



White Paper di Websense®

# Protezione delle informazioni essenziali

Consolidare le fondamenta della piattaforma business di Internet

Internet può essere lo strumento più importante per la produttività aziendale. L'utilizzo libero di questa piattaforma di business, tuttavia, mette a repentaglio il patrimonio più delicato dell'azienda, ovvero le sue informazioni essenziali, che possono spaziare dalla proprietà intellettuale ai rendiconti finanziari, fino ai dati personali dei clienti e dei dipendenti.

I responsabili della sicurezza devono spostare il proprio focus della protezione dalla salvaguardia dell'infrastruttura dagli attacchi in ingresso, un modello adatto a confini perimetrali e a Internet come risorsa di contenuti, alla salvaguardia delle informazioni essenziali contro minacce a tecnica mista e perdite di dati accidentali o dolose, come richiede il Web 2.0 e Internet come piattaforma di business.

I requisiti per la sicurezza del Web, la protezione della posta elettronica e la prevenzione della perdita di dati sono cambiati. Per ulteriori informazioni al riguardo, leggere quanto segue:

- [Dove e perché i metodi tradizionali non funzionano](#)
- [Come l'accuratezza e il contesto influiscono sulla protezione efficace mirata alle informazioni](#)
- [Cosa fare per proteggere le informazioni essenziali e dire sì anziché bloccare i processi aziendali che si avvalgono di Web 2.0 e di Internet come piattaforma aziendale](#)

## Introduzione

Oggi Internet coinvolge ogni aspetto e risorsa dell'azienda. Le organizzazioni efficienti fanno sempre più affidamento su Internet come piattaforma di business, tramite software come servizio e applicazioni basate sul Web, luoghi di lavoro remoti e su una rete di partner. Questa piattaforma Web 2.0 consente vantaggi competitivi e offre Employee 2.0, il dipendente sempre connesso, ovunque e in qualsiasi momento.

A differenza di quanto accadeva nel passato, quando le aziende bloccavano il codice sorgente, la ricerca proprietaria, i documenti finanziari e le informazioni che consentono l'identificazione personale all'interno di server sicuri o in segmenti di rete isolati, le aziende di oggi lasciano che queste importanti informazioni fluiscano in modo relativamente libero entro e oltre i propri confini.

Per i responsabili della sicurezza, la piattaforma Internet è al contempo un amico e un nemico. Web 2.0 consente una collaborazione e uno scambio di informazioni senza precedenti, e le aziende che chiudono la porta alle opportunità offerte da Web 2.0 rischiano di perdere il proprio vantaggio competitivo. Web 2.0 introduce, tuttavia, una nuova tipologia di rischio, con minacce attivate da Internet che sfruttano le nuove tecnologie e vulnerabilità. Si tratta di minacce che non colpiscono più il nucleo o il margine esteso della rete, ma usano invece Web 2.0 e le comunicazioni convergenti per integrarsi in modo invisibile con le operazioni giornaliere.

Anche i rischi non vengono tutti da criminali o dall'esterno. L'apertura della piattaforma Internet ha aumentato il rischio proveniente dall'interno. Che si tratti di problemi di responsabilità con contenuto inappropriato, riduzione della produttività o perdita accidentale o dolosa di informazioni aziendali essenziali, i rischi attivati da Internet stanno costringendo i responsabili della sicurezza a occuparsi di problemi di sicurezza che non sono più così netti.

Per mantenere il passo con questi cambiamenti, è necessaria anche l'evoluzione della protezione della rete. Difese mirate alla rete o all'endpoint, basate su firme o comportamenti, metodi buoni o cattivi non sono sufficienti contro queste minacce. Quel che è peggio, queste minacce usano un modello "on o off" semplicistico che può danneggiare Internet come piattaforma aziendale. Nessuna azienda può semplicemente "disattivare" Internet. Internet è uno strumento di business che deve essere gestito e protetto in modo adeguato, come ogni altra risorsa importante dell'azienda. I responsabili della sicurezza devono essere propositivi verso le attuali possibilità di protezione dei dati e avere fiducia che le informazioni aziendali essenziali saranno protette in modo sicuro.

