WHITE PAPER

Bitdefender

MSP

La guida definitiva ai test indipendenti di EDR e AV

COME UTILIZZARE LA RICERCA DI TERZE PARTI PER SCEGLIERE LA PROTEZIONE MIGLIORE

www.bitdefender.it

Tra la gestione della propria attività o la necessità di coordinare un piccolo team di professionisti IT, non resta molto tempo per altro. È difficile restare al passo con i cambiamenti, le evoluzioni e gli sviluppi che avvengono ogni giorno nella sicurezza informatica. Devi occuparti dei clienti, gestire l'impiego dei dispositivi e cercare la prossima innovazione per promuovere la tua azienda sul mercato! Quindi, come puoi assicurarti di aver implementato la giusta piattaforma di sicurezza per la tua azienda?

Ti rivolgi agli esperti, analisti indipendenti di terze parti che hanno un'esperienza reale per comprendere e valutare le varie opzioni di sicurezza informatica. In questa breve guida, condivideremo una breve storia dei test indipendenti sulla sicurezza informatica, mostrando alcuni dei migliori analisti sul mercato e contribuendo a sfatare alcuni luoghi comuni su questi educatori tecnologici essenziali.

TUTTI I PRINCIPALI AUTORI DI AV DI NUOVA GENERAZIONE DEVONO CONFRONTARSI CON LE STESSE CONDIZIONI NEI TEST INDIPENDENTI.

I criminali informatici stanno bypassando le soluzioni AV che si basano sulle firme per identificare le minacce. Tramite l'esplosione di nuovi malware, l'aumento di attacchi privi di file e la mercificazione di strumenti avanzati di attacco, stanno cambiando le regole del gioco. Le soluzioni AV di nuova generazione esistono proprio per questa necessità di avere tecnologie comportamentali e di intelligenza artificiale basate su cloud in grado di rilevare tali minacce sconosciute.

Ma, ovviamente, inquadrare la scelta di un antivirus facendo solo un confronto tra quelli basati sulle firme e quelli dotati di IA è un presupposto errato. Molti fornitori affermati hanno perfezionato l'IA, sfruttandola con successo insieme ad altre tecnologie più tradizionali. Invece, la domanda dovrebbe essere: come si confrontano i fornitori più recenti con quelli più affermati? Anche se molti fornitori più recenti hanno esitato a partecipare ai test pubblici, la necessità vitale di stabilire prove oggettive della propria efficacia è stata evidenziata dai principali analisti del settore. Il 2017 Gartner Magic Quadrant for Endpoint Protection Platforms ha rilevato: "I test standardizzati, come quelli di AV-Comparatives e AV-Test, sono ancora i migliori indicatori dell'efficacia."

Attualmente, i fornitori di sicurezza per endpoint devono partecipare a test indipendenti per essere considerati strumenti seri a livello aziendale. Per esempio, Gartner include la partecipazione ai test indipendenti come requisito essenziale per l'inserimento nel suo Magic Quadrant for Endpoint Protection Platforms:

"Il prodotto EPP aziendale del fornitore deve aver partecipato a test indipendenti, di natura pubblica e noti per l'accuratezza e l'efficacia, entro i 12 mesi precedenti il 30 giugno 2019, o essere un attuale partecipante all'interfaccia pubblica VirusTotal. Ne sono un esempio MITRE ATT&CK Evaluations, Virus Bulletin, AV-TEST, AV-Comparatives, NSS Labs e SE Labs."[1]

1 Gartner, Magic Quadrant for Endpoint Protection Platforms, agosto 2019

Quindi, in cosa consiste esattamente un test di sicurezza informatica indipendente?

