

## Informazioni sui servizi

La Sicur Control System Srl è una società che opera nel settore della Safety Solutions come System Integrator.

I segmenti di mercato interessati vanno dall' **Istruzione** (Università, scuole, istituti di istruzione), al **Banking & Finance** (banche, uffici postali, imprese di assicurazione), fino ad interessare il **commercio al dettaglio** (negozi, distributori di benzina, supermercati), i **trasporti** (aeroporti, ferrovie, porti, sorveglianza del traffico, stazioni di pedaggio), ed il **settore industriale** (industrie di processo, di ingegneria, edili, farmaceutiche, energetiche ed imprese). Di particolare rilievo sono le esperienze maturate in ambito **Istituzionale** (Forze di Polizia, militare, carceraria).

La Sicur Control System Srl ha stretto alleanze con aziende produttrici nel settore delle telecomunicazioni, videocontrollo e produzione software al fine di offrire ai nostri clienti soluzioni personalizzate e tecnologicamente all'avanguardia.



## Partnership



## Certificazioni



Dasa-Rägister  
EN ISO 9001:2008  
IQ-0611-09

## Sicur Control Sistem S.r.l.

Via Benedetto Croce snc, 87046 Montalto  
Uffugo (CS)  
Sede Operativa:  
C/da Piano di Maio snc, 87036 Rende (CS)

Tel.: +39 0984 446959  
Fax: +39 0984 448146

Website: [www.sicurcontrolsystem.it](http://www.sicurcontrolsystem.it)  
Indirizzo di posta elettronica:  
E-mail: [info@scs-web.it](mailto:info@scs-web.it)  
PEC: [info@pec.scs-web.it](mailto:info@pec.scs-web.it)



La protezione dei dati e dei beni intellettuali è un compito essenziale per qualsiasi azienda.

L'accesso, la trasmissione, l'elaborazione e la gestione del dato attraverso i più diversi strumenti di comunicazione, dal server al PC o notebook, dal cellulare al tablet, è ormai un fattore fondamentale per il successo delle aziende di qualsiasi dimensione e tipologia.

Inoltre la continuità dei servizi di rete e l'accessibilità ininterrotta alle informazioni sono fondamentali ed ogni organizzazione deve essere in grado di proteggere i dati e le informazioni da minacce di ogni tipo in un contesto dove i rischi informatici, causati dalle violazioni dei sistemi di sicurezza, sono in continuo aumento.



## Integrità

## Riservatezza

## Disponibilità

obiettivi principali della sicurezza di un' impresa

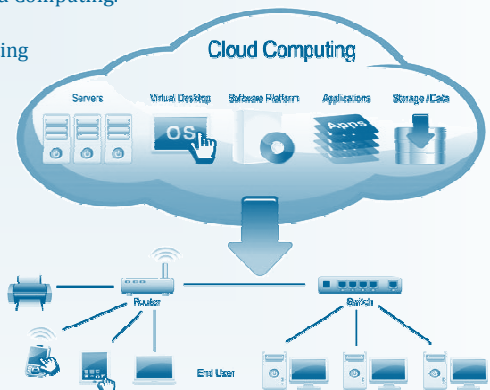
# Sicurezza tra le nuvole: il Cloud Computing

Gli ultimi sviluppi nel settore ICT hanno prodotto un cambiamento radicale di prospettiva nella gestione delle infrastrutture tecnologiche facendo sì che il business punti forte sul Cloud Computing.

Il Cloud Computing consente di trasferire le attività gestionali delle aziende dai propri pc, soggetti a rischi ed a costi di manutenzione, verso strutture centralizzate in grado di assicurare monitoraggio e protezione, generando importanti vantaggi in termini di innovazione (grazie ai software costantemente aggiornati ed efficienti), riduzione dei costi (grazie alla virtualizzazione in remoto) e miglioramento dell'affidabilità (che include stabilità e sicurezza).