**400 MILIONI DI DOLLARI:** il valore dei segreti commerciali trafugati da uno scienziato DuPont per un rivale cinese<sup>1</sup>

## Protezione adeguata delle informazioni essenziali

L'applicazione di una protezione adeguata è critica e soggettiva. Ogni azienda deve proteggere le proprie informazioni sensibili e i flussi di lavoro in modalità adeguate al proprio ambiente, ai rischi e al tipo di rischi. Consideriamo le sfide e i problemi di oggi.

### È possibile identificare i dati sensibili e regolati e impedirne la perdita?

**La situazione:** I dati sono oggi la valuta di un'organizzazione. Vengono salvati, e si accede ad essi da database, archivi di documenti, condivisioni di file, file system di utenti finali e dispositivi di storage portatili. Vengono scambiati all'interno dell'organizzazione e condivisi esternamente con venditori, partner, utenti finali, consumatori, enti di governo e molte altre controparti.

**Il problema:** i dati vengono spesso salvati, usati e scambiati in modo inadeguato, e sono sempre più il bersaglio di attacchi e furti. La mancata protezione dei dati comporta rischi di non conformità, multe, procedimenti legali, perdita di vantaggio competitivo, danni al marchio e persino violazioni della sicurezza nazionale. Questi rischi sono aggravati dalla proliferazione di applicazioni e scambio di informazioni.

**La risposta di oggi:** gli strumenti tradizionali di prevenzione della perdita di dati si basano su semplicistici controlli "on o off" basata su una primitiva identificazione dei dati. Ad esempio, un'elementare "congettura" riguardo a corrispondenze di parole chiave può produrre falsi positivi o più corrispondenze che non costituiscono vere e proprie violazioni, ma che determinano blocchi sulla trasmissione o sull'acquisizione di file. Il blocco di dati in movimento o la rimozione di dati a riposo con questo approccio carico di falsi positivi porta letteralmente il flusso di dati e, per estensione, l'intera azienda a un arresto. Inoltre, queste soluzioni "on o off" solitamente non hanno il concetto del workflow o delle politiche aziendali e non sono in grado di adattarsi alle mutevoli esigenze dell'azienda.

Funzionari giapponesi, che non avrebbero mai dovuto avere dati di questo tipo sui propri sistemi, hanno scaricato dati segreti sul sistema di difesa missilistico Aegis DEGLI Stati Uniti in scambio di materiale pornografico.<sup>2</sup>

Un sondaggio dell'AMA ha rivelato che il 18 per cento delle aziende bloccano le visite dei dipendenti a blog esterni.<sup>3</sup>

Perché le aziende si preoccupano? Cisco è stata citata in giudizio a causa del blog esterno di un dipendente.<sup>4</sup>

### I responsabili IT possono dire sì ai blog?

**La situazione:** i blog sono un ottimo esempio Web 2.0 di scambio di informazioni e contenuti generati dagli utenti. I blog possono aiutare un'organizzazione finanziaria a scoprire aziende nelle quali investire, un'azienda multimediale a trovare idee per trame o una società che opera nel campo della tecnologia a cercare opportunità commerciali e promuovere la notorietà.

**Il problema:** lo scambio innocente di informazioni va bene, ma nessuna entità vuole che i propri utenti siano compromessi dalle vulnerabilità di un blog, portino contenuti inadeguati nell'organizzazione, perdano tempo, o ancora peggio, pubblichino dati sensibili dei clienti, nuove trame o proprietà intellettuale. Questi problemi chiamano in causa la responsabilità dell'organizzazione.

**La risposta di oggi:** secondo i metodi tradizionali di sicurezza dei contenuti e della rete l'unica risposta è interrompere la comunicazione con i blog o lasciarla attiva con la scomoda consapevolezza di un rischio sempre in agguato. Questa eccessiva risposta non corrisponde alle esigenze delle aziende che hanno invece bisogno di scambio di informazioni e strumenti moderni.

