TD SYNNEX

Acronis | AUTHORIZED CLOUD DISTRIBUTOR

Acronis e NIS2

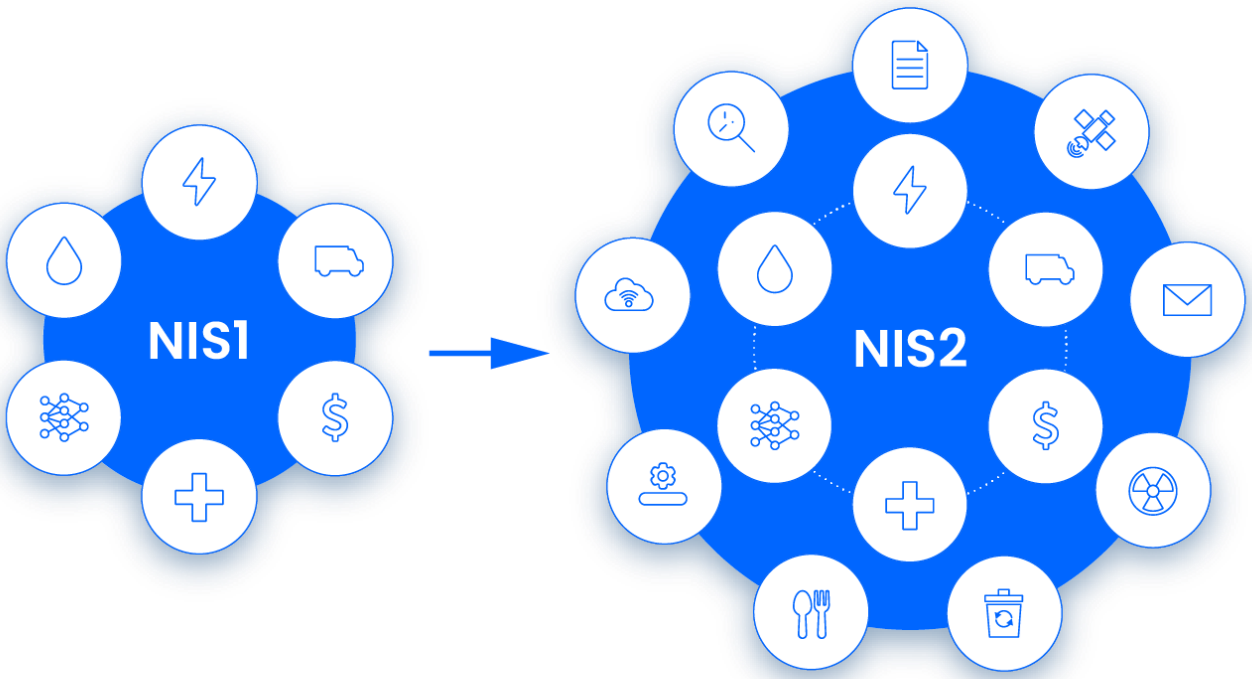
L’unica soluzione pensata per MSSP e NIS2 ready

30 Maggio 2025

Webinar

Andrea Catapano – Business Development Manager – TD SYNNEX
Andrea Pezzoni – Security Presales Specialist – TD SYNNEX

A chi si rivolge



Energy Essential Entity	**Health** Essential Entity	**Transport** Essential Entity	**Finance** Essential Entity	**Water Supply** Essential Entity
Digital Infrastructure Essential Entity	**Public Administration** Essential Entity	**Digital Providers** Important Entity	**Postal Services** Important Entity	**Waste Management** Important Entity
Space Essential Entity	**Foods** Important Entity	**Manufacturing** Important Entity	**Chemicals** Important Entity	**Research** Important Entity

Obblighi NIS2

1. **Gestione del Rischio di Sicurezza Informatica (Gestione e Valutazione rischio e incidenti)**
2. **Protezione dei Dati (Gestione Vulnerabilità)**
3. **Continuità Operativa e Ripristino di Emergenza**
4. **Monitoraggio e Notifica degli Incidenti**
5. **Formazione Continua**

