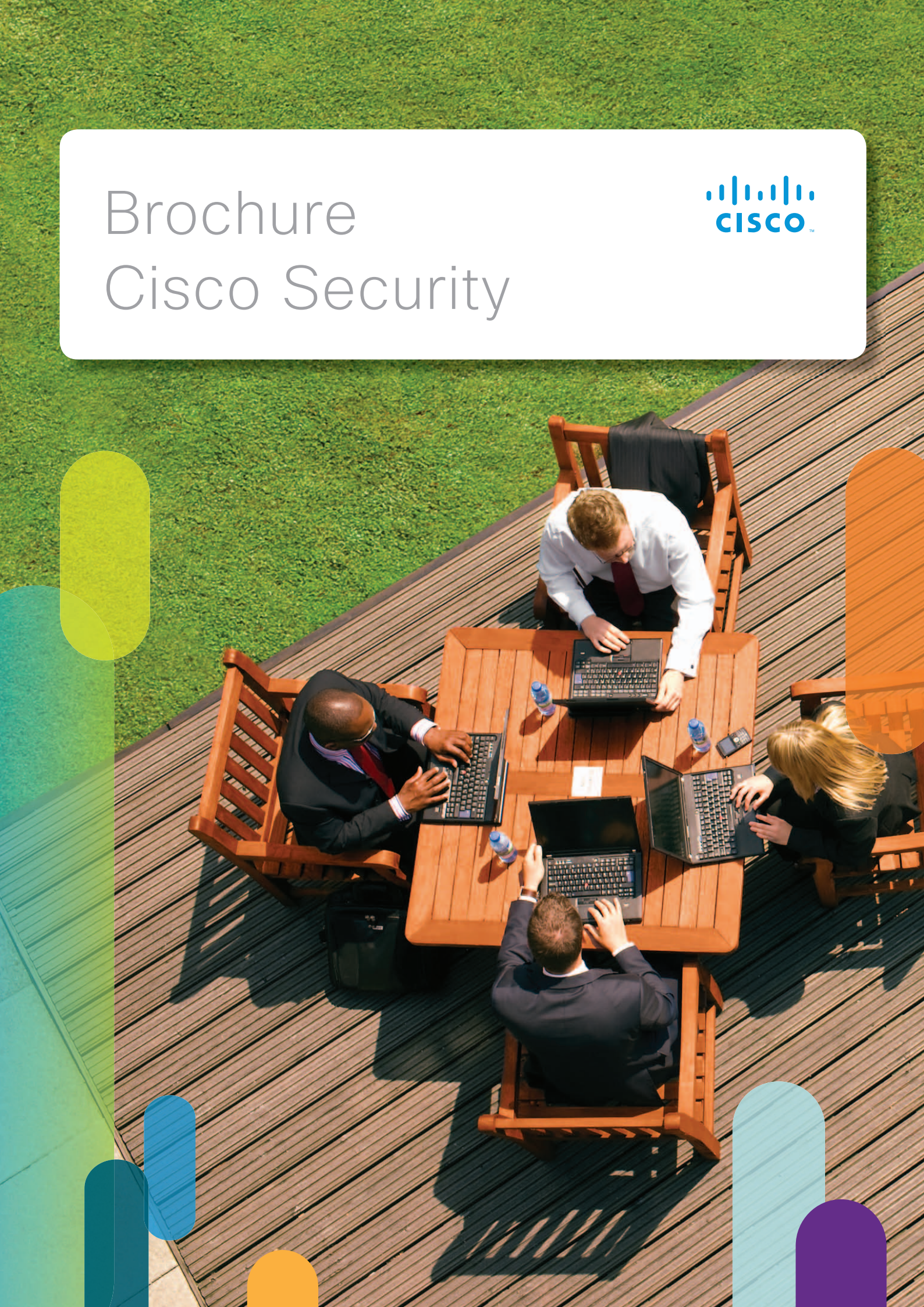


# Brochure Cisco Security

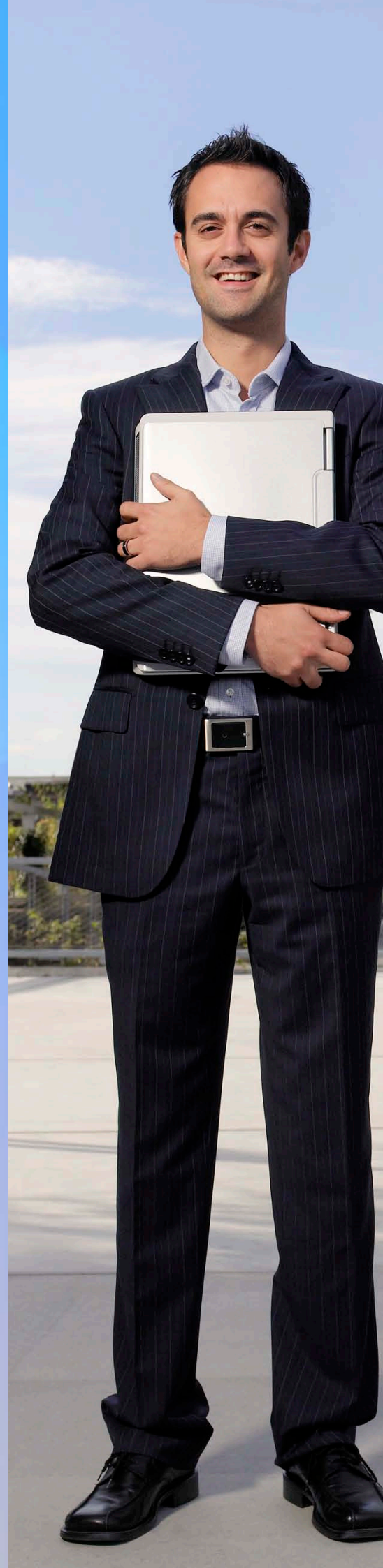


## La sicurezza oggi è ancora più importante

Gli approcci tradizionali alla sicurezza avevano un solo scopo: proteggere le risorse in rete da rischi e malware provenienti dall'esterno.

Oggi, invece, le aziende devono considerare l'uso di smartphone e iPad, la consumerizzazione dell'IT e l'avvento dei social media negli ambienti di lavoro. Inoltre vi sono connessioni di dipendenti da remoto, e l'accesso extranet di fornitori e partner, e a volte anche servizi cloud. La sicurezza ha un ruolo sempre più importante ed è decisamente più complessa.

Le aziende hanno un bisogno continuo di difendersi dalle minacce in rete, di proteggere dati e risorse importanti e implementare i controlli necessari per soddisfare i requisiti delle normative, e una chiara demarcazione tra dentro e fuori non esiste più. A queste sfide si aggiunge la necessità di un approccio collaborativo fra i team e le persone. I responsabili IT devono garantire la protezione delle informazioni senza perdere i benefici garantiti dai nuovi, potenti strumenti di "collaboration".



## Cisco Secure Borderless Networks

Le reti Cisco® Secure Borderless Network permettono alla forza lavoro di essere altamente produttiva e allo stesso tempo aiutano le aziende a tenere sotto controllo i costi e la complessità della sicurezza di rete.