"Anche per le aziende che non temono la riduzione della produttività, la virulenza dell'ambiente delle minacce Web è tale da non poter essere ignorata." - Burton Group.<sup>5</sup>

<sup>2</sup> <http://www.infosecnews.org/hypermail/0704/13040.html>

<sup>3</sup> <http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/>

<sup>4</sup> <http://www.forbes.com/technology/forbes/2008/0407/044a.html>

<sup>5</sup> "Burton Group Security and Risk Management Strategies report, "Web Filtering: Completing the Evolution from Acceptable-Use to Serious Malware Defense," Jan. 1 08  
<http://www.burtongroup.com/Research/PublicDocument.aspx?cid=1185>

### Gli strumenti possono distinguere il Web 2.0 buono e quello cattivo?

**La situazione:** Web 2.0 è molto diverso dal mondo dei siti informativi in categorie di contenuto semplici. Web 2.0 usa la programmazione dinamica per generare pagine Web specifiche che presentano contenuti differenziati in base al momento, alla cronologia e agli attributi dell'utente. Questa rete non si limita affatto a sporadiche visite a MySpace, ma è costituito da siti commerciali, come Wikipedia, LinkedIn, YouTube e Google, che supportano la ricerca legittima e le operazioni aziendali.

**Il problema:** I cambiamenti nelle tecnologie Internet mettono i criminali in condizioni di mirare alle informazioni essenziali e favoriscono la divulgazione accidentale. Accanto a contenuti accettabili e "sicuri", i siti di Web 2.0 possono anche ospitare malware transitori e contenuti spinosi forniti dagli utenti non sottoposti ad alcun controllo e non regolamentati. Non esiste il pulsante "fare clic per accettare" per mettere in allarme gli utenti. Collegamenti danneggiati, widget dannosi e script incorporati introducono il malware nei contenuti e nelle pagine. Gli utenti che visitano siti benigni possono essere indirizzati a siti che esplorano il computer dell'utente alla ricerca di dati sensibili, password e vulnerabilità.

**La risposta di oggi:** le risposte di oggi si basano su concetti tradizionali di blocco basati su siti buoni o cattivi. Una risposta di questo tipo non tiene conto della mutevole vulnerabilità a livello di contenuti. La reputazione non è sufficiente per affrontare le minacce basate sui contenuti. Ad esempio, la reputazione di MySpace varia a seconda dei contenuti serviti su ciascuna pagina e quando i siti buoni come MSNBC vengono compromessi a livello di contenuto, la reputazione è irrilevante. Se questi contenuti non diventano parte di una comprensione granulare del sito nel suo complesso e della sua rispettiva classificazione, le soluzioni tradizionali agiscono con blocchi eccessivi o insufficienti e non sono in grado di consentire l'uso sicuro del Web per fini commerciali.

Tra i 26.000 siti compromessi dall'exploit di un motore di ricerca, MSNBC è stato colpito da hacking subito prima della trasmissione del campionato universitario di pallacanestro NCAA nel marzo 2008.<sup>6</sup>

L'incidenza sempre crescente delle minacce multi-canale sta plasmando il mercato della protezione dei contenuti e un approccio "a silos" per il filtraggio e-mail e Web offrirà una risposta inadeguata a tali minacce. – Forrester Research<sup>7</sup>

### Le soluzioni possono proteggere gli utenti e i dati dai diversi attacchi provenienti da Web 2.0 e posta elettronica?

**La situazione:** le applicazioni e-mail e Web sono diventate strettamente intrecciate in webmail e e-mail con contenuti HTTP. Questi canali di comunicazione servono anche altre applicazioni aziendali come ERP e CRM, soprattutto nei servizi hosted. Le comunicazioni convergenti semplificano i flussi di lavoro, riducono gli errori e consentono operazioni non-stop.

**Il problema:** Il crimine commerciale di oggi combina spam, email e applicazioni con tecniche multicanale. Una minaccia a tecnica mista in ingresso, ad esempio, utilizza la posta elettronica per indurre gli utenti a visitare URL contraffatti o anche URL noti compromessi con codice nocivo in grado di catturare password e-mail e installare software di key logging o Trojan. L'aspetto più dannoso è che questo può essere personalizzato in modo da rubare a individui e imprese dati specifici di elevato valore. Questi attacchi mirati spesso passano inosservati, soprattutto su siti di settori nicchia.

<sup>6</sup> <http://www.itbusiness.ca/it/client/en/Home/News.asp?id=47631>

<sup>7</sup> "Content Security Is Becoming A Competition Among Suites: Websense Rounds Out Its Security Portfolio With Its Acquisition Of SurfControl" by Chenxi Wang, Ph.D., December 2007, Forrester Research, Inc.

