e attribuire le azioni.

La fiducia dipenderà dalla capacità di sapere non solo chi ha fatto qualcosa, ma quale sistema, servizio o processo automatizzato ha agito, con quale autorità e con quale accountability. Nel tempo, questo stesso livello di fiducia dovrà prepararsi anche alla **post-quantum cryptography**, mentre le imprese inizieranno a valutare come evolveranno la crittografia attuale, i certificati e le strategie di protezione dei dati di lungo periodo in un mondo quantum-ready.

La resilienza includerà giurisdizione e governance dell'infrastruttura

Le organizzazioni valuteranno **la propria postura di sicurezza non solo attraverso prodotti e strumenti, ma anche attraverso governance dell'infrastruttura, giurisdizione, controllo dei dati e indipendenza operativa.** Dove operano i sistemi e chi li governa influenzeranno sempre di più le decisioni di sicurezza.

La regolazione rafforzerà questo cambiamento. **Cybersecurity, compliance, strategia infrastrutturale e resilienza operativa continueranno a convergere.**

Le decisioni architetturali diventeranno decisioni di governance. Le scelte cloud diventeranno scelte di sicurezza. Le strategie legate all'AI diventeranno questioni di accountability.

Il posizionamento di Aruba per la prossima fase

È questo l'ambiente per cui Aruba si sta posizionando: **infrastruttura europea, interoperabilità, compliance by design, resilienza operativa e governance integrata.** Significa mettere a disposizione tecnologie avanzate e gestire uno stack digitale completo che lasci le organizzazioni saldamente al posto di guida.

La cybersecurity non è più soltanto la funzione che protegge la trasformazione digitale dalle interruzioni. **Sta diventando la disciplina che abilita la trasformazione, rafforza la resilienza e permette alle organizzazioni di evolvere attraverso il controllo strategico.** Il vantaggio futuro apparterrà a chi saprà evolvere senza perdere il controllo.

CAPITOLO 07

Conclusioni

La cybersecurity non è più soltanto una questione di esposizione al rischio. È una questione di interdipendenza, governance e controllo.

Man mano che gli ambienti digitali si distribuiscono tra piattaforme cloud, servizi SaaS, API, identità, fornitori e sistemi guidati dall'AI, un evento cyber può attraversare rapidamente l'ecosistema di business e impattare operatività, compliance, reputazione e crescita.

Molte organizzazioni hanno risposto a questa complessità aggiungendo strumenti, controlli e capacità specialistiche. Ma **più sicurezza non significa automaticamente più controllo.**

Quando tecnologie, provider, responsabilità e requisiti regolatori si accumulano senza un modello operativo coerente, la visibilità può aumentare mentre l'accountability diventa più difficile da tracciare.

La frammentazione diventa quindi una delle sfide cyber centrali della prossima fase enterprise.

Per questo la cybersecurity deve diventare strutturale. Deve essere parte del modo in cui gli ambienti digitali vengono progettati, ospitati, gestiti e governati. L'obiettivo non è più soltanto prevenire gli attacchi o rispondere agli incidenti. **È preservare l'integrità digitale: la capacità di proteggere persone, dati,**

servizi, clienti, reputazione del brand e continuità operativa, permettendo al tempo stesso alle organizzazioni di innovare, rispettare le regole e crescere con fiducia. Per grandi imprese europee e PMI, questo cambiamento è particolarmente rilevante.

Regolazione, sovranità, governance dell'infrastruttura e controllo della supply chain stanno diventando inseparabili dalle decisioni di cybersecurity.

Dove vengono eseguiti i servizi, chi li gestisce, come vengono governate le dipendenze e come viene dimostrata l'accountability sono ormai domande di business tanto quanto domande tecniche.

L'approccio di Aruba risponde a questa esigenza attraverso la cybersecurity come controllo strutturale. Combinando fondamenta basate in UE, servizi ospitati da Aruba, tecnologie aperte dove possibile e modelli di delivery flessibili Managed/SaaS o Self-Managed/PaaS, Aruba aiuta le organizzazioni a passare da una protezione frammentata ad ambienti digitali sicuri, governabili e scalabili.

La cybersecurity sta diventando il fondamento che consente alla trasformazione digitale di restare affidabile, compliant, resiliente e sostenibile, permettendo alle organizzazioni di continuare a crescere senza perdere il controllo.

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