Identificazione dei soggetti interessati

Entità Essenziali	Entità Importanti
Energia	Poste
Trasporti	Gestione dei rifiuti
Finanza (DORA)	Industria chimica
Pubblica Amministrazione	Ricerca
Salute	Alimentare
Aerospaziale	Manifattura per entità Essenziali
Distribuzione e gestione acque	Provider digitali
Infrastrutture digitali	
Fatturato >50M €	Fatturato >10M €
Dipendenti >250	Dipendenti >50

Un'entità può comunque essere considerata "essenziale" o "importante" anche se non soddisfa i criteri di fatturato e numero dipendenti

Sanzioni

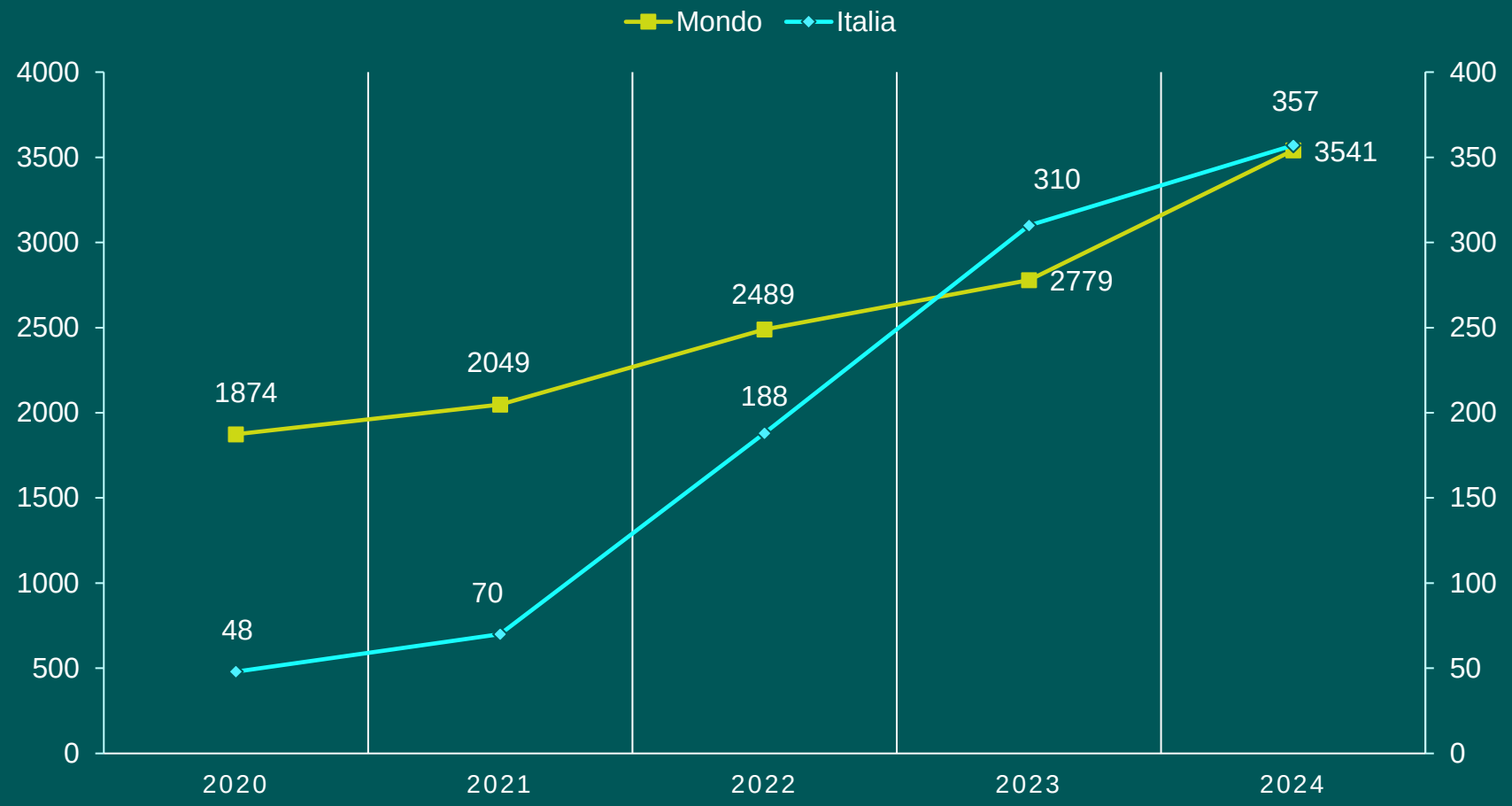
Entità Essenziali	Entità Importanti
Sanzioni amministrative Soggetti coinvolti: - CISO - CEO - Consiglio di amministrazione Multe fino a 10M € o 2% del fatturato annuale	Sanzioni amministrative Soggetti coinvolti: - CISO - CEO - Consiglio di amministrazione Multe fino a 7M € o 1,4% del fatturato annuale

