KASPERSKY lab

# CYBERSECURITY PER L'AZIENDA: CALCOLARE I COSTI, TROVARE IL VALORE

*Le aziende hanno sempre cercato di spremere al massimo le loro risorse IT per ottenere i maggiori vantaggi possibili al costo minore, ma calcolare il ROI non è così semplice.*

# INTRODUZIONE

Quando si verifica una violazione, ogni secondo è importante e rappresenta un costo. Ma poche aziende comprendono il ruolo del ROI per la loro cybersecurity. Come può l'azienda trovare il valore? E se bilanciare i vari profitti potesse consentire all'azienda di concentrarsi sulle soluzioni di cybersecurity più adatte alle sue esigenze e, nel frattempo, ottenere il massimo dall'investimento?

La soluzione di cybersecurity implementata dall'azienda influisce sul ROI:

**Classica/ tradizionale:** la maggior parte in loco, supportata da ampi team di amministrazione nelle aziende di dimensioni più grandi.

**Soluzione cloud:** gestita tramite strumenti e console basata su cloud, senza la necessità di hardware aggiuntivo.

**Appaltata:** in cui un fornitore di servizi di terze parti esterno (un MSP) si occupa di tutte le attività.

Ogni soluzione offre vantaggi specifici e influisce sul budget in modo diverso, ma per le aziende con risorse limitate in sede, o che preferiscono appaltare la gestione a terzi, la cybersecurity basata su cloud rappresenta la soluzione migliore, poiché assicura sia facilità di gestione sia convenienza in termini di costi.

# QUANDO MENO RISORSE DEVONO FORNIRE PIÙ RISULTATI

**"Fare di più con meno" è stato il mantra aziendale degli ultimi anni, ma non rappresenta certo una novità per il personale IT.** Le aziende hanno sempre cercato di spremere al massimo le loro risorse IT per ottenere i maggiori vantaggi possibili al costo minore: la vera sfida per il personale IT di oggi è tenere testa alla complessità contando su risorse limitate.

E quando si tratta di cybersecurity, le aziende di tutte le dimensioni lottano per restare al passo delle minacce in continua evoluzione, mantenendo al tempo stesso il controllo su una gamma sempre più ampia di hardware, dispositivi, applicazioni e utenti finali.

Già nel 2013, PriceWaterhouseCooper aveva segnalato un calo delle assunzioni del personale di cybersecurity; nello stesso periodo, secondo lo studio di Kaspersky Lab il 58% delle aziende affermava che la loro sicurezza IT non disponeva di risorse sufficienti in almeno un'area: personale, sistemi o competenze. Andiamo avanti e arriviamo al T4 del 2016, momento in cui le imprese rilevano una carenza di competenze informatiche e ampliano i propri budget per sopperirla.

Ma non si parla solo di competenze: il 40% delle aziende indica l'aumento della complessità dell'infrastruttura come elemento chiave dei propri budget di cybersecurity. È interessante notare che nessuno sembra aver compreso il ruolo del ROI per la cybersecurity: il 62% delle grandi imprese e il 59% delle PMI affermano che continueranno a investire, indipendentemente dalla loro capacità di calcolare il ROI.

**In che modo le aziende possono esaminare il ROI per la cybersecurity? E se bilanciare i vari profitti potesse consentire all'azienda di concentrarsi sulle soluzioni di cybersecurity più adatte alle sue esigenze e, nel frattempo, ottenere il massimo dall'investimento?**

# DETTAGLI PRATICI DELLA CYBERSECURITY

**Essenzialmente, per gestire i costi della cybersecurity e ottenere il ROI, è necessario esaminare tre aree chiave connesse:** CAPEX, OPEX e risorse umane. In parole povere, facciamo riferimento al kit di cui l'azienda ha bisogno, a quanto costerà gestirlo e a dove trovare le persone in grado di monitorare entrambi questi due elementi.

