Sessione

Dalla protezione alla prova della resilienza

Alessio Pennasilico | CS Clusit
Matteo Brusco | Distribution Sales Manager Italy Spain/PT | N-able

Alessio Pennasilico aka -=mayhem=-



Foto relatore

CISO

Member of the Board of Directors of the Association of IT Professionals

Member of the Scientific Committee

Senior Partner, Information & Cyber Security Advisor @Security Evangelist & Ethical Hacker

Vice President of the Committee for the Safeguarding of Impartiality

Member of the Scheme Committee

Scientific Director of the publication

Senior Advisor of the Cyber Security & Data Protection Observatory of the Politecnico di Milano

Core faculty

Matteo Brusco

Distribution Sales Manager Italy Spain/PT | N-able



Foto relatore

Dal 2017 faccio parte di N-able

Sono responsabile della gestione dei rapporti con i distributori, del sostegno alla crescita dei partner

e dell’attuazione delle strategie di canale nell’area dell’Europa meridionale.

Il mio obiettivo principale è instaurare collaborazioni continue basate sulla fiducia e sul valore.

Prima di entrare in N-able, ho maturato un'esperienza professionale a tutto tondo nel settore IT.

Ho iniziato la mia carriera come sistemista,

per poi lavorare direttamente come fornitore di servizi gestiti (MSP)

e infine passare alla distribuzione IT.

Sono appassionato di tecnologia, lavoro di squadra e di aiutare i partner ad avere successo

in un panorama in continua evoluzione.

PERCHÉ CAMBIA LA CONVERSAZIONE ?

Dalla protezione alla prova della resilienza

Non basta più dire “siamo protetti”. Dobbiamo dimostrare di essere preparati, di saper rispondere e di poter ripristinare.

PREVENIRE

Dimostrare che il rischio, le vulnerabilità e le identità sono sotto controllo.

RISPONDERE

Dimostrare che un incidente può essere rilevato e contenuto.

RIPRISTINARE

Dimostrare che dati e servizi critici possono tornare operativi.

LA BUSINESS RESILIENCE NON È UNA PROMESSA.

È qualcosa che dobbiamo poter dimostrare.

IL RISCHIO È CONNESSO

Un incidente non colpisce soltanto chi viene attaccato.

Clienti, fornitori, cloud e servizi digitali trasformano un problema tecnico in un rischio operativo condiviso.

ATTACCANTE → **MSP** → **CLIENTI** → **BUSINESS**

01

ACCESSO

Una compromissione può propagarsi attraverso ambienti e servizi connessi.

02

DIPENDENZE

La continuità del cliente dipende da fornitori, cloud e servizi digitali.

03

IMPATTO

Il problema tecnico diventa operativo: servizi indisponibili, dati inaccessibili, business fermo.

48%

delle violazioni è coinvolta una terza parte (in aumento dal 15% nel 2024 al 30% nel 2025)

78

aziende isolate a seguito dello sfruttamento di una vulnerabilità nello strumento di assistenza remota di un MSP

PROTEGGERE UN AMBIENTE NON BASTA.

Dobbiamo proteggerne la capacità di continuare a operare.

Sources: Verizon DBIR 2026; Huntress SOC via Dark Reading, Apr 2026; ENISA Threat Landscape 2026.

IL RISULTATO

La Business Resilience non è assenza di incidenti.

È la capacità di continuare ad operare quando gli incidenti si verificano.

01

MINORE ESPOSIZIONE

Ridurre le vulnerabilità sfruttabili prima che vengano individuate dagli attaccanti.

02

MINORE INTERRUZIONE

Rilevare e contenere l’attività prima che coinvolga l’intera azienda.

03

RECOVERY PIÙ RAPIDO E SICURO

Ripristinare con sicurezza dati integri e servizi prioritari.

La Business Resilience si misura nei risultati di business, non nel numero di tool implementati.