Responsabilità

- **Sospensione Temporanea** (l'Autorità può richiedere la sospensione temporanea di certificazioni o autorizzazioni, limitando l'operatività dei servizi)

- **Responsabilità Personale** (le persone fisiche responsabili della gestione delle aziende o delle PA possono essere oggetto di misure disciplinari, come la sospensione temporanea delle funzioni dirigenziali o un cambio del board)

Confronto crescita Italia vs Mondo



Mondo +27%

Italia +15%

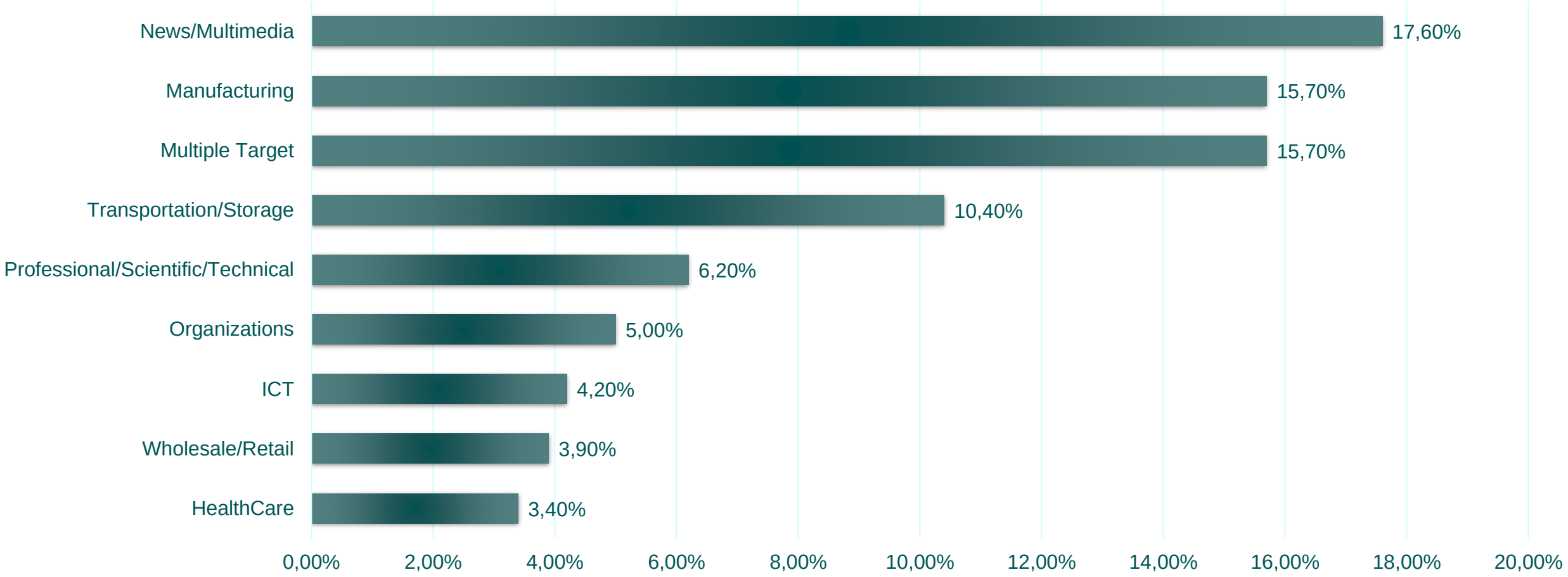
2024 vs 2023

Italia

PIL 1,8%
Popolazione 0,7%
Attacchi 10%

Francia 4%
Germania 3%
UK 3%

Vittime (Italia)



Danni per le aziende colpite

Economici

Danni derivanti da:

- Fermo Produzione
- Tempi di ripristino
- Riscatti
- Perdita di commesse

Reputazionali

Danni di immagine derivanti dall'attacco e dalle sue conseguenze sull'azienda colpita, senza trascurare il problema legato alla perdita di dati sensibili personali.