## INIZIAMO DAL CAPEX:

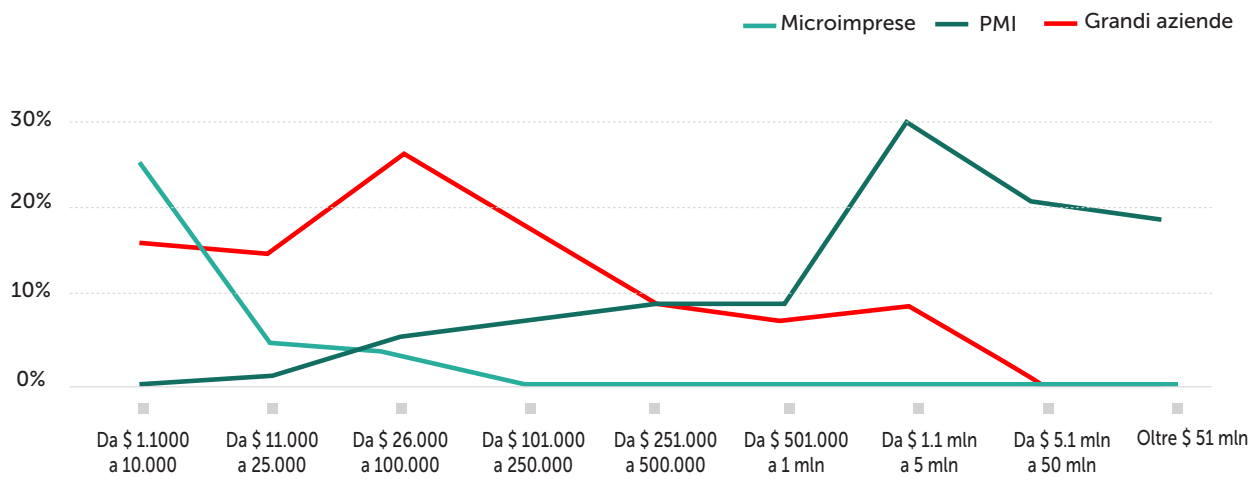
I CISO o i manager della cybersecurity saranno lieti di sapere che i loro budget aumenteranno, con l'approvazione dell'alta dirigenza: il 38% delle grandi imprese e il 33% delle PMI affermano che la dirigenza sta chiedendo loro di aumentare gli investimenti per la cybersecurity.

L'altra faccia della medaglia, naturalmente, è che le aspettative in termini di risultati sono superiori. Uno svantaggio dell'aumento degli investimenti nella cybersecurity può essere la complessità: più hardware, più dispositivi, più applicazioni. Tutto deve essere integrato, gestito e monitorato. È assodato che per ogni aumento del 25% in termini di funzionalità si rileva un aumento del 100% della complessità. Il 55% delle PMI indica come sfida chiave il crescente volume di dispositivi di cui necessita.

### Chi gestirà tutti questi elementi?

E qui arriviamo a parlare di OPEX e risorse umane, entrambi aspetti riguardanti le competenze...

## Budget di sicurezza IT




*Percentuali delle aziende il cui budget per la sicurezza IT rientra in ogni intervallo.*

# IL FATTORE UMANO: CALCOLARE I COSTI DI UNA CARENZA DI COMPETENZE DELLA CYBERSECURITY

**Nonostante più della metà (il 54%) delle piccole e medie imprese creda che a un certo punto la loro sicurezza IT sarà compromessa**, e comprenda il ruolo fondamentale della preparazione la prevenzione e l'individuazione delle minacce, il 40% afferma di non disporre di intelligence o informazioni dettagliate sufficienti sulle minacce che si trovano a dover affrontare.

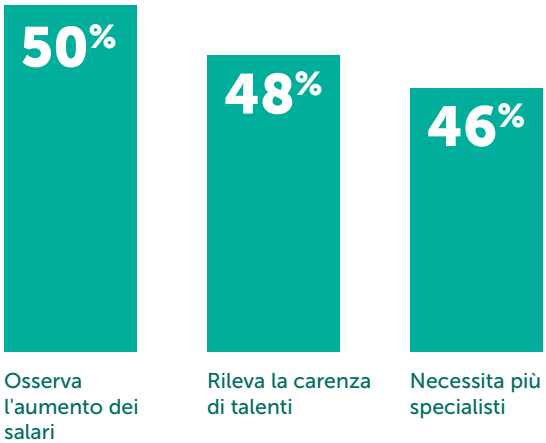
Se consideriamo che il team IT di una PMI media di 16 persone dispone di soli due esperti di sicurezza, è facile comprendere perché le risorse umane ricoprano un ruolo tanto importante nella pianificazione della cybersecurity, così come qualsiasi tecnologia o infrastruttura. Non c'è da stupirsi se più di un terzo delle aziende di tutto il mondo ritiene che il miglioramento delle competenze degli specialisti sia uno dei principali tre elementi dell'investimento della cybersecurity. Metà delle aziende afferma inoltre di rilevare una carenza di talenti.

