



# Valtellina Cyber Security Solution



# la società Valtellina

Dal 1937 Valtellina è all'avanguardia nella trasformazione di società e industria.

Valtellina da sempre precorre i tempi: TLC, Banda Larga, Energie Rinnovabili, Data Center, Smart City, Fabbriche 4.0.

**Dove si costruisce il progresso, dove si realizza il futuro, c'è Valtellina. In Italia e nel mondo.**

## Valtellina nel mondo



Fatturato complessivo 2017: ca. € 180 milioni



Numero addetti: oltre 1.800 collaboratori



Sedi operative: Italia 21; Romania 1; Brasile 4; Argentina 2

## Quality System

Il Sistema di Gestione Integrato è verificato con frequenza annuale dagli Enti di Certificazione. Per assicurare un livello qualitativo sempre crescente sia in termini di servizio erogato che di professionalità delle proprie risorse, la Direzione Generale, informa, forma, addestra e coinvolge il personale di ogni livello e funzione aziendale.



**ITALIA**  
ISO 9001:2015  
ISO 14001:2015  
ISO 45001:2018  
ISO 27001:2013



**ROMANIA**  
ISO 9001:2008  
ISO 14001:2004  
OHSAS 18001:2007

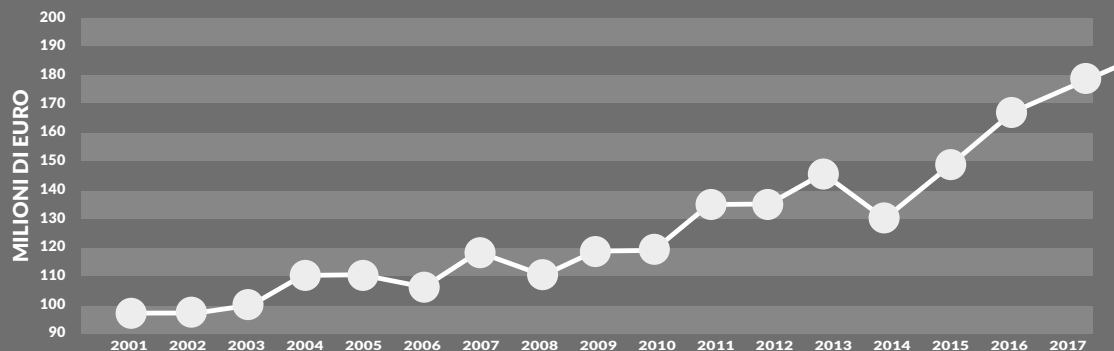


**ARGENTINA**  
OHSAS 18001:2007



**BRASILE**  
ISO 9001:2015  
ISO 14001:2015  
ISO 18001:2007

## Trend di mercato

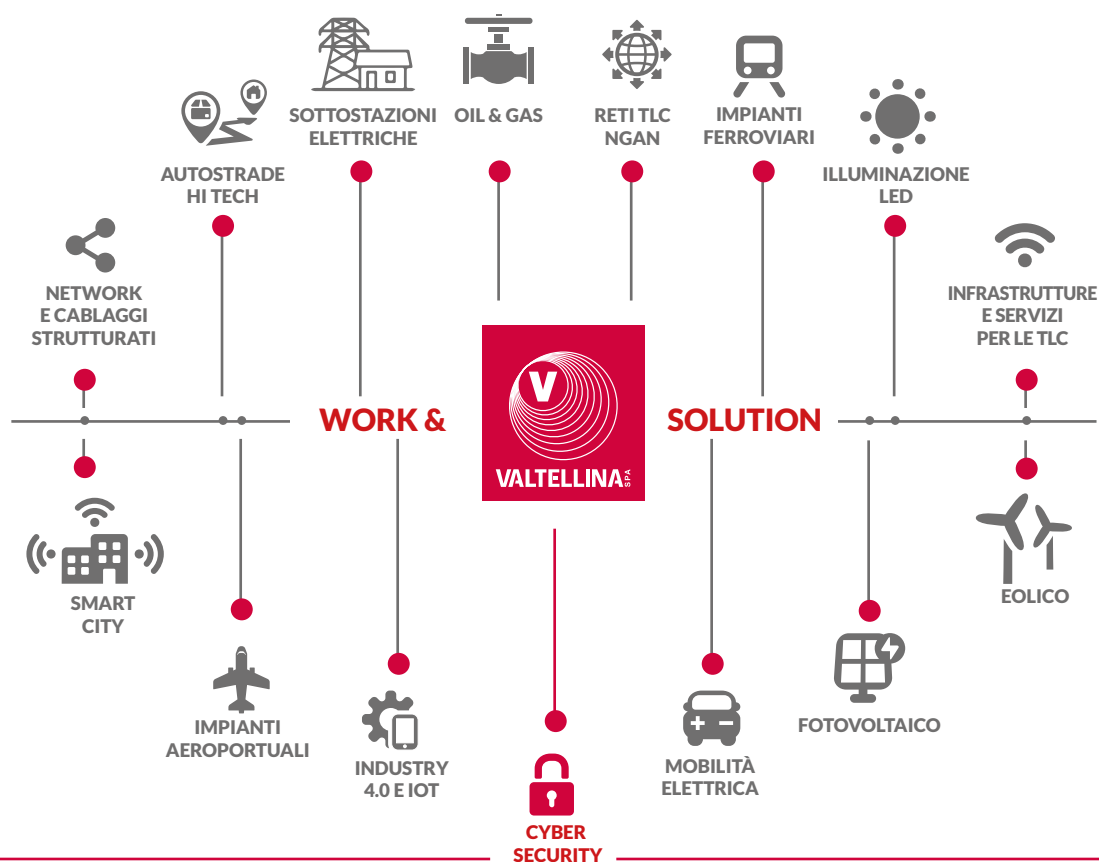


# le divisioni operative

La Cyber Security è parte integrante dell'evoluzione della Valtellina finalizzata ad essere System Integrator in diverse soluzioni trasversali al mondo TLC.