Sanzioni

Il costo previsto dal Regolamento Europeo 2016/679, GDPR, può arrivare, per le aziende private, fino a € 20M o il 4% del fatturato globale.

Competitivi

Furto di progetti, brevetti e possibile rivendita a competitor o attraverso aste nel dark web.

Comprehensive built-in features

A NIS2

Business Mgmt.		Backup and Disaster Recovery					Cybersecurity							
														
Remote Monitoring Access (RMM)	Patch Management	Trad. Backup	Backup as a service	Archive as a service	Disaster Recovery as a service	Data visibility	Data Loss Prevention	Incident investigation	Ransomware protection	Vulnerability assessment	Detection & response	Endpoint protection	Malware Resistance	Messaging Security

Acronis Cyber Protect Cloud

One Platform, One Agent, All within One Protection Plan

Complete coverage of NIST framework: Govern, Identify, Protect, Detect, Respond and Recover

DATA PROTECTION

Backup

Standard Backup

- Backup of 25+ workload types
- Local and cloud storage
- Encryption and deduplication
- Ransomware-proof backup
- **Microsoft 365**
  - Exchange Online, SharePoint Online, OneDrive, Teams, OneNote
  - Email Archiving EAP
  - Group management

Advanced Backup

- One-click mass recovery
- Continuous data protection
- Backup frequency for Microsoft 365 and Google Workspace
- Off-host validation, replication, and conversion to VMs
- Support for additional workload types
- Backup notarization

Disaster Recovery

FREE

- Test failover
- Cloud-only VPN connection

Advanced DR

- Production and test failover to Acronis Cloud
- Orchestration with runbooks
- AI-assisted Automated test failover
- Fast Automated Failback with near-zero downtime
- Multiple connectivity options:
  - IPsec Multisite VPN, L2 site-to-site open VPN, Cloud-only VPN

CYBERSECURITY

Detection and Response

FREE

- AI-based anti-malware protection
- #CyberFit score (Security posture assessment)
- Device control

Advanced Security + EDR

- Gen AI-guided incident investigation, analysis, automated response
- Single-click response, including attack-specific rollback and recovery
- Next Generation Antivirus (NGAV)
- Anti-ransomware protection
- 0-day and exploit protection
- URL filtering
- Anti-malware scans of backups

Advanced Security + XDR

- Extended endpoint protection with visibility and response across most vulnerable attack surfaces - email, identity, Microsoft 365 apps
- Gen AI-guided incident investigation, analysis, response and recovery

Advanced Security + MDR

- 24/7/365, Continuous monitoring with expedited investigation from security analysts
- Event triage, prioritization, and rapid response including recovery

Security Awareness Training

- Rich and engaging library of training courses
- Phishing simulation and exercises
- Mobile-friendly learning experience
- Available in multiple major languages

SaaS Security

Advanced Email Security

- Phishing and Quishing prevention
- Business Email Compromise prevention
- Malware protection
- APT and zero-day protection
- Account takeover detection
- Incident response service
- Microsoft 365, Google Workspace, Exchange and any SMTP supporting email service

Advanced Collaboration Apps Security

- Microsoft 365 SharePoint, OneDrive and Teams security protection
- Malware protection
- APT and zero-day protection
- Incident response service

OPERATIONS

Management

FREE

- **Endpoint**
  - Device Sense™ device discovery
  - Hardware inventory
  - Vulnerability assessment (Windows/Mac/Linux)
  - Remote desktop (RDP)
- **Microsoft 365**
  - Security posture risks dashboard
  - User management (onboard, offboard)

Advanced Management - Endpoint

- Software inventory
- Vulnerability assessment (third-party apps)
- Automated patch management
- ML-based monitoring
- Software deployment
- AI-enabled remote scripting
- Automated pre-patch backup
- HDD health monitoring
- Next-gen remote desktop and assistance

Advanced Management - Microsoft 365

- Remediation of tenant security posture risks
- Remediation of user security posture risks