**La risposta di oggi:** la maggior parte delle aziende protegge ancora ogni canale e direzione di comunicazione con filtri indipendenti per e-mail in uscita e contenuti di dati, filtri in entrata di spam e virus e bloccando URL inappropriati e dannosi. Questi silos separati si concentrano sugli URL o sulle intestazioni e-mail, anziché su entrambi e raramente prestano attenzione ai dati stessi o ne bloccano dinamicamente la trasmissione in uscita. Si tratta di una reazione basata su un quadro cronologico delle minacce, creato sulla base di controlli, firme, reputazione e comportamento obsoleti. Le minacce a tecnica mista bypassano facilmente questi controlli con il morphing e spostandosi nel Web mentre rubano i dati.

**Marzo 2008: la grande catena di supermercati Hannaford Brothers è stata denunciata in seguito a intrusioni di rete che potrebbero avere compromesso 4,2 milioni di record relativi alle carte di credito.<sup>8</sup>**

Questi esempi illustrano la complessità e la difficoltà di proteggere la piattaforma Internet. Le soluzioni tradizionali si sono rivelate inadeguate, a giudicare da un sondaggio di IDC del 2008 sulle principali minacce alla sicurezza della rete. Con la perdita involontaria di dati per la prima volta in cima all'elenco, le principali preoccupazioni dei responsabili della sicurezza sono ora le seguenti:

1. Dipendenti che inavvertitamente rendono pubblici dati sensibili
2. Trojan, virus, worm e altro codice dannoso
3. Spam
4. Furti di dati da parte di dipendenti o partner commerciali
5. Hacker<sup>9</sup>

## Nuovi requisiti

Le difese della sicurezza devono spostare il punto focale della protezione dalla salvaguardia dell'infrastruttura dagli attacchi in ingresso, un modello adatto a confini perimetrali e a Internet come risorsa di contenuti, alla salvaguardia delle informazioni essenziali contro la fuoriuscita di dati, come richiede Web 2.0 e Internet come piattaforma di business. Anziché operare in silos, le protezioni devono collaborare attraverso canali applicativi, tecniche di controllo e prospettive d'uso. Tramite la collaborazione, gli strumenti possono esaminare in tempo reale sia il contenuto che il contesto per identificare con precisione e bloccare sofisticate minacce.

Per il successo a lungo termine, occorre soddisfare due gruppi: responsabili del rischio e utenti finali. I responsabili del rischio vogliono la visibilità e il controllo affidabile sulla perdita di dati. Gli utenti finali vogliono rimanere produttivi ed efficienti. Gli utenti finali non possono essere banalizzati. Utenti frustrati (o nocivi) spesso aggirano questi strumenti oppure impostano regole di blocco talmente blande da risultare irrilevanti. Con questi gruppi esigenti, le soluzioni devono essere efficaci e adatte sia alle minacce che ai requisiti aziendali.

## Una nuova formula protettiva = Accuratezza + Contesto

L'accuratezza e il contesto sono centrali per il successo. L'identificazione accurata richiede l'analisi approfondita di contenuti e dati, sia esternamente, su Internet, che internamente, attraverso la rete e i sistemi e i server aziendali. L'accuratezza va salvaguardata durante l'uso e la modifica dei dati e dei contenuti, sui siti Web e nelle applicazioni aziendali. Dato il ritmo del cambiamento dei contenuti (costante e istantaneo), l'identificazione accurata richiede notevoli risorse di elaborazione e ricerca, nonché la condivisione dei dati sulle minacce per individuare le minacce su più canali di comunicazione: "Lo spam contiene malware", " Su quel sito Web è presente uno spammer" o "Questi dati non possono essere pubblicati su quel blog o inviati tramite e-mail a quell'indirizzo".

Il contesto richiede che le soluzioni considerino più aspetti dell'utilizzo prima di passare all'azione. Anziché pensare ai canali di comunicazione - Si tratta di e-mail? Si tratta di un sito Web? - gli strumenti devono valutare il contenuto e i dati, nonché il contesto del loro utilizzo: Chi è l'utente? Di che tipo di dati si tratta? Quali sono i canali di comunicazione e le applicazioni utilizzati nel workflow? Questa prospettiva più ampia crea un sistema di protezione più articolato e accurato rispetto allo sledgehammer, o all'approccio tutto o niente del passato. L'inclusione del contesto rende rilevanti le valutazioni e dà un senso ai controlli.