Valtellina offre soluzioni all'avanguardia e competitive in settori sinergici al proprio core business storico, vale a dire le infrastrutture per reti di telecomunicazione. Ciò si attua in campi d'intervento strategici per il funzionamento di strutture complesse e delicate come gli aeroporti, dove la Cyber Security è decisiva.

La propositività spazia dall'Industria 4.0 alle Smart Cities, che vedono la Cyber Security come componente essenziale dell'operatività.



MANTIENE PRIVATE LE TUE INFORMAZIONI E PASSWORD



FA ATTENZIONE A CIÒ CHE PUBBLICHI ONLINE



CONTROLLA LE TUE IMPOSTAZIONI SULLA PRIVACY



ACQUISTA IN SICUREZZA IN SITI WEB AFFIDABILI



VERIFICA PASSWORD SICURA



PROTEGGE TUTTI I TUOI DISPOSITIVI CON UN ANTIVIRUS



RICORDA DI DISCONNETTERTI



CONTROLLA L'URL DEL SITO WEB



CONTROLLA LE EMAIL PRIMA DI APRIRLE



EVITA PHISHING E TRUFFE

# I pericoli

Da quando il Cyberspazio è diventato dominio operativo, l'attenzione su questo tema è incrementata in modo non trascurabile, soprattutto se si considera la complessa natura degli attacchi informatici e la loro rapidità nell'evolversi.

Si tratta di attacchi sempre più mirati e basati su campagne di infezione tramite malware avanzati, appositamente costruiti o che sfruttano vulnerabilità del sistema in cui si trovano. Gli attacchi sono specifici per l'organizzazione bersaglio e quindi in grado di aggirare le soluzioni di protezione tradizionali.

Tatticamente è richiesto quindi un cambio di approccio tecnologico per dotare le infrastrutture di strumenti avanzati di indagine degli incidenti digitali.