Automation

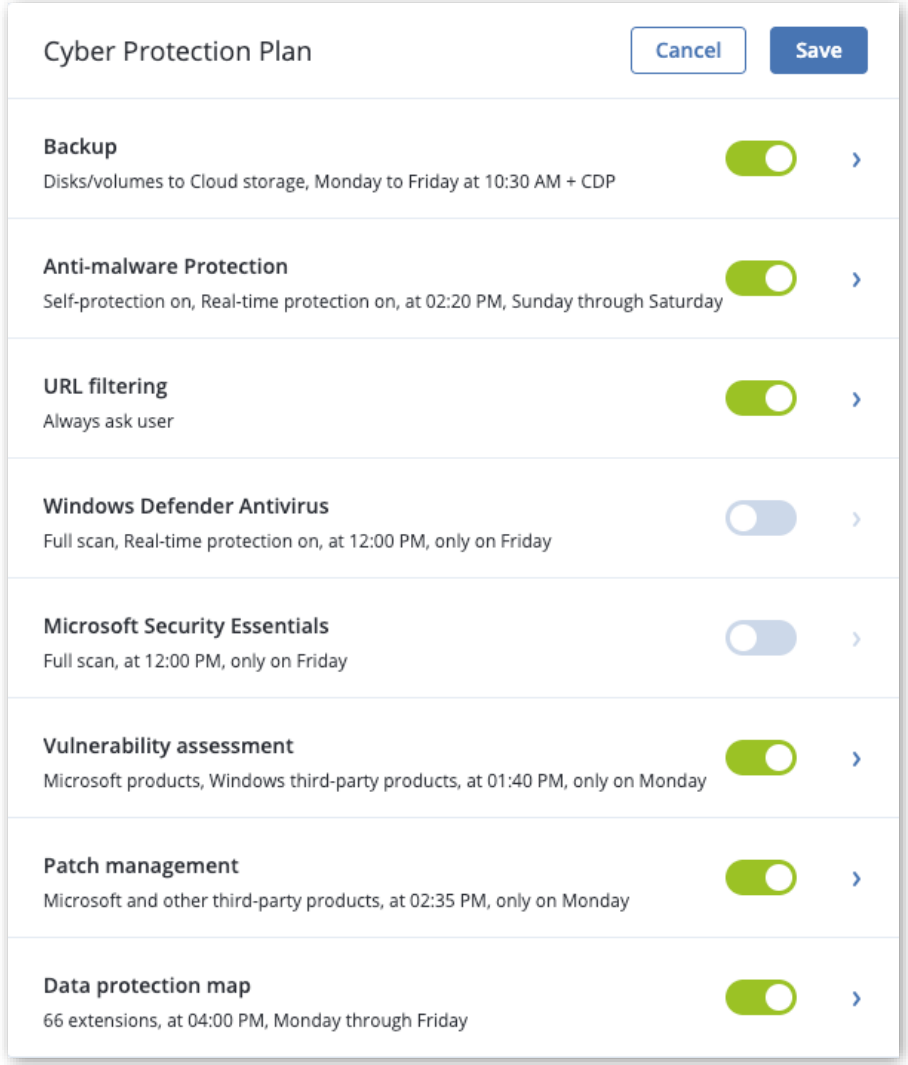
Advanced Automation

- Integrated ticketing
- Automatic time tracking
- Billing and invoicing
- Contract and SLA management
- Stock inventory management
- KPI reporting
- Integrated quoting

Un piano di protezione

Copre tutti gli aspetti di protezione informatica:

- Backup
- Protezione antimalware
- Ripristino di emergenza
- Filtro URL
- Valutazioni delle vulnerabilità
- Gestione delle patch
- Individuazione dei dati (tramite mappa della protezione dei dati)
- Gestione di Microsoft Defender Antivirus e Microsoft Security Essentials



Perché? Migliore protezione con meno sforzo, automatizzato

Requisiti NIS2 (art. 21) e come Acronis può aiutare [1/3]

GESTIONE E VALUTAZIONE DEL RISCHIO

- Il fornitore di servizi utilizza #**CyberFit Score per eseguire un report sullo stato di sicurezza di tutti i dispositivi** per un cliente e scopre che molti di essi non hanno impostato la crittografia del disco e corregge il problema per il cliente.
- Con la **rilevazione automatica**, il partner trova i dispositivi non autorizzati e li rimuove dall'ambiente del cliente.