Una Cisco Secure Borderless Network assicura elevatissimi livelli di protezione integrando la sicurezza nella rete. Gli utenti hanno accesso a tutto ciò di cui hanno bisogno, ma il loro accesso è regolato, non solo in base alla user ID o al ruolo, ma anche in base al dispositivo usato. Per esempio, un portatile aziendale avrà livelli di accesso alle risorse più alti rispetto ad uno smartphone personale di un dipendente. Grazie alle tempestive indicazioni fornite da Cisco Security Intelligence Operations, la rete è in grado di far fronte alle minacce, anche le più recenti, bloccandole immediatamente. E con la disponibilità di soluzioni flessibili, varie opzioni di implementazione, partner strategici e servizi globali, una Cisco Secure Borderless Network estende la sicurezza alle persone, ai dispositivi e alle sedi a cui si desidera dare accesso, assicurando la massima protezione.

Scopri in dettaglio le nostre soluzioni nelle pagine seguenti.

 [Continua](#)

## Sicurezza della rete

L'infrastruttura di network security Cisco identifica e blocca le intrusioni, gli attacchi e gli exploit, prevenendo gli accessi non autorizzati. Con l'utilizzo di un firewall e di un sistema di intrusion prevention, disponibili in modalità standalone o integrata, i clienti possono affrontare qualsiasi pericolo e rispettare le normative sulla sicurezza, come lo standard PCI DSS (Payment Card Industry Data Security Standard).