**È necessario superare i limiti tecnologici che hanno segnato il recente passato nella lotta ai crimini informatici e ottenere da un sistema difensivo i seguenti vantaggi tattici:**

- nessuna superficie di attacco
- nessun sovraccarico di risorse sui sistemi
- nessun punto cieco nell'analisi di sicurezza.



E-MAIL MALWARE



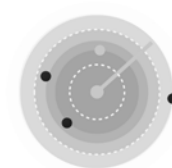
TROJAN



FIREWALL



LOGIC BOMB



SCANNING SYSTEM



COMPUTER WORM



DDOS ATTACK



PHISHING



CREDIT CARD FRAUD



DATA LOSS



PASSWORD



SOFTWARE BUG

# La soluzione

Per essere in grado di rilevare, tracciare e rispondere agli attacchi in modo estremamente efficace, Valtellina e il partner Reaqta propongono il progetto ProBOS (Protection Beyond Operating System - Development of the next generation cyber security solution).

Dal progetto, parte del programma Horizon2020 della Comunità Europea, è stata generata la soluzione Hive.

Hive risponde alle minacce e protegge le organizzazioni da attacchi noti e non, adottando un approccio completamente nuovo e basato su:



**INTELLIGENZA  
ARTIFICIALE**



**FUNZIONALITÀ DI  
HYPERVISORING**



**ANALISI  
DINAMICA  
DEI PROCESSI**



**ANALISI BIG  
DATA DEI  
COMPORAMENTI**

Hive è una soluzione di analisi post-exploitation, basata su analisi comportamentale di processo (unica al mondo a farlo in locale) con diversi campi di applicazione:



**SOC/CERT/  
CSIRT**



**Endpoint  
Protection**



**Normative  
(GDPR/NIS)**



# BUSINESS CASE

## AEROPORTO MILANO BGY

La necessità della Cyber Security è fra i temi più importanti e delicati in senso assoluto per una realtà complessa come un aeroporto, dove l'informatica è imprescindibile per il suo funzionamento: dal controllo dei voli, alla gestione dei servizi interni che coinvolgono direttamente i passeggeri. I sistemi IT e ICT possono essere a ragione considerati "il cervello" di un moderno aeroporto, che non può permettersi momenti di crisi o, peggio, di andare in tilt. Questa esigenza è ancora più impegnativa e stringente per una struttura come quella dell'aeroporto di Milano Bergamo, che in questi ultimi anni è cresciuto maggiormente in Italia e si colloca come terzo scalo nazionale con un movimento di oltre 12 milioni di passeggeri nel 2017.

La sicurezza informatica, la prevenzione dagli attacchi di hacker, sono considerati aspetti primari e quindi meritevoli di massime attenzioni anche dal punto di vista delle forniture di specifici servizi IT e di rete.

In tale contesto SACBO, società che gestisce lo scalo bergamasco, ha affidato la sua cyber sicurezza per i prossimi tre anni a Valtellina. Da sottolineare come SACBO ha potuto verificare direttamente la competenza e

professionalità dei nostri specialisti in quanto ci occupiamo da tempo della gestione e conduzione dell'infrastruttura PASSIVA/ ATTIVA di rete esistente nell'aeroporto di Milano Bergamo.

Il contratto è stato rinnovato ad inizio 2018: ci siamo nuovamente aggiudicati il servizio per la gestione e la conduzione dell'intera infrastruttura di rete aeroportuale e degli uffici di SACBO per i prossimi 4 anni.

Lo scorso 3 luglio è stato sottoscritto un nuovo accordo/contratto, sinergico e aggiuntivo alla collaborazione già in essere, appositamente dedicato alla sicurezza informatica: cureremo, come sopra riportato, il servizio di Cyber Security interno della stessa infrastruttura.

