I PROBLEMI DELLA SICUREZZA AZIENDALE ALLA LUCE DELLE NUOVE NORME

Quanto è connessa la vostra sicurezza ?

A causa dei molti, improvvisi cambiamenti avvenuti quest'anno, le difficoltà affrontate dai professionisti della sicurezza per proteggere adeguatamente le proprie reti sono state ulteriormente amplificate.

97%

ammette che la propria organizzazione incontra seri problemi nel tentativo di proteggere la rete

(88% in Italia)

La rete è il cuore pulsante dell'organizzazione, che definisce il modo in cui opera e innova lungo il percorso di trasformazione digitale. I progressi sono però limitati dai problemi di affidabilità e performance

86%

sostiene la necessità di migliorare affidabilità e prestazioni della rete in tutta l'organizzazione

Di conseguenza la capacità di innovazione dei team IT è fortemente ridotta.

del tempo del personale IT è dedicato all'ordinaria gestione anziché all'innovazione

(47% in Italia)

La capacità di mitigare le minacce può essere limitata dalla mancanza di tempo dei team dedicati alla sicurezza IT. La visibilità in tempo reale su rete e dati è fondamentale.

87%

desidera una soluzione di sicurezza capace di migliorare le applicazioni esistenti, con una riduzione dei falsi positivi e minori tempi di risposta

(84% in Italia)

Tuttavia alcune organizzazioni ancora considerano la sicurezza IT come un costo necessario anziché un importante elemento di differenziazione, ciò che ha comportato una spesa significativa negli ultimi 12 mesi per mitigare le violazioni.

63%

ritiene che la propria organizzazione consideri la sicurezza IT un costo più che un valore aggiunto

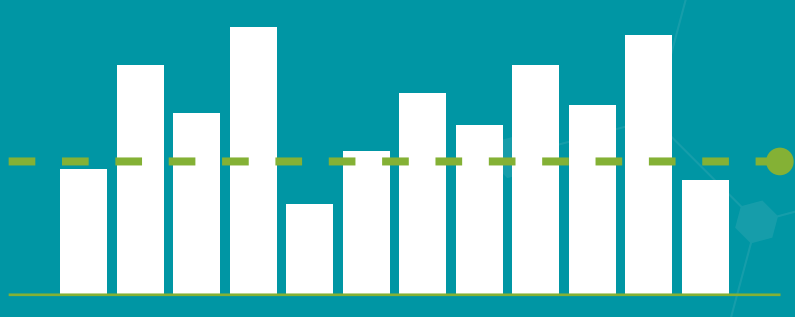
(34% in Italia)

97%

afferma che negli ultimi 12 mesi la propria organizzazione ha speso denaro per porre rimedio alle violazioni

(96% in Italia)

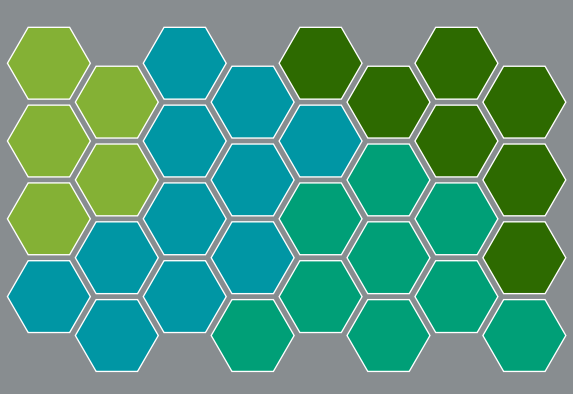
Spesa media per reazione/correzione delle violazioni negli ultimi 12 mesi



US$276,099

US$ 249.368 in Italia

Per affrontare il problema e districarsi tra i necessari periodi di test, le organizzazioni adottano un ventaglio di fornitori e soluzioni tecnologiche.



95%

afferma che la propria organizzazione lavora con diversi fornitori di tecnologia per la creazione dell'ambiente di sicurezza di rete

(93% in Italia)

Componenti critici della sicurezza sono la visibilità e l'applicazione delle policy. Oltre alle difese perimetrali, una rete realmente *Threat Aware* ha la capacità di applicare la sicurezza in ogni punto, dai router agli switch, nel cloud e su tutti i link che tengono insieme l'organizzazione.

99%

conviene che una Threat-Aware Network avrebbe un impatto positivo sull'organizzazione

(100% in Italia)

JUNIPER® NETWORKS

In una recente indagine indipendente commissionata da Juniper sono stati intervistati mille professionisti IT e della sicurezza in nove Paesi (Francia, Germania, Israele, Italia, Paesi Bassi, Regno Unito, Stati Uniti, Arabia Saudita, Emirati Arabi Uniti) di aziende con 1000 dipendenti e oltre, appartenenti a diversi settori, tra cui istruzione, servizi finanziari, PA, servizi sanitari, IT e telecomunicazioni, industria manifatturiera, media, tempo libero e intrattenimento, retail, trasporti e servizi pubblici/energia.

www.juniper.net