Con il costo medio di una violazione dei dati che ha raggiunto ormai la cifra di 3,86 milioni di dollari, e il costo di una "violazione seria" (un milione di dati danneggiati) che è aumentato di cento volte, la sicurezza informatica non è qualcosa su cui nessuno può permettersi di scommettere. E con un tempo medio per identificare e contenere una violazione di circa 280 giorni, il conto alla rovescia per il proprio rischio di un'esposizione forse è già iniziato.[2]

Anche se probabilmente sei già consapevole della posta in gioco, spesso non è facile capire come si confrontano le decine di piattaforme disponibili sul mercato, o addirittura come si comportano rispetto alle loro promesse. Devi avere la CERTEZZA che il tuo investimento funzionerà. Ed è improbabile che tu abbia il tempo, l'esperienza e la tolleranza al rischio per introdurre una minaccia reale nel tuo sistema per condurre test approfonditi e oggettivi.

Per fortuna, diverse organizzazioni imparziali di terze parti hanno cercato di colmare questa lacuna. Alcune sono operative da oltre un decennio, mentre altre sono arrivate nel settore da poco. Tutte hanno evoluto le proprie metodologie di test insieme all'intero settore. Anche se ognuna utilizza un diverso sistema di punteggio (e non tutti i test includono ogni piattaforma), condividono generalmente un certo livello di standard rigorosi, un grado di trasparenza nella propria metodologia e un impegno nell'imparzialità tra i vari fornitori.

Chi testa il meglio del meglio?

I test condotti pubblicamente ed eseguiti da laboratori indipendenti di terze parti sono il punto di riferimento nell'affollato mercato della sicurezza informatica attuale. Tutti questi test hanno alcune caratteristiche comuni:

- Non sono finanziati dai fornitori
- Eseguono test relativi a prestazioni, falsi positivi e protezione
- Utilizzano enormi raccolte di malware
- Offrono ai fornitori la possibilità di contestare o chiarire i

2 IBM, Rapporto sul costo di una violazione dei dati, 2020

Una lunga storia di test AV indipendenti

1989

Virus Bulletin inizia a pubblicare ricerche e analisi sulle minacce

1991

Virus Bulletin organizza la prima conferenza internazionale

1999

AV-Comparatives nasce come progetto studentesco all'Università di Innsbruck

2005

AV-Test viene fondato a Magdeburg, in Germania

2007

NSS Labs viene lanciata come startup in Texas, negli Stati Uniti

2015

MITRE rilascia la piattaforma ATT&CK

2018

MITRE annuncia le valutazioni basate su ATT&CK

Apprendi la terminologia dei test AV

Malware significa semplicemente "software dannoso". Da virus a cavalli di Troia, fino a ransomware, adware e spyware, il termine include qualsiasi codifica intenzionalmente progettata per causare danni, ottenere dati senza autorizzazione o ingannare l'utente finale tramite false interpretazioni.

I test pubblici vengono eseguiti da laboratori indipendenti di terze parti su richiesta di un fornitore, a volte senza neppure il suo coinvolgimento. In genere, questi test si concentrano su standard rigorosi e assegnano dei voti, incluso quelli negativi, per ogni categoria. Alcuni test pubblici richiedono un costo di partecipazione, ma addebitandolo allo stesso modo a tutti i fornitori, mantengono l'imparzialità nei risultati.

Test privati o su commissione vengono fatti per volere del fornitore e spesso vengono anche finanziati direttamente da esso. Sebbene meno preziosi per i clienti che cercano di confrontare le piattaforme, questi test forniscono importanti conferme e feedback ai fornitori che lanciano nuovi prodotti e servizi. Inoltre, i test privati possono fornire preziosi confronti con determinati fornitori che normalmente evitano i test pubblici, consentendo ai fornitori di considerare le differenze sul mercato in un contesto significativo.

Gli ambienti di test del mondo reale offrono le informazioni più significative sul valore di una piattaforma. Questi test usano malware e virus online, e spesso vengono eseguiti per un periodo di tempo prolungato con continui aggiornamenti in tempo reale dei codici dannosi e degli URL inseriti. Sono anche progettati per selezionare l'opzione "Consenti" ogni volta che l'intervento dell'utente è richiesto dalla piattaforma, assicurandosi di tenere conto dell'errore dell'utente nel testare le reali capacità di protezione del sistema.

La protezione viene misurata dalla capacità della piattaforma di respingere correttamente gli attacchi di malware, che possono essere segnalati come "falsi positivi" o ping che superano le protezioni dell'AV. Lo standard varia tra i test, ma in genere è consentita una bassa percentuale come primo indicatore dell'integrità di una piattaforma.