Un aspetto chiave del contesto è Internet stesso. La destinazione Internet è valida oppure compromette la conformità alle normative, la sicurezza o le informazioni proprietarie? Questa comprensione contestuale combina le informazioni sul Web e sulle minacce per contrassegnare le destinazioni inappropriate o rischiose, esporre gli indirizzi di spam e rilevare le trasmissioni inopportune. Le organizzazioni possono prendere decisioni migliori riguardo al rischio di accesso o al rischio dello scambio di informazioni.

Applicando questi requisiti per l'identificazione accurata e risposte basate sul contesto, la tabella sottostante riepiloga le caratteristiche che segnano il passaggio da una struttura di sicurezza basata sull'infrastruttura a una basata sulle informazioni.

Requisiti delle soluzioni per proteggere e attivare le caratteristiche della piattaforma di Internet business

#### Characteristics

- Incorporare controlli su Web e e-mail e contro la perdita di dati per una copertura completa
- Ispezionare i flussi di dati di più canali in entrata e in uscita
- Combinare più tecniche di rilevamento, identificazione e classificazione
- Incorporare informazioni bidirezionali di utenti dati, canali e destinazioni Internet
- Offrire semplici meccanismi per implementare rapidamente policy accurate e ottenere visibilità, con la flessibilità necessaria per ottimizzare e aggiungere controlli e processi man mano che si approfondisce la conoscenza del rischio
- Nonostante la natura dinamica dei contenuti e dei dati, creare un'associazione stabile tra le policy e gli utenti, i dati, le destinazioni e i canali di comunicazione