### **LA SOLUZIONE HIVE È STATA DA NOI PROPOSTA A SACBO IN COLLABORAZIONE CON LE SOCIETÀ REAQTÀ E CYBER ARMOR.**

HIVE è frutto dell'impegno di ricerca della società ReaQta che l'ha elaborata; la specifica soluzione destinata ad essere applicata presso l'Aerostazione di Milano Bergamo, è stata sviluppata nell'ambito della collaborazione commerciale attualmente in essere tra Valtellina e Cyber Armour (distributrice di HIVE) e di cui Valtellina è Partner.

### **VANTAGGI IMPORTANTI ANCHE SUL FRONTE "PRIVACY"**

La validità della soluzione permetterà a SACBO di essere all'avanguardia per quanto riguarda il delicato tema dell'antifrode/anti breccia nei confronti di attacchi strutturati (attacchi informatici contro bersagli sensibili) e predisporre le condizioni ottimali anche sul fronte dei nuovi regolamenti europei sulla privacy.





## IL SERVIZIO DI CYBER SECURITY DI VALTELLINA RIGUARDA I SEGUENTI CAMPI DI APPLICAZIONE

- 1** Ricostruire automaticamente un attacco anche complesso dal punto di vista logico, ripulendo le informazioni utili dal rumore, indicando l'albero di interazione dei processi coinvolti (compresi movimenti laterali di utente/macchina).
- 2** Ricostruire automaticamente l'attacco dal punto di vista temporale, indicando per ogni processo quali eventi sono stati generati (descritti per tipo e severità, come escalation di privilegi o creazione di persistenza, etc.).
- 3** Dettagliare gli eventi associati fino alla generazione di IoC per ciascun evento (sempre con la possibilità di mitigare centralmente con un click).
- 4** Isolare gli endpoint a livello hypervisor per raccogliere evidenze forensi e/o proseguire nell'analisi della minaccia senza compromettere il resto della rete.
- 5** Ricercare rapidamente IoC su tutta l'infrastruttura.
- 6** Ricercare e individuare backdoor dormienti e varianti di malware per una completa sanificazione post-incidente.

Il servizio proposto da Valtellina funzionerà inoltre anche come Endpoint Protection, ad esempio nel caso di malware, ransomware o attacchi specifici (anche tipo fileless e full in-memory), con una sandbox attiva H24 su ogni endpoint, anche se offline.

## EUROPA



**ITALY**  
HEADQUARTERS  
VALTELLINA S.p.A.  
valtellina@valtellina.com  
Via Buonarroti, 34  
24020 Gorle (Bergamo)  
Tel. +39 035 42 05 111  
Fax +39 035 29 77 29



**ROMANIA**  
VALTELLINA EST EUROPA  
valtellinaee.ro@valtellina.com  
Strada Turda n. 50  
550052 Sibiu Romania  
Tel. +40 269259939  
Fax +40 269240264

## AMERICA



**ARGENTINA**  
VALTELLINA SUD AMERICA  
vsa.comunicaciones@valtellina.com.ar  
Buenos Aires  
Parque Industrial Buen Ayre (PIBA)  
General Martín de Gainza 801  
Moreno (C.P. 1744) Buenos Aires  
Tel. +54 0237 4057770 / 75

Rosario  
Edison 857  
Villa Gobernador Gálvez  
(C.P. 2124) Provincia de Santa Fe  
Tel. +54 0341 3171888/9



**BRAZIL**  
VALTELLINA DO BRASIL  
valtellinadb.br@valtellina.com São Paulo  
Rua Waldemar M. Ferreira, 67  
Jordanópolis  
São Bernardo do Campo - SP  
CEP 09891-010

Rio de Janeiro  
Rua Conego Felipe, 315  
Taquara RJ  
CEP 22713-010

Niteroi  
Rodovia Amaral Peixto, Km 06  
Tribobaó São Gonçalo - RJ  
CEP 24750-070

Jaboatão  
Rua Prof. Paes Leme, 90  
Piedade - Jaboatão dos Guararapes - PE  
CEP 54400-460