Caratteristiche:

- Monitoraggio e avvisi delle minacce globali
- Inventario software e hardware
- Rilevamento automatico di nuovi carichi di lavoro
- #CyberFit Score

GESTIONE DEGLI INCIDENTI

- Il motore XDR funziona per i dispositivi del client e scopre **che un utente esegue uno script sospetto da una posizione geografica insolita**, suggerendo un account compromesso. Il partner sospende l'account di dominio dell'utente come passaggio di ripristino. Lo script è stato ricevuto tramite e-mail e i partner aggiungono l'indirizzo alla blacklist.

Caratteristiche:

- Sicurezza informatica + EDR/XDR
- Sicurezza e-mail
- Backup forense

RECUPERO DI EMERGENZA

- Il cliente è un'azienda di logistica, con ogni ora di inattività che costa 10.000 EUR. I **loro locali sono rimasti senza elettricità e connessione Internet**. L'MSP avvia tutti i suoi server di produzione dai backup in un cloud Acronis a Roma e gli utenti si collegano a quei server tramite VPN e continuano a lavorare.

Caratteristiche:

- Disaster Recovery
- Safe Recovery
- Bare Metal Recovery

Requisiti NIS2 (art. 21) e come Acronis può aiutare [2/3]

SICUREZZA DELLA CATENA DI FORNITURA

- **Il partner è considerato parte della supply chain del cliente e deve essere conforme a NIS2**. Acronis obbliga l'MSP a utilizzare MFA e garantisce che i dati archiviati siano immutabili, quindi anche se qualcuno dirotta i sistemi informativi del partner, non sarà in grado di fare nulla con i dati del cliente.

Caratteristiche:

- Sicurezza informatica + EDR/XDR
- Sicurezza e-mail
- MFA
- Backup immutabili

MANUTENZIONE SISTEMI INFORMATICI

- Uno dei server utilizzati nel processo di produzione del cliente si guasta e, poiché la sede è lontana, ci vorrebbe molto tempo prima che l'MSP arrivi. L'MSP **ordina a qualcuno in loco di riavviare il server e premere un tasto**, dopodiché il sistema viene automaticamente ripristinato dal backup del giorno prima.

Caratteristiche:

- Ripristino con un clic
- Backup continuo (CDP)
- Scripting informatico
- Scansione di backup

GESTIONE DELLE VULNERABILITA‘

- **Gli aggressori iniziano a sfruttare una vulnerabilità nota durante una campagna di attacco**. La gestione automatizzata delle patch garantisce che tutti i carichi di lavoro del cliente vengano patchati entro pochi giorni dal rilascio della patch da parte del fornitore del software.

Caratteristiche:

- Scansione delle vulnerabilità
- Gestione automatizzata delle patch

Requisiti NIS2 (art. 21) e come Acronis può aiutare [3/3]

CIFRATURA

FORMAZIONE

- **Acronis Security Awareness Training** fornisce concetti essenziali di sicurezza informatica agli utenti finali non tecnici, che spesso rappresentano il "punto debole" nelle difese di sicurezza informatica. Il programma include campagne di phishing simulate per rafforzare la consapevolezza e supporta la conformità ai requisiti **NIS2**.

Caratteristiche:

- Security Awareness Trainings (SAT)