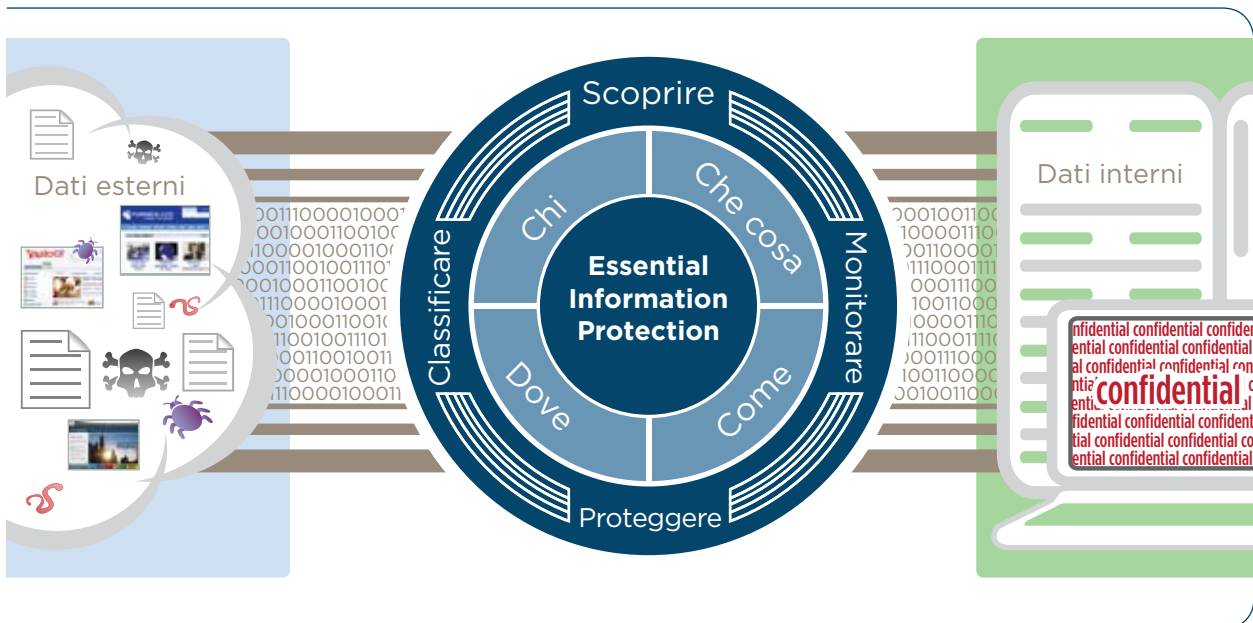
#### Esempi

- **Prevenzione della perdita di dati:** la soluzione deve essere in grado di identificare con precisione le informazioni nei dati a riposo in archivi e file system; dati in movimento all'interno e in uscita dall'organizzazione; e i dati in uso in applicazioni all'endpoint. La soluzione, inoltre, deve essere in grado di capire cosa i dati significano in termini di regolamenti, dati proprietari e policy interne, e consentire di adattare le policy ai processi aziendali. Nello stesso tempo, deve essere in grado di applicare policy coerenti e attivare flussi di lavoro che vanno dalla gestione degli incidenti, la risposta e la notifica automatica agli incidenti, il riepilogo e il reporting dettagliato.
- **Contenuti, informazioni e "user-aware blogging":** la soluzione deve capire la categoria del blog, essere in grado di identificare l'utente e identificare i dati in tempo reale, con un'accuratezza sufficiente per bloccare la pubblicazione di informazioni troppo private. Grazie alla corretta classificazione del sito host, della sua reputazione e del contenuto reale di un blog, la soluzione deve impedire la compromissione di utenti e sistemi o l'accesso inopportuno al blog.
- **Minacce Web 2.0:** la soluzione deve essere in grado di capire i siti Web, i contenuti Web, le applicazioni e il malware oltre la sola reputazione, considerando l'uso e il contesto Internet per una valutazione dei rischi in tempo reale. Solo con questo livello di comprensione è possibile bloccare le minacce con accuratezza e in tempo reale. Sarebbe possibile prevenire la minaccia anche nel caso in cui fosse compromesso un sito noto e con una buona reputazione.
- **Minacce per Web e posta elettronica:** una soluzione deve essere in grado di identificare i collegamenti in una e-mail e risalire ai siti o ai contenuti dannosi. In base a questa identificazione accurata, le soluzioni devono essere in grado di agire in tempo reale per bloccare la posta elettronica e qualsiasi altro tentativo di accedere a quel sito Web, visualizzare i contenuti e trasmettere i dati a quella destinazione.

## Dire sì con Essential Information Protection™

Websense® integra sicurezza Web, sicurezza della posta elettronica e sicurezza dei dati per proteggere le informazioni essenziali e promuovere l'uso sicuro e produttivo della piattaforma Internet. Websense Essential Information Protection difende le comunicazioni multicanale, salvaguarda l'uso di Web 2.0 e previene la perdita di dati. Essential Information Protection utilizza ThreatSeeker™ Network, un'infrastruttura avanzata atta a rilevare tempestivamente le minacce sui canali e-mail e Web e identificare e bloccare in tempo reale i siti Web ad alto rischio, e dotata di tecniche e tecnologie per l'identificazione dei dati. ThreatSeeker Network fornisce i necessari sistemi di protezione alle soluzioni Websense di sicurezza per Internet, posta elettronica e dati, al fine di offrire il più aggiornato livello di protezione da perdite di dati, contenuti indesiderati e minacce informatiche.

ThreatSeeker Network combina euristica, analisi binaria, reputazione, analisi delle immagini, analisi lessicale, rilevazione di modelli, analisi statistica, elaborazione del linguaggio naturale, fingerprinting dei dati ed esperti di ricerca in diverse discipline. Queste tecniche e capacità strettamente interconnesse identificano e classificano i dati e i contenuti all'interno dell'azienda e su Internet per promuovere la comprensione delle nuove minacce al loro nascere.



Websense Essential Information Protection classifica le minacce esterne ed esegue il monitoraggio dell'utilizzo dei dati interni per impedire la perdita di informazioni regolamentate e riservate.

Le soluzioni Websense sfruttano questa precisa classificazione e il contesto Internet per gestire la sicurezza e l'uso corretto del Web, la sicurezza e la conformità della posta elettronica e la prevenzione della perdita di dati. Queste soluzioni si combinano per andare oltre la sicurezza tradizionale e prevenire le minacce a tecnica mista che travalicano i vettori di rischio in entrata e in uscita e mettono a repentaglio le informazioni essenziali. Grazie all'integrazione diretta di prodotto e in combinazione con la ricerca di ThreatSeeker Network, questa suite di prodotti considera l'intera gamma dei componenti rilevanti: l'utente, i dati, i canali di comunicazione e la destinazione Internet.

