

# DATA PROTECT

Il servizio riunisce le principali funzionalità per la protezione informatica, quali: backup, antiransomware e antimalware, protezione degli endpoint, disaster recovery e molto altro.

## CYBERSECURITY, MANAGEMENT, BACKUP & DISASTER RECOVERY

Data Protect di TWT è la soluzione in cloud che **integra sicurezza informatica, protezione dei dati e gestione degli endpoint** per proteggere in modo completo dispositivi, sistemi e dati, eliminando le complessità.

### Vantaggi

- Dati conservati e gestiti in Italia (conformemente alle normative vigenti, come GDPR)
- Dati protetti in modalità criptata
- Assistenza di tecnici esperti di 1° e 2° livello
- Ridondanza dei sistemi e delle infrastrutture
- Un'unica e intuitiva console protetta da Autenticazione a 2 fattori (2FA)
- Un'unica soluzione per tutte le funzionalità indispensabili
- Massima integrazione fra servizi e diverse funzionalità
- Scalabilità illimitata in cloud per adattarsi ad ogni esigenza



Funzionalità essenziali per la sicurezza e la protezione completa dei dati e dei sistemi dalle minacce informatiche.

**Protezione attiva**

Grazie alle tecnologie basate su Intelligenza Artificiale, il servizio è in grado di proteggere attivamente i sistemi dalle minacce informatiche. L'analisi statica e comportamentale permette infatti di prevenire eventuali criticità.

**Antimalware e antivirus basati su AI**

L'antivirus è basato su intelligenza artificiale per proteggere da malware, ransomware, cryptojacking e altre minacce informatiche.

**Controllo del dispositivo**

Analizza rapidamente i dispositivi per rilevare e prevenire l'accesso non autorizzato ai dati e la loro trasmissione tramite i canali dei computer locali.

**Vulnerability Assessment**

Identifica e colma le vulnerabilità nella sicurezza, grazie alla scansione costante dei sistemi.



Il backup è disponibile sia in cloud che in locale ed è pianificabile secondo le proprie necessità di orario e di contenuto, il tutto senza interferire nelle attività quotidiane.

**Backup dei file e delle applicazioni**

Soluzione ideale per la gestione ed il mantenimento in piena sicurezza dei dati, in quanto permette al Cliente di impostare il salvataggio automatico della sua infrastruttura virtuale o fisica.

I dati vengono custoditi in Italia nei Data Center di TWT e salvati su storage di classe enterprise.

**Backup incrementali e differenziali**

Si tratta di due tipi di salvataggio che consentono di ottimizzare lo spazio e le tempistiche del backup, andando ad analizzare i file modificati rispetto ad un primo backup completo, piuttosto che a creare nuovi backup completi ad ogni salvataggio.

**Protezione dei dati di Google Workspace e di Microsoft Office 365**

È possibile proteggere i dati contenuti e creati in Microsoft Exchange Online, OneDrive for Business, Microsoft Teams, SharePoint Online, Gmail, Drive, Contatti e Calendario grazie al backup cloud-to-cloud.

**Backup e archivio criptati**

La criptazione dei backup AES-256 consente la conformità normativa e migliora la sicurezza dei dati in transito e archiviati.

**Deduplicazione**

Il sistema rileva i dati ripetuti nei backup, in modo da risparmiare spazio di storage non archiviando gli stessi dati più volte.

**Monitoraggio e reportistica**

Una dashboard con informazioni dettagliate e con un'ampia gamma di report, ideale per identificare e risolvere rapidamente le criticità, monitorare i sistemi e pianificare le attività.



Funzionalità indispensabili per la gestione centralizzata dei sistemi di protezione, per la configurazione rapida degli endpoint, per l'assistenza degli utenti da remoto ed il monitoraggio della sicurezza.

**Gestione centralizzata della sicurezza**

È possibile ottimizzare l'effort del reparto IT grazie a una gestione centralizzata dei piani di protezione che includono tutte le configurazioni di sicurezza necessarie.

**Assistenza remota**

La funzionalità consente di prestare assistenza, intervenendo da remoto, sull'endpoint dell'utente. Prima della sessione l'utente visualizzerà in modo evidente un messaggio di avviso per concedere il consenso all'assistenza da remoto sul proprio dispositivo.

**Raccolta di inventari hardware**

Permette di avere sempre un inventario aggiornato di tutte le risorse hardware eseguendo scansioni automatiche e manuali.



La soluzione di **Disaster Recovery** consente di avere sempre disponibili tutte le risorse aziendali anche in caso di eventi catastrofici o inaspettati, salvaguardando la business continuity.

**VANTAGGI**

Il meccanismo di replica può coprire qualsiasi carico di lavoro, sia esso proveniente da Windows o Linux.

Bastano pochi minuti per trasferire i carichi di lavoro di produzione nel Data Center in Cloud, anche in caso di un problema sull'intero sito, per tornare rapidamente operativi.

Il Cliente ha la possibilità di lanciare test in qualsiasi momento ed in autonomia. Il test effettua un tentativo di recupero da disastro, simulando l'attivazione delle macchine nel Sito secondario, senza interferire con le macchine di produzione (Sito primario). L'operazione permette di verificare se le repliche e le procedure di Disaster Recovery funzionino correttamente.

Il servizio consente di incrementare ulteriormente i livelli di protezione con le **opzioni advanced**, in aggiunta alle funzionalità di base e secondo le necessità specifiche del Cliente.