La preoccupazione principale? Nello studio viene indicata una linea netta tra la disponibilità di talenti e il costo di ripristino da una violazione: le aziende che faticano a trovare migliori talenti per la sicurezza spendono in media tre volte di più per riprendersi da una violazione; una notevole spesa per il ripristino per le PMI si presenta sotto forma di un aumento dei salari del personale (in media $ 14.000).

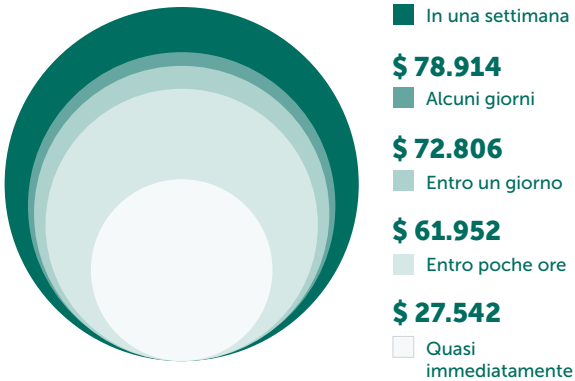
Il detto "il tempo è denaro" è perfetto per la cybersecurity: quando si verifica una violazione, ogni secondo è importante e rappresenta un costo. Una violazione rilevata quasi immediatamente costa alla PMI in media $ 28.000, arrivando fino a $ 105.000 se passa inosservata per più di una settimana. Secondo i dati effettivi, viene compromessa una media di 417 record, anche con il rilevamento istantaneo. Questa cifra sale a oltre 70.000 quando la violazione passa inosservata per più di una settimana.

**Vantaggi:** le risorse umane hanno la stessa importanza delle risorse tecnologiche nella lotta alle cyberminacce. L'importante è il modo in cui si trova l'equilibrio perfetto per l'azienda.

## Il fattore umano




## Il tempo è denaro



# CAVALLI DA CORSA: IN CHE MODO LA SOLUZIONE DI CYBERSECURITY IMPLEMENTATA DALL'AZIENDA INFLUISCE SUL ROI

**L'azienda può scegliere tra tre principali opzioni per la propria soluzione di cybersecurity:**

**Classica/ tradizionale**
La maggior parte in loco, supportata da ampi team di amministrazione nelle aziende di dimensioni più grandi.

**Soluzione cloud**
Gestita tramite strumenti e console basata su cloud, senza la necessità di hardware aggiuntivo.

**Appaltata**
In cui un fornitore di servizi di terze parti esterno (un MSP) si occupa di tutte le attività.

Ciascuna offre vantaggi specifici e influisce sul budget in modo diverso.

## SICUREZZA TRADIZIONALE IN LOCO:

L'approccio classico è il programma di cybersecurity originale fai da te. I team interni responsabili della tecnologia, i responsabili delle decisioni aziendali e finanziarie scelgono la soluzione ,o le soluzioni, più adatte alle esigenze dell'azienda, incluse le risorse hardware per supportarla, e gestiscono tutte le attività internamente da sé. Un aspetto positivo sta nel fatto che disporre di tutti gli elementi internamente assicura il massimo controllo sulla sicurezza, tuttavia l'aspetto negativo è che sono necessarie risorse e competenze in sede per sfruttarne tutti i vantaggi.
Le aziende che scelgono di utilizzare diversi fornitori per i diversi componenti della loro sicurezza avranno anche il duplice problema di complessità e integrazione, comportando ulteriori requisiti per le competenze interne. Le organizzazioni che utilizzano gli approcci tradizionali alla cybersecurity possono ridurre i costi, preferendo soluzioni che offrono console centralizzate, migliori funzionalità di automazione e gestione dei sistemi, oltre alla possibilità di proteggere e controllare vari dispositivi. Verrà ridotto il tempo che il personale amministrativo dedica alle attività quotidiane, ma sarà comunque necessario verificare di disporre delle competenze necessarie affinché tutto funzioni correttamente.