IL MODELLO OPERATIVO

Una strategia. Tre capacità operative connesse.

Nessuna singola competenza o prodotto garantisce la Business Resilience. Il risultato dipende da come i controlli lavorano insieme.



PRIMA DI UN ATTACCO

Endpoint Resilience

Conoscere l’ambiente su cui si opera. Rafforzarlo continuamente.
Intervenire prima che l’esposizione diventi interruzione.

RISCHIO

Asset sconosciuti • Vulnerabilità • Deviazioni di configurazione • Remediation manuale

RISPOSTA

N-central / N-sight

Unified visibility

Endpoint hardening

Patch and vulnerability management

Policy-driven automation

RISULTATO : Ridurre le opportunità disponibili per un attaccante.

DURANTE UN ATTACCO

Security Resilience

Rilevare rapidamente i comportamenti anomali. Contenere con precisione. Impedire che una compromissione diventi un’interruzione estesa.

RISCHIO

Segnali frammentati • Compromissione delle credenziali • Indagini tardive • Risposta lenta

RISPOSTA

Adlumin

Visibilità unificata sull’intera superficie di attacco

Monitoraggio continuo dello stato di rischio

Rilevamento e analisi a più livelli

Risposta automatizzata, contenimento e remediation, competenza SOC

RISULTATO : Contenere l’incidente prima che interrompa il business.

DOPO UN ATTACCO

Data Resilience

Proteggere punti di ripristino sicuri. Verificare che siano realmente utilizzabili. Ripristinare i servizi essenziali per il business.

RISCHIO

Backup compromessi • Recovery incerto • Downtime eccessivo • Servizi prioritari indisponibili

RISPOSTA

Cove Data Protection

Protezione dei dati cloud-native

Copie immutabili sempre attive

Monitoraggio delle anomalie

Test di ripristino automatizzati e ripristino flessibile

RISULTATO : Ripristinare con sicurezza i dati integri e i servizi critici.

LA RISPOSTA CONNESSA

La Business Resilience nasce dalla connessione tra i prodotti.

La Business Resilience è un ciclo chiuso, non una collezione di dashboard.

1	**HARDEN**	Ridurre esposizione e configuration drift
2	**DETECT**	Correlare le attività anomale nell’intero ambiente
3	**CONTAIN**	Isolare con precisione e limitare la propagazione
4	**RECOVER**	Ripristinare dati integri e servizi prioritari
5	**IMPROVE**	Integrare quanto appreso in policy e automation

Il ciclo non si ferma mai. Ogni incidente migliora la baseline successiva.

L’OPPORTUNITÀ PER GLI MSP

Dai tool a un servizio di Business Resilience.

I clienti hanno bisogno di un risultato che possano comprendere, misurare e dimostrare.

CONOSCERE e PROTEGGERE

Visibilità sugli asset, policy, patching e remediation delle vulnerabilità

MONITORARE e RISPONDERE

Visibilità 24×7, rilevamento, investigazione e contenimento delle minacce

PREPARARSI al RIPRISTINO

Copie protette, test di ripristino e priorità dei servizi critici

DIMOSTRARE e MIGLIORARE

Reportistica, lezioni apprese e miglioramento continuo della postura

NON VENDETE TRE PRODOTTI. OFFRITE UN UNICO RISULTATO.

Un servizio gestito ripetibile rende la Business Resilience visibile, operativa e dimostrabile.

TRE DOMANDE

Quanto è resiliente il business dietro la tecnologia?

01 Cosa deve continuare a funzionare per il cliente?

02 Cosa accade negli “spazi” tra prevenzione, risposta e ripristino?

03 Potete dimostrare che il recovery funzionerà?

MINIMIZZARE IL RISCHIO. RIDURRE L’IMPATTO. MANTENERE LA CONTINUITÀ.

OFFRITE BUSINESS RESILIENCE.

Q&A

Contatti:

Venite a trovarci al nostro Stand!