## ADVANCED SECURITY

L'opzione Advanced Security aumenta la protezione informatica integrata e la reattività nel contrastare le nuove minacce informatiche. Estende la protezione alla navigazione su Internet, ai dati di backup, al processo di ripristino dei dati e previene gli exploit. Inoltre, permette l'acquisizione di dati forensi per eventuali indagini.

### Filtro URL

La funzionalità consente di proteggere i sistemi dalle minacce informatiche come malware e phishing provenienti dagli URL. Grazie a questo sistema è possibile bloccare l'accesso degli utenti ai siti Internet potenzialmente pericolosi.

### Prevenzione exploit

Ideale per prevenire gli attacchi avanzati, come quelli zero-day e fileless, sfruttando l'analisi comportamentale.

### Analisi forensi

Raccolta e salvataggio di prove digitali in archivio per eventuali indagini forensi e risoluzione rapida in caso di incidenti.

Ripristino del backup con verifica antimalware e antivirus

Grazie alla scansione antimalware integrata, il sistema impedisce il ripristino dai backup dei file infetti. Il servizio, infatti, consente di individuare gli eventuali virus e garantisce che i dati del backup siano completamente sicuri.



## ADVANCED MANAGEMENT

L'opzione Advanced Management semplifica la gestione delle vulnerabilità e permette di migliorare l'infrastruttura IT attraverso una gestione delle patch ancora più avanzata.

### Patch management

Per garantire la protezione degli ambienti aziendali sono fondamentali le patch e gli aggiornamenti software che correggono preventivamente le vulnerabilità. La funzionalità consente di pianificare o eseguire manualmente la distribuzione delle patch, assicurando ai dati una protezione continua.

### Fail-safe patching

Una patch contenente errori può rendere inutilizzabile un sistema. Per questo motivo, prima di implementare le ultime patch, il servizio crea un backup automatico che consente di ripristinare facilmente uno stato precedente in caso di necessità.

### Monitoraggio dello stato dell'hard disk

Monitora l'integrità dell'hard disk, sfruttando il machine learning per prevedere le criticità e indicare le misure necessarie per correggerle precocemente.

### Raccolta di inventari software

Permette di avere sempre a disposizione l'inventario software e risparmiare tempo. Esegue automaticamente oppure manualmente la scansione dei sistemi per una panoramica completa di tutti i software installati.



## ADVANCED EMAIL SECURITY

L'opzione aumenta i livelli di protezione delle caselle di posta elettronica rilevando qualsiasi minaccia via email prima che raggiunga gli utenti finali.

Blocca le minacce quali spam, phishing, compromissione dell'e-mail aziendale (BEC), ransomware e malware, minacce persistenti avanzate (APT) e zero-day, proteggendo le caselle di Microsoft 365, Google Workspace e Open-Xchange. La funzionalità sfrutta una soluzione di sicurezza e-mail in cloud di nuova generazione basata su Perception Point.

### Filtro antispam

Il sistema blocca le email dannose con filtri anti-spam basati sulla reputazione, sfruttando i dati combinati di diverse tecnologie leader di mercato.

### Antielusione

Individua il contenuto dannoso occulto con la decompressione ricorsiva dei contenuti in unità più piccole (file e URL) che vengono analizzate dinamicamente da più motori in meno di 30 secondi.

### Intelligence delle minacce

L'intelligence sulle minacce, con informazioni combinate provenienti da sei origini leader di mercato, scansiona gli URL e i file in circolazione.

### Analisi statica basata sulla firma

Il sistema identifica le minacce note con i migliori motori antivirus per identificare firme altamente complesse.

### Anti-phishing

È in grado di rilevare gli URL dannosi e bloccarli, grazie ai quattro principali motori di reputazione degli URL, combinati alla tecnologia di riconoscimento dell'immagine avanzata di Perception Point che convalida gli URL stessi.

### Anti-spoofing

Previene attacchi senza payload (spoofing, domini simili e nomi visualizzati ingannevoli) grazie ad algoritmi di apprendimento automatico e con i controlli di reputazione IP, SPF, DKIM e DMARC.

### Rilevamento dinamico di nuova generazione

Individua e blocca gli attacchi avanzati come APT e zero-day con l'esclusiva analisi a livello di CPU che li rileva e li blocca nella fase di exploit, identificando le deviazioni dal normale flusso di esecuzione durante il runtime.

### Reporting

Fornisce set di dati facilmente accessibili e gestibili, nonché report settimanali, mensili e ad hoc.

### Guida contestuale per l'utente finale

Il sistema contrassegna le e-mail con banner personalizzabili in base a criteri, l'opzione è utile a fornire informazioni aggiuntive e aumentare la consapevolezza riguardo all'email security.



## ADVANCED BACKUP

L'opzione rafforza le funzionalità del backup ed estende le sue capacità a SAP HANA, Oracle DB e cluster di applicazioni. Il backup può essere abilitato sia per workstation, che per Virtual Machine e Server.

### **Protezione continua dei dati**

Permette agli utenti di non perdere il lavoro non salvato definendo una lista di applicazioni critiche utilizzate di frequente. Monitora tutte le applicazioni in elenco ed effettua costantemente il salvataggio delle informazioni tra un backup pianificato e l'altro, garantendo che nessun dato vada perduto.

### **Mappa della protezione dei dati**

La mappa della protezione offre uno strumento di reportistica che permette di conoscere quali dati e sistemi sono monitorati e protetti.

### **Report dei backup pianificati**

La funzionalità offre visibilità della protezione dei dati inviando periodicamente i report dei backup in formato PDF o Excel, nella lingua richiesta e ai destinatari definiti.