ASSET MANAGEMENT

- **SW & HW Inventory**
- **Device Sense**

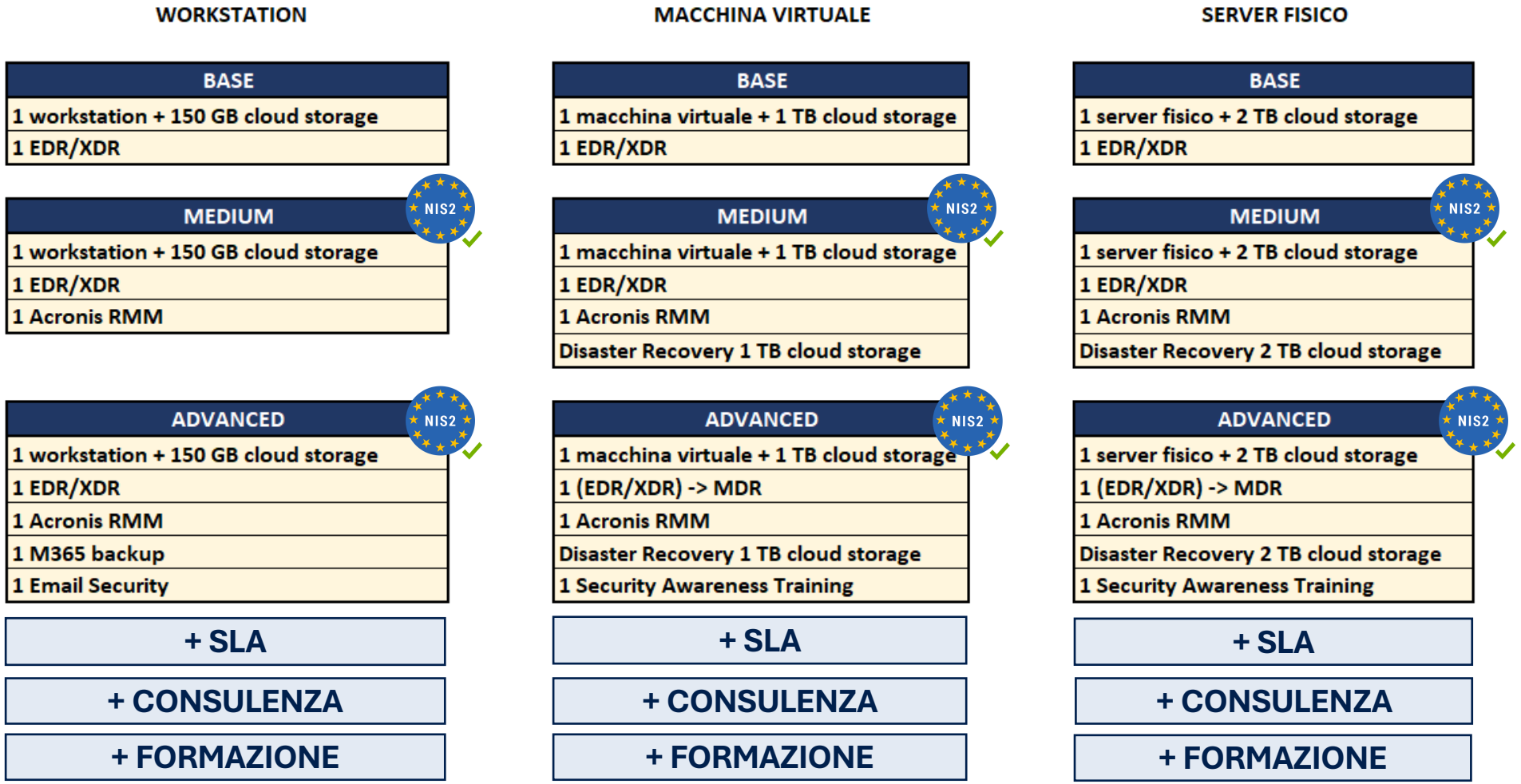
MFA E COMUNICAZONE DI EMERGENZA

- **Tramite Managed Detection and Response (MDR), Acronis fornisce monitoraggio, reporting e integrazione in tempo reale con i sistemi client**, facilitando una comunicazione di emergenza efficace come previsto da **NIS2**. Gli incidenti vengono immediatamente risolti, incluso l'uso del Disaster Recovery per la continuità aziendale. Utilizzando la console Acronis, i partner hanno tutti i dettagli necessari per conformarsi ai requisiti di comunicazione.

Caratteristiche:

- MDR (Managed Detection and Response)
- Monitoraggio e reporting
- Integrazione in sistemi specifici del cliente

CICLO DI VENDITA: modello di INTEGRAZIONE SERVIZI: durata media: 45-70gg



Garantire compliance e presenza locale

Scegli tra oltre 50 data center nel mondo per archiviare i dati – Acronis Hosted, Google Cloud and Microsoft Azure