I falsi positivi sono file puliti che vengono identificati erroneamente come dannosi. Questo standard viene anche misurato con una bassa percentuale che riceve un voto positivo, inoltre, è un indicatore essenziale della precisione della piattaforma.

Le prestazioni fanno il punto su quanto ogni piattaforma disponga di risorse nell'ambiente di sistema e sono un valore essenziale per bilanciare il grado di protezione di una piattaforma contro il consumo di risorse del sistema.

risultati
- Indicano le piattaforme che non superano i test in una o più categorie in base ai risultati

Considerando questi criteri, ecco alcuni dei principali laboratori indipendenti di terze parti per test antivirus e antimalware.

AV-Comparatives

In sintesi

- Certificato dall'European Institute for Computer Anti-Virus Research (EICAR)
- Certificato IS0 9001:2015 da TÜV Austria
- Verificato ogni anno per il controllo qualità da TÜV Austria

AV-Comparatives è noto per i suoi test del mondo reale relativi a protezione, malware e prestazioni. Dato che molti dei vettori di minacce odierni hanno origine online, il suo test di protezione del mondo reale è un'analisi particolarmente critica di qualsiasi piattaforma antivirus o antimalware per i clienti aziendali che proteggono dati e risorse aziendali vitali.

Per quanto riguarda i test di protezione del mondo reale, AV-Comparatives ha dichiarato, "Questi test valutano le capacità di protezione del "mondo reale" della suite con le impostazioni predefinite (tra cui le funzionalità di protezione all'esecuzione). Ci proponiamo di effettuare questi test in maniera rigorosa. Per questo motivo sono molto costosi in termini di tempo e risorse, quindi vengono inclusi solo i prodotti scelti per i test annuali delle serie principali."

Fondamentalmente, il test per la protezione del mondo reale di AV-Comparatives si concentra quasi esclusivamente sulla protezione piuttosto che sui falsi positivi o sulle prestazioni. Inoltre, questo test non considera le chiavette USB o le minacce LAN, ma solo quelle provenienti da Internet. Il test dei falsi allarmi nel test di protezione dinamico dell'intero prodotto del "mondo reale" è costituito da due parti: domini bloccati per errore (durante la navigazione) e file bloccati per errore (durante il download/installazione). È necessario testare entrambi gli scenari perché provare solo uno dei due casi precedenti potrebbe penalizzare i prodotti che non si concentrano principalmente su un tipo di metodo di protezione, filtro URL o protezione dei file basata su accesso / comportamento / reputazione.

AV-Comparatives offre anche un test di protezione del mondo reale migliorato, introdotto nel dicembre 2019. Man mano che gli attacchi continuano a diventare sempre più sofisticati, anche i test devono diventare più approfonditi. Il primo round di questo nuovo test ha selezionato un sottoinsieme di fornitori da testare contro scenari di attacchi avanzati, verificando così non solo la loro capacità di fermare gli attacchi, ma, quando hanno fermato ogni attacco, valutarne anche la capacità di arrestare le violazioni prima dell'esecuzione degli attacchi.[3]

AV-TEST

In sintesi

- Un laboratorio di test indipendenti con sede in Germania
- Fondato da Andreas Marx
- Rende disponibili al pubblico i risultati mensili dei test

AV-Test si concentra sulle certificazioni ed è noto per il suo sistema di classificazione flessibile che valuta software antivirus, strumenti antimalware e software di sicurezza per piattaforme Windows, Mac e Android. Di particolare rilievo è il suo test dei malware, eseguito continuamente su un database di oltre tre milioni di file, e-mail e siti web potenzialmente dannosi, con un massimo di 35.000 nuove minacce aggiunte ogni giorno. Ogni anno, AV-Test presenta il suo premio per la migliore protezione a una piattaforma in ciascuna delle categorie di test sia per il pubblico aziendale che per quello dei consumatori finali. AV-Test valuta ogni piattaforma di sicurezza informatica