Il Cloud Computing nasce per soddisfare due specifiche esigenze: prevenire la perdita accidentale o dolosa dei propri dati informatici con strutture altamente qualificate e renderne disponibile l'accesso da qualunque postazione di lavoro dotata di una connessione ad internet, sia esso il pc di casa o uno smartphone avanzato.

Le aziende fornitrici di servizi Cloud necessitano di soluzioni efficaci, scalabili ed elastiche per il management della sicurezza dei dispositivi mobili, delle workstation e dei server, e per la protezione della loro rete contro le minacce esterne.



cloud computing architecture security scalability web applications privacy ISO Certifications Https SSL

I vantaggi offerti da una gestione del sistema in modalità Cloud dipendono dalla possibilità di spostare facilmente dati, macchine virtuali e applicazioni da un server all'altro, all'interno e tra diversi data center sicuri. Quindi, è necessario avere la certezza che l'infrastruttura sia adeguatamente sicura prima di eseguire qualsiasi tipo di migrazione e/o di elaborazione. Per questo, i dati sono immagazzinati in un datacenter privato protetto da firewall, i database crittografati e vengono utilizzati dei meccanismi più o meno sofisticati per l'individuazione di intrusioni da parte di cyber-crime.

I sistemi di Cloud Computing non sono meno sicuri dei sistemi tradizionali, ma possono essere messi a rischio a causa del comportamento inopportuno degli utenti. L'utilizzo di prodotti e meccanismi di sicurezza non adeguati, lascia i sistemi Cloud esposti e vulnerabili ad una larga serie di attacchi, rischiando di dovere affrontare diverse problematiche tra cui malware, mancato aggiornamento da parte degli utenti dei sistemi con successiva perdita dei dati, e più frequentemente all'installazione di applicazioni nocive finalizzate al furto di dati privati quali codici di carte di credito ecc.

La *Sicur Control System Srl* propone una vasta gamma di soluzioni hardware



Network Firewall Policy Internet Protocol Protocol Firewall Security

re, software o combinazione di entrambi per consentire ai possessori di sistemi Cloud di rafforzare la policy di sicurezza aziendale. Tale protezione è ottenuta attraverso misure organizzative e tecnologiche tese ad assicurare l'accesso solo ad utenti autorizzati (autenticazione), la fruizione (disponibilità) di tutti o soli i servizi previsti per quell'utente nelle modalità previste dal sistema, l'oscuramento (crittografia) dei dati scambiati in una comunicazione e la protezione del sistema da attacchi di software malevoli.

I sistemi offerti consentono di preservare gli asset aziendali da utilizzi impropri e garantire una maggiore sicurezza, compliance ed impedire comportamenti nocivi finalizzati al furto e/o alla manomissione di dati sensibili (prevenzione contro le intrusioni, firewalling applicativo e di rete, web-filtering, antivirus, antispam, QoS, monitoraggio del traffico nei tunnel VPN ed SSL, protezione del traffico VoIP ecc.).

L'offerta prevede anche procedure e sistemi di backup per salvaguardare e preservare i dati e fronteggiare guasti hardware o incidenti all'infrastruttura (Disaster Recovery).

Uno dei prodotti di punta è rappresentato da un sistema di Anomaly Detection ispirato a tecniche di intelligenza artificiale, e utilizzato per identificare accessi non autorizzati o comportamenti anomali degli utilizzatori del sistema Cloud. Il sistema fa uso di pattern (profili) dell'utilizzo normale del sistema ricavati da misure statistiche ed euristiche sulle caratteristiche dello stesso, come la cpu o la memoria utilizzata e le attività di I/O di un particolare utente o programma. Le anomalie vengono analizzate e il sistema ne definisce la pericolosità per l'integrità del sistema ed eventualmente le blocca. Il tutto avviene con l'ausilio di una console amministrativa web-based per il management, il monitoring e il reporting dei dati analizzati.