Con questo approccio, Websense è unico nell'identificazione e nella gestione accurata e istantanea dei seguenti elementi:

- **Chi** è autorizzato ad accedere in tempo reale a specifici siti Web, contenuti sensibili o applicazioni
- **Quali dati** rivestono un'importanza fondamentale per l'organizzazione e devono essere protetti da fughe accidentali o intenzionali
- **In che modo** gli utenti possono comunicare i dati sensibili e in che modo l'organizzazione può utilizzare le risorse online in modo più sicuro e produttivo
- **Quali siti** gli utenti sono autorizzati a visitare e dove possono essere inviati i dati sensibili senza rischi di sicurezza

Le soluzioni Websense integrate per il Web, la posta elettronica e la sicurezza dei dati garantiscono alle organizzazioni sicurezza ed efficienza. Websense rappresenta la rete di sicurezza nella quale i dipendenti possono rimanere produttivi su qualsiasi rete, in qualsiasi momento e ovunque. I responsabili del rischio riducono la responsabilità legale, applicano policy di conformità, impediscono la perdita di dati e acquistano visibilità nelle proprie attività in vista di rischi in continua trasformazione. Grazie a tecniche di ricerca avanzate ed efficaci controlli integrati, Websense Essential Information Protection offre una combinazione unica di intelligenze per Web, contenuti e utenti volta a contrastare le minacce al loro manifestarsi, aiutare le aziende a realizzare il pieno potenziale della piattaforma Internet per il business e consentire ai responsabili della sicurezza di dire sì alle nuove tecnologie e capacità.

## Riassumendo

Sebbene Internet rappresenti ormai uno strumento di importanza strategica, il suo utilizzo mette a repentaglio le informazioni aziendali essenziali, quali formule proprietarie, codice sorgente, piani commerciali, elenchi di clienti e così via. Le minacce convergenti veicolate dalla posta elettronica e da Internet, e alimentate dalle tecnologie Web 2.0, si avvalgono ora di manovre clandestine per eludere i sistemi di protezione tradizionali.

Per assicurarsi che le procedure di attenuazione del rischio tengano il passo con le minacce, le aziende devono rielaborare le proprie strategie riguardo a Internet, posta elettronica e sicurezza dei dati. Le aziende dovrebbero concentrare la loro attenzione non sulle tecnologie, ma sui dati. Questi ultimi sono l'elemento più rilevante. Come vengono utilizzati? Chi li usa? Dove e quando è sicuro usarli? Chi può riceverli? Attraverso quali canali possono essere inviati in sicurezza?

Questa prospettiva orientata ai dati significa che, anziché investire in silos di protezione con copertura limitata, le aziende uniranno le difese nelle tecnologie, canali di comunicazione e applicazioni attraverso cui i dati vengono trasportati e utilizzati. Questa integrazione aumenta l'accuratezza della rilevazione e della qualità della risposta. Anziché limitarsi all'applicazione proattiva, questa integrazione garantisce una protezione adeguata perché consente di usare il contesto per capire gli usi di business legittimi e adattare le risposte. Con la protezione dei dati sensibili, informazioni essenziali di ogni azienda, le organizzazioni possono sfruttare e difendere la piattaforma di business Internet.

## Informazioni su Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), leader mondiale nelle tecnologie di protezione integrata per Web, posta elettronica e dati, fornisce Essential Information Protection a più di 42 milioni di dipendenti in oltre 50.000 organizzazioni in tutto il mondo. Distribuite attraverso la rete globale di partner di canale, le soluzioni software e hosted di Websense aiutano le aziende a bloccare i codici maligni, prevenire la perdita di informazioni confidenziali e applicare le policy di utilizzo di Internet e di sicurezza. Per ulteriori informazioni, visitare il sito [www.websense.com](http://www.websense.com) e

- **Effettuare la registrazione per ricevere avvisi di sicurezza e rapporti sulle minacce:**  
<http://www.websense.com/securitylabs/>
- **Visualizzare informazioni sulle soluzioni e materiali didattici di supporto**  
<http://www.websense.com/global/en/ProductsServices/>
- **Scaricare whitepaper e case study e partecipare a sessioni webcast**  
<http://www.websense.com/global/en/ResourceCenter/>
- **Valutare le soluzioni**  
<http://www.websense.com/global/en/Downloads/>
- **Individuare e contattare un rivenditore Websense**  
<http://www.websense.com/global/en/Partners/Channel/FindPartner/>