THE CHANNEL CO. CRN DATA CENTER 50 2024

45+7

DATA CENTERS

Anche in Italia

Acronis Data Center

Google Data Center

Azure Data Center

Acronis Cyber Protect Cloud è in hosting su data center certificati

ROMA

AGID

Certificazioni di sicurezza dei prodotti Acronis

Riconoscimenti del settore della sicurezza

MVI member

VIRUSTOTAL member

Cloud Security Alliance member

Anti-Malware Testing Standard Organization member

Anti-Phishing Working Group member

MRG-Effitas participant and test winner

Anti-Malware Test Lab participant and test winner

ICSA Labs certified

NioGuard Security Lab participant and test winner

AV-Comparatives approved business security product

VB100 certified

AV-Test participant and test winner

Data center Acronis Cloud: sicurezza e riservatezza

Rispetto di standard di sicurezza internazionali come ISO 27001 e NIST

Controllo degli accessi

Criteri di controllo degli accessi in tutta l'azienda

- Controllo degli accessi centralizzato
- ID utente univoci e password complesse
- Protocolli di autenticazione sicuri (certificati LDAP, Kerberos, SSH)
- Autenticazione a due fattori
- Web Application Firewall (WAF)

Sicurezza dei dati

Rete multilivello e basata su zone

- Crittografia dei dati in transito e a riposo in tempo reale
- Trasferimento protetto dei dati su HTTPS (TLS)
- Crittografia AES-256 di livello aziendale per i dati dei clienti
- Disponibilità dei dati con tecnologia Acronis CloudRAID

Sicurezza fisica

Alte grate e controllo della sicurezza 24 ore su 24, 7 giorni su 7

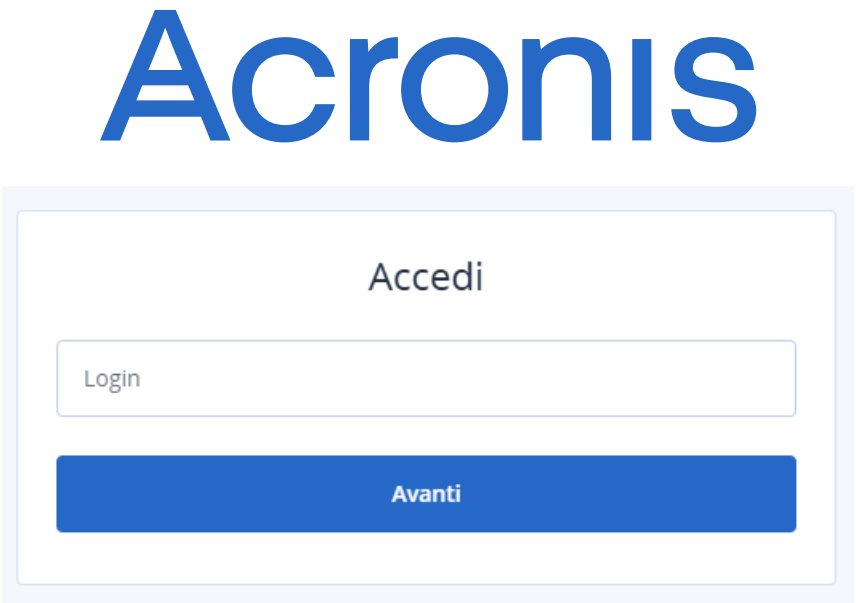
- Per l'accesso sono necessarie la scansione biometrica della geometria della mano e una scheda di prossimità
- Videosorveglianza con 90 giorni di archiviazione delle riprese
- Personale di sicurezza presente ininterrottamente

Sicurezza dell'infrastruttura

Infrastruttura ridondante ad alta disponibilità

- Gruppi di continuità e generatori diesel di emergenza
- Sistemi HVAC, reti e gruppi di continuità ridondanti
- Sistemi VESDA, di campionamento dell'aria e Dual Zone Pre-Action (con tubazioni a secco)
- Monitoraggio di temperatura e umidità

Hands-on



TD SYNNEX

“Cyber Security is a journey that evolves with the threats.”

Johannes Drooghaag

Q&A

06 GIUGNO: I servizi di TD SYNNEX per la compliance

13 GIUGNO: Affidare le chiavi della sicurezza ad un partner fidato

20 GIUGNO: Sonicwall CSE – ZTNA fatto semplice

https://events.tdsynnex.it/cyber-unit-missione-protezione/

TEAM SECURITY: security.it@tdsynnex.com
SPEAKER: andrea.pezzoni@tdsynnex.com andrea.Catapano@tdsynnex.com