			
<a href="#">Serie Cisco ASA 5500 Adaptive Security Appliance</a>	<a href="#">Cisco Intrusion Prevention System (IPS)</a>	<a href="#">Cisco Next-Generation ISR</a>	<a href="#">Cisco Virtual Security Gateway</a>
<ul style="list-style-type: none"> <li>• Combina firewall, VPN, un'opzione per la sicurezza dei contenuti e un sistema anti-intrusione che estende la sicurezza di rete a tutti i processi aziendali</li> <li>• Fornisce protezione dalle minacce e servizi di comunicazione altamente sicuri per fermare gli attacchi prima che possano interferire con le attività dell'impresa</li> <li>• Riduce i costi di implementazione e offre una sicurezza globale per reti di tutte le dimensioni</li> <li>• Supporta una vasta gamma di ambienti di rete dalle piccole-medie imprese a quelle di grandi dimensioni</li> </ul>	<ul style="list-style-type: none"> <li>• Identifica, classifica e blocca il traffico pericoloso, compresi worm, spyware, adware, virus e application abuse</li> <li>• Offre prestazioni elevate nel riconoscimento intelligente delle minacce e una protezione che copre un'ampia gamma di scenari di implementazione</li> <li>• Analizza in modo correlato ogni minaccia globale con il filtro relativo alla reputazione per prevenire le minacce</li> <li>• Offre la tranquillità di una garanzia per la copertura e la velocità dei tempi di risposta alle vulnerabilità di applicazioni Microsoft, Cisco e numerose altre applicazioni aziendali<sup>1</sup></li> <li>• Promuove la business continuity e aiuta le aziende a soddisfare i requisiti di legge e normativi</li> </ul>	<ul style="list-style-type: none"> <li>• Offre una vasta gamma di funzionalità integrate tra cui firewall, anti-intrusione, VPN e filtraggio del contenuto</li> <li>• Favorisce l'integrazione di nuove funzionalità di network security su router esistenti</li> <li>• Offre ulteriore protezione senza l'aggiunta di hardware e massimizza la sicurezza di rete</li> <li>• Riduce i costi relativi alla manutenzione ordinaria e all'amministrazione, riducendo il numero totale di dispositivi necessari</li> </ul>	<ul style="list-style-type: none"> <li>• Rende sicure le virtual network e gli ambienti di rete multisede</li> <li>• Offre accessi multi-sede affidabili con policy di sicurezza granulari, specifiche per area e content-aware</li> <li>• Supporta il provisioning dinamico delle policy per la sicurezza e delle trust zone durante l'istanza VM (virtual machine)</li> <li>• Permette il rafforzamento della protezione (e il monitoraggio) dei dispositivi mobile</li> </ul>

1. La copertura dipende dalla "signature" per le soluzioni Cisco, Microsoft e di terze parti. I dettagli per il service level agreement, comprendente copertura, rrimedi, termini e condizioni, saranno resi disponibili da Cisco al momento del rilascio, attualmente programmato per la prima metà del 2011. Per maggiori informazioni, contattare il vostro rivenditore Cisco.

## Email e sicurezza web

Le soluzioni Cisco per la sicurezza web ed email riducono il rischio di costosi downtime causati da spam, virus e minacce web. Sono disponibili in varie soluzioni, tra cui dispositivi standalone, servizi di hosted security e implementazioni con gestione centralizzata.



Cisco IronPort Email Security – In modalità cloud, ibrida oppure on-premises

- Offre un approccio a più livelli per combattere spam, virus e minacce combinate allo scopo di proteggere le aziende di ogni dimensione
- Consente un controllo outbound integrato attraverso la prevenzione della perdita di dati e la crittografia
- Riduce i tempi di downtime, semplifica l'amministrazione dei servizi di mailing aziendale e snellisce il lavoro di supporto tecnico
- Offre un reporting completo e la tracciatura della messaggistica per una maggiore flessibilità amministrativa
- Offre soluzioni flessibili per poter evolvere al crescere delle esigenze aziendali



Cisco Web Security – In modalità cloud oppure on-premises

- Offre la difesa più efficace contro i malware basati su web: il Cisco Security Intelligence Operations (SIO) combina la migliore reputazione web del mercato con l'intelligenza nell'analisi dei contenuti
- Fornisce controlli delle policy evoluti e complessi che sono molto efficaci per siti web 2.0 con contenuti dinamici e applicazioni on-line
- Offre delle funzionalità avanzate per il reporting consentendo una visibilità ed una flessibilità senza confronti per l'uso web
- Offre opzioni di implementazione diversificate quali la modalità on-premises, cloud, per utenti mobili ed una combinazione delle stesse

### Un approccio proattivo alle minacce

I prodotti Cisco per la sicurezza anticipano le minacce perché sfruttano l'intelligenza di Cisco Security Intelligence Operations (SIO). Il Cisco SIO è il più grande sistema di sicurezza basato su cloud che utilizza live almeno un milione di feed provenienti dalle soluzioni Cisco email, web, firewall e sistemi di prevenzione delle intrusioni (IPS) installate.