| **COSTI TIPICI ($)*** *Costi approssimativi con due uffici e 100 endpoint in totale* | **COSTI ANNUALI ($)** |
|---|---|
| Uffici connessi tramite una rete | |
| Risorse amministrative per la sicurezza IT: $ 4.000 al mese | **48.000** |
| Hardware: almeno $ 3.000 | **costi "una tantum"** |
| Software di cybersecurity: € 4.614 (circa $ 4.800) per la licenza di un anno | **4.800** |
| Formazione delle competenze in sede: $ 1.500 all'anno | **1.500** |
| **COSTI ANNUALI TOTALI** | **54.300** |
| **COSTI ANNUALI "UNA TANTUM"** | **3.000** |

**I costi sono approssimativi e solo a scopo informativo. I costi per situazioni aziendali specifiche potrebbero differire da quelli qui indicati.*

## SICUREZZA BASATA SU CLOUD:

**Con circa due terzi delle PMI che già utilizza una media di tre soluzioni cloud, non sorprende che la sicurezza basata su cloud sia una delle opzioni disponibili in più rapida crescita.** Il basso costo di accesso, la facilità di gestione e le flessibili opzioni di licensing flessibili sono elementi perfetti per le PMI che mirano a una scalabilità on demand, in qualsiasi direzione.

Ciò che rende la sicurezza basata su cloud particolarmente interessante sul fronte del budget, è che è molto rapida da implementare, facile da eseguire e senza investimenti hardware aggiuntivi. Dato che tutte le infrastrutture necessarie sono ospitate dal fornitore nel cloud, i clienti non devono acquistare o mantenere un server (o una licenza per esso) per la loro console di gestione. Questo consente alle aziende più piccole di utilizzare soluzioni di sicurezza all'avanguardia senza dover assumere personale qualificato o disporre di hardware di fascia alta per la gestione. Per le PMI impegnate nella crescita delle competenze per proteggersi da minacce sempre più sofisticate, si tratta di uno scenario vincente.

Una delle motivazioni chiave a supporto, è che la console basata su cloud consente la gestione di più endpoint, dispositivi mobili e file server in remoto, da qualsiasi posizione. Di solito è pronta all'uso e altamente intuitiva, ciò significa che gli amministratori IT senza competenze specializzate sulla sicurezza possono facilmente utilizzare le funzioni di sicurezza di fascia alta. I criteri di sicurezza predefiniti, sviluppati da analisti della cybersecurity qualificati, offrono intelligence e best practice in sede, senza dover effettuare nuove assunzioni o formare i dipendenti esistenti per utilizzare la nuova console cloud. Tutto è intuitivo e pronto per l'esecuzione.

Poiché tutto è centralizzato, gli amministratori della soluzione basata su cloud possono controllare lo stato di protezione di un massimo di 1000 nodi aziendali da qualsiasi dispositivo online e da qualsiasi posizione. La creazione di rapporti e il monitoraggio delle licenze viene gestito facilmente attraverso una semplice e intuitiva interfaccia. Si dispone così della migliore sicurezza, ottenendo il meglio dal personale attuale.

| **COSTI TIPICI ($)*** *Costi approssimativi con due uffici e 100 endpoint in totale* | **COSTI ANNUALI ($)** |
|---|---|
| Nessuna necessità di connettere gli uffici tramite una rete | |
| Risorse amministrative: $ 2.000 al mese | **24.000** |
| Costo della licenza: € 200 (circa $ 208) al mese | **2.500** |
| Competenze base in sede richieste: $ 700 all'anno | **700** |
| **COSTI ANNUALI TOTALI** | **27.200** |
| **COSTI ANNUALI "UNA TANTUM"** | **0** |

**I costi sono approssimativi e solo a scopo informativo. I costi per situazioni aziendali specifiche potrebbero differire da quelli qui indicati.*

## ORIENTARSI VERSO L'APPALTO A UN MSP

Questa opzione fa salire la sicurezza basata su cloud a un livello superiore. Invece di una persona interna che utilizza la console basata su cloud, un'azienda può appaltare la gestione a terzi esperti che non hanno bisogno di essere in loco per mantenerne il controllo. È possibile ottenere tutti i vantaggi di una soluzione leader di sicurezza senza mettere a dura prova i bilanci. Non c'è da stupirsi se il 40% delle PMI e il 26% delle aziende molto piccole affermano di pensare che un MSP potrebbe essere la risposta alle loro esigenze di sicurezza. Quasi un quarto delle PMI ha intenzione di adottare questo approccio alla sicurezza nei prossimi 12 mesi.

