TWT
CONNECT YOUR BUSINESS

DATA PROTECT

CYBERSECURITY, MANAGEMENT, BACKUP & DISASTER RECOVERY

The service combines the principal functions for cyber protection such as: backup, anti-ransomware and anti-malware, endpoint protection, disaster recovery and much more besides.

TWT Data Protect is the in-cloud solution that **integrates cybersecurity, data protection and endpoint management** to fully protect devices, systems and data, while eliminating complexities.

Advantages

- Data stored and managed in Italy (in compliance with current legal provisions, such as the GDPR)
- Data protected by means of encryption
- Assistance provided by 1st and 2nd level technicians
- Redundancy of systems and infrastructures
- One single and intuitive console protected by 2 Factor Authentication (2FA)
- One solution for all essential functions
- Maximum integration between services and various functions
- Unlimited scalability in the cloud for simple adaptation to any requirement
- The four main elements of the service are also available in Advanced mode

ESSENTIAL FUNCTIONS

Essential functions for the security and complete protection of data and systems from cyber threats.

Active protection
Thanks to AI-based technologies, the service actively protects systems from cyber threats. In fact, static and behavioural analyses enable the prevention of any criticalities.

AI-based anti-malware and antivirus to counter ransomware and zero-day threats
The antivirus is based on artificial intelligence to protect from malware, ransomware, cryptojacking and other cyber threats.

Device control
Analyses devices rapidly to detect and prevent unauthorized access to data and their transmission through local computer channels.

Vulnerability Assessment
Identifies and mitigates security vulnerabilities, thanks to on-going system scans.

Essential functions for the centralized management of protection systems, for the rapid configuration of endpoints, for the assistance of remote users and the monitoring of security.

Centralized security management
It is possible to optimize the efforts of the IT department thanks to the centralized management of protection plans that include all the necessary security configurations.

Remote assistance
Enables assistance to be provided, by operating remotely on the user's endpoint. Before the session, a notice will be clearly displayed on the user's screen asking them to grant consent to remote assistance on their device.

Collection of hardware inventories
Provides a constantly updated inventory of all hardware resources by effecting automatic and manual scans.

The backup function is available both in the cloud and locally. It can be planned to suit specific requirements in terms of timing and content, without interfering with everyday activities.

Backup of files and applications
This is the ideal and perfectly secure data management and maintenance solution, since it enables the Client to set the automatic save function of their virtual or physical infrastructure.
Data are stored in Italy at the TWT Data Center and saved on Enterprise-class storage.

Incremental and differential backup
These are two types of data saving methods enabling the optimization of backup space and times, since they analyse the modified files by comparing them to one of the first complete backups rather than creating completely new backups each time data is saved.

Protection of Google Workspace and Microsoft Office 365 data
It is possible to protect the data contained and created in Microsoft Exchange Online, OneDrive for Business, Microsoft Teams, SharePoint Online, Gmail, Drive, Contacts and Calendar, thanks to the cloud-to-cloud backup.

Backup and storage of encrypted data
The encryption of AES-256 backups ensures compliance with legislative norms and enhances the security of transiting or stored data.

Deduplication
The system detects duplicate data in backups and saves space, by not storing the same data repeatedly.

Monitoring and reporting
A dashboard displays detailed information and a wide range of reports, which are ideal for detecting and solving criticalities rapidly, monitoring the systems and planning activities.

The Disaster Recovery solution enables uninterrupted access to all company resources even in the event of catastrophic or unforeseen events, so that business continuity is safeguarded.

ADVANTAGES

The replication mechanism can cover any workload, whether originating from Windows or Linux.

It just takes a few minutes to transfer production workloads to the in-Cloud data centre, also in the event of a problem involving the entire site, to recover operativity very rapidly.

The Client can launch tests on their own at any time. The test makes a disaster recovery attempt, by simulating the start-up of the machines in the secondary site, without interfering with the production machines (Primary site). This operation makes it possible to check that Disaster Recovery replications and procedures work correctly.