Cisco SIO soppesa e processa i dati, classificando automaticamente le minacce e creando regole con più di 200 parametri. I ricercatori di sicurezza raccolgono e forniscono le informazioni sugli eventi di sicurezza che possono impattare significativamente le reti, applicazioni e dispositivi.

Le regole vengono fornite dinamicamente ai dispositivi Cisco di sicurezza installati ogni 3-5 minuti. Il team Cisco SIO pubblica inoltre le raccomandazioni sulle migliori pratiche e consigli tattici per contrastare le minacce.

Per maggiori informazioni, visitare il sito [www.cisco.com/go/sio](http://www.cisco.com/go/sio)

## Secure Mobility

Cisco promuove la connettività mobile altamente sicura con VPN, sicurezza wireless e con le soluzioni di sicurezza per il telelavoro che estendono l'accesso alla rete in modo semplice ma protetto ad una vasta utenza e ad un'ampia gamma di dispositivi. Le soluzioni Cisco Secure Mobility offrono i più completi e versatili endpoint, opzioni di connettività e piattaforme per venire incontro alle esigenze diversificate ed in evoluzione delle aziende.



### La soluzione Cisco AnyConnect Secure Mobility

- Fornisce un'esperienza di connettività intelligente, agevole e affidabile
- L'ideale per aziende che vogliono dare agli utenti una scelta di come, quando, dove e con quale dispositivo accedere ai loro dati
- Si combina con i dispositivi Adaptive Security Serie ASA 5500 a livello di headend per forzare la policy relativa alla connettività con accesso remoto, la quale è content-aware, ampia e preventiva
- Incorpora le appliance Cisco IronPort S-Series Web Security per l'applicazione delle policy "context-aware", tra cui il potenziamento dell'utilizzo accettabile e la protezione da malware per tutti gli utenti

### Il software Cisco Adaptive Wireless IPS

- Fornisce il monitoraggio automatizzato e wireless delle performance e delle vulnerabilità per offrire visibilità e controllo attraverso la rete
- Mantiene una costante attenzione sull'ambiente RF per soddisfare le esigenze delle reti più grandi
- Svolge un monitoraggio automatico allo scopo di rilevare anomalie della rete wireless e per identificare accessi non autorizzati e attacchi RF
- Si integra con i prodotti Cisco per la network security per creare un approccio a più livelli alla wireless security

### Cisco Virtual Office

- Estende a dipendenti che lavorano fuori dagli ambienti di lavoro tradizionali servizi di rete altamente sicuri, completi e gestibili
- Attraverso le versioni standard o express offre un'efficace scalabilità per soddisfare i requisiti delle diverse implementazioni
- Comprende sistemi headend e di siti remoti, aggregazione di siti remoti e servizi forniti da Cisco e da partner certificati
- Offre ai dipendenti un'esperienza simile a quella in ufficio ovunque si trovino attraverso servizi completi di telefonia IP, wireless, dati e video




## Secure Access Control

Cisco TrustSec® fornisce l'accesso sicuro alla vostra rete e alle sue risorse attraverso un controllo degli accessi basato sulle policy, sul networking "identity-aware", e sull'integrità dei dati e servizi di confidenzialità. Cisco TrustSec vi permette di essere conformi ai requisiti normativi, potenziare la sicurezza e aumentare l'efficienza operativa. È disponibile come appliance o come servizio integrato 802.1X basato sull'infrastruttura.