Il vero vantaggio dell'appalto a un MSP per la sicurezza è che le aziende di qualsiasi dimensione ottengono accesso ai migliori talenti per la sicurezza senza investimenti o necessità di competenze per la gestione. Le PMI potrebbero implementare opzioni di livello enterprise senza dover pensare al budget. E dato che l'MSP dispone di competenze interne, l'azienda può risparmiare sui costi e sulla comprensione della security intelligence e della threat intelligence in tempo reale. Come con le soluzioni basate su cloud, l'opzione MSP offre grande flessibilità. Dato che il fornitore del software è in esecuzione nell'infrastruttura, di solito è molto facile per l'MSP soddisfare la flessibilità stagionale o altri requisiti di scalabilità. In questo modo si risparmiano preoccupazioni legate alla gestione e al budget di abbonamenti e licenze.

| COSTI TIPICI ($)* | COSTI ANNUALI ($) |
|---|---|
| *Costi approssimativi con due uffici e 100 endpoint in totale* | |
| Nessuna necessità di connettere gli uffici tramite una rete, ma richiesta una distanza ragionevole dal partner MSP. | |
| Tutto l'IT: $ 3.000 al mese | **36.000** |
| Nessuna competenza in sede richiesta | **0** |
| **COSTI ANNUALI TOTALI** | **36.000** |
| **COSTI ANNUALI "UNA TANTUM"** | **0** |

**I costi sono approssimativi e solo a scopo informativo. I costi per situazioni aziendali specifiche potrebbero differire da quelli qui indicati.*

# PENSARE IN MODO DIVERSO PER MASSIMIZZARE IL VALORE

**La complessità rappresenta una minaccia per la sicurezza, l'efficienza e la crescita.** Crea spazio per gli errori e limita la capacità di gestire il cambiamento. Il personale IT è fin troppo consapevole di questi problemi. Ma cosa si può fare per mitigarli senza limitare le necessità degli utenti finali o sovraccaricare risorse già gravate?

Esplorando le varie opzioni per la cybersecurity in precedenza non prese in considerazione, ad esempio quelle basate su cloud o l'MSP, si potrebbe aumentare il ROI che si ottiene dalla sicurezza. Grazie alla sicurezza basata su cloud o appaltata sarà possibile ridurre il tempo di amministrazione IT e la necessità di competenze interne o di nuovo hardware. In alternativa, l'azienda può preferire un'opzione tradizionale con una soluzione in loco, ma che offra controlli centralizzati e il tipo di funzioni avanzate per la gestione del sistema che consentono di ottenere il meglio dalle risorse umane e dell'infrastruttura.

Essere preparati prima che si verifichino problemi è sempre stato il piano migliore. Se l'azienda non trova o non può permettersi ulteriori talenti, può rivelarsi un'ottima idea semplificare il lavoro del personale esistente per massimizzarne le capacità. Se non è possibile mettere in pratica questa strategia, perché non orientarsi verso l'appalto? Tutto dipende da cosa si intende fare per massimizzare il valore. Ma grazie alle opzioni offerte da Kaspersky Lab, quando si tratta di cybersecurity efficace, l'azienda non deve fare alcuno sforzo.

# L'AZIENDA È PRONTA A SCEGLIERE LA SUA ARMA PER LA CYBERSECURITY?

**Se l'azienda non è sicura dell'approccio alla cybersecurity più adatto alle sue esigenze, è il momento di mettere alla prova la teoria...**

È possibile scaricare la prova gratuita di **Kaspersky Endpoint Security for Business** e scoprire in che modo la crittografia e gli efficienti controlli intuitivi, oltre alle funzioni avanzate di gestione del sistema possono proteggere l'azienda anche dalle minacce più avanzate.

L'azienda cerca la facilità di utilizzo offerta dal cloud? È possibile registrarsi per la prova gratuita di **Kaspersky Endpoint Security Cloud** e scoprire in prima persona in che modo ridurre i costi e i sovraccarichi di risorse gestendo più endpoint, dispositivi e file server in remoto, da qualsiasi posizione.

Appaltare a un esperto di terze parti? **Per informazioni, basta visitare la pagina sugli MSP di Kaspersky Lab.**

*Sito Web globale di Kaspersky Lab*

*Blog B2B di Kaspersky Lab*