Improve the levels of protection with the **advanced options**:

ADVANCED SECURITY

The Advanced Security option enhances integrated cyber protection and responsiveness in countering new cyber threats. It extends protection to Internet browsing, backup data and the data recovery process, as well as preventing exploits. Moreover, it enables the acquisition of forensic data for any investigation purposes.

URL filter
This function enables systems to be protected from cyber threats such as malware and phishing originating from URLs. Thanks to this system, it is possible to block the users' access to potentially dangerous Internet websites.

Exploit prevention
Ideal for preventing advanced attacks such as those of the zero-day and fileless types, by exploiting behavioural analysis.

Forensic analyses
This function gathers and stores digital evidence for use in the event of forensic investigations being required and to enable a rapid resolution in the case of an incident.

Backup recovery with antimalware and antivirus inspection
Thanks to the integrated antimalware scan, the system prevents the recovery of infected files from the backup. In fact, this service enables the detection of any viruses and ensures that backup data are completely safe.

ADVANCED MANAGEMENT

The Advanced Management option simplifies vulnerability management and enables the IT infrastructure to be improved through an even more advanced patch management.

Patch management
Patches and software updates for preventively correcting vulnerabilities are essential for guaranteeing the protection of company environments. The function enables the planning or manual distribution of patches to ensure uninterrupted data protection.

Fail-safe patching
A patch containing errors can make a system inoperable. For this reason, before implementing the latest patches, the service creates an automatic backup to facilitate reversion of the system to a previous state whenever necessary.

Monitoring of hard disk status
The function monitors the integrity of the hard disk by exploiting machine learning, to anticipate criticalities and indicate the measures that need to be taken to correct them at an early stage.

Gathering of software inventories
Enables constant access to the software inventory and saves time. Effects automatic or manual system scans to provide a complete overview of all installed software.

ADVANCED EMAIL SECURITY

This option raises the protection levels of e-mail boxes by identifying any malicious emails before they reach the end-users.
It blocks such threats as spam, phishing, business e-mail compromise (BEC), ransomware and malware, advanced persistent threats (APT) and zero-day, by protecting the mailboxes of Microsoft 365, Google Workspace and Open-Xchange. The function exploits an in-cloud e-mail security solution of the latest generation based on Perception Point.

Antispam filter
To block malicious emails with reputation-based anti-spam filters, by exploiting combined data of various market leading technologies.

Anticircumvention
To detect occult malicious content by means of the recursive decompression of contents into smaller units (files and URLs) which are analysed dynamically by more than one engine in less than 30 seconds.

Threat intelligence
With integrated information from six market leading sources, threat intelligence scans the URLs and files in circulation.

Signature-based static analyses
The system detects known threats with premium antivirus engines to identify highly complex signatures.

Anti-phishing
To detect malicious URLs and block them, thanks to the four main URL reputation search engines, combined with Perception Point advanced image recognition which validates URLs.

Anti-spoofing
To prevent payload-less e-mail attacks (spoofing, deceptive look-alike source addresses and names) thanks to automatic learning algorithms and IP, SPF, DKIM and DMARC reputation checks.

Latest generation dynamic detection
To identify and block advanced attacks such as APT and zero-day with analysis at CPU level only, which detects them and blocks them in the exploit phase, by identifying deviations from the normal execution flow during runtime.

Reporting
To provide sets of data that are simple to access and manage, along with weekly, monthly and special reports.

Contextual guidelines for the end-user
The system marks e-mails with banners that may be personalized to reflect certain criteria. This option is useful for supplying additional information and enhancing awareness of e-mail security.

ADVANCED BACKUP

This option strengthens the backup functions and extends their capacity to SAP HANA, Oracle DB and application clusters. The backup may be enabled for both workstations and for Virtual Machines and Servers.

On-going data protection
Enables users not to lose unsaved work by defining a list of frequently used critical applications. It monitors all the applications in the list and constantly saves information between one planned backup and another to ensure that no data are lost.

Data protection map
The data protection map provides a reporting tool with information on which data and systems are monitored and protected.

Planned backups report
This function provides data protection visibility by sending periodic backup reports in PDF or Excel format, in the requested language and addressed to pre-defined recipients.