		
<p><a href="#">Network Admission Control Appliance</a></p>	<p><a href="#">Cisco Secure Access Control System</a></p>	<p><a href="#">La soluzione CiscoWorks LAN Management</a></p>
<ul style="list-style-type: none"><li>• Applica le policy di network security su tutti i dispositivi permettendo l'accesso solo ai dispositivi "conformi" e fidati</li><li>• Blocca l'accesso ai dispositivi non conformi e limita i potenziali danni causati da rischi e minacce emergenti</li><li>• Protegge gli investimenti esistenti attraverso la compatibilità con applicazioni di gestione di terze parti e opzioni di implementazione flessibili</li><li>• Riduce virus, worm, e il rischio di accessi indesiderati, promuovendo l'efficienza e integrandosi con altri prodotti Cisco</li></ul>	<ul style="list-style-type: none"><li>• Controlla l'accesso alla rete in base a condizioni e attributi dinamici attraverso un'interfaccia di gestione facile da usare</li><li>• Soddisfa i requisiti di accesso attraverso politiche "rule-based" particolarmente flessibili e facili da gestire</li><li>• Semplifica le attività di amministrazione e aumenta la compliance attraverso il monitoraggio integrato, la reportistica e le funzionalità di troubleshooting</li><li>• Adotta una politica degli accessi che sfrutta le funzionalità di integrazione incorporate e l'implementazione distribuita</li></ul>	<ul style="list-style-type: none"><li>• Semplifica la configurazione, l'amministrazione, il monitoraggio e il troubleshooting delle reti Cisco</li><li>• Massimizza la sicurezza della rete attraverso l'integrazione con i sistemi di controllo degli accessi TrustSec e le verifiche di cambiamenti a livello di rete</li><li>• Aumenta la disponibilità generale della rete identificando e risolvendo velocemente i problemi</li></ul>

## Gestione della sicurezza

Cisco offre strumenti centralizzati per semplificare la gestione dell'intera implementazione della vostra sicurezza di rete. Inoltre, Cisco è partner dei migliori vendor di tecnologie per poter offrire sistemi SIEM (Security Information and Event Management) pre-testati e pienamente compatibili con i prodotti per la sicurezza Cisco. Questa varietà di opzioni di gestione vi offre la flessibilità di scegliere le soluzioni di amministrazione della network security che meglio si adattano alle vostre esigenze di business e al vostro ambiente di lavoro.

		
<b>Cisco IronPort Security Management Appliance</b>	<b>Cisco Security Manager</b>	<b>Partner SIEM approvati</b>
<ul style="list-style-type: none"><li>• Semplifica la gestione della sicurezza attraverso i prodotti Cisco IronPort per la sicurezza email e web</li><li>• Offre ai dispositivi per la sicurezza della posta elettronica un servizio di reportistica centralizzato, il tracciamento dei messaggi e la messa in quarantena dello spam</li><li>• Fornisce ai dispositivi di web security la gestione centralizzata delle web policy</li><li>• Permette di delegare l'amministrazione delle politiche di accesso al web e di avere categorie URL personalizzate</li></ul>	<ul style="list-style-type: none"><li>• Facilita la configurazione e la gestione di firewall, VPN, sensori IPS e servizi di sicurezza integrata Cisco</li><li>• L'ideale per il controllo delle implementazioni grandi o complesse dei dispositivi Cisco per la rete e la sicurezza</li><li>• Supporta un controllo degli accessi basati sul ruolo e un framework per approvare proposte ed integrazioni</li><li>• Offre opzioni flessibili di gestione dei dispositivi, tra cui la gestione "policy-based" e metodi per implementare modifiche alla configurazione</li></ul>	<ul style="list-style-type: none"><li>• I vendor SIEM che hanno ricevuto l'approvazione all'utilizzo dei prodotti Cisco vi permettono di rispondere alle vostre specifiche esigenze di sicurezza e reportistica e avere la certezza che le soluzioni saranno perfettamente interoperabili</li><li>• Le soluzioni sono accompagnate da manuali con consigli per l'implementazione e informazioni relative all'integrazione per un'amministrazione completa affinché tutti i prodotti dei partner tecnologici possano aiutare a rendere le vostre attività più veloci ed efficienti</li></ul>

### Perché Cisco?

Cisco ha un approccio completo e globale alla sicurezza. Integrando la protezione di rete in ogni componente della rete, Cisco semplifica il compito di soddisfare i moderni requisiti di protezione, indipendentemente dall'applicazione o dal servizio. La Cisco Secure Borderless Network unisce una eccellente threat intelligence, un portfolio di soluzioni flessibili, partner strategici e servizi che estendono la sicurezza alle persone, ai dispositivi e alle sedi che si desidera, permettendo alle aziende di costruire soluzioni che ne garantiscono la sicurezza e di raggiungere i loro obiettivi di business.

Per maggiori informazioni, visitare il sito [www.cisco.com/go/security](http://www.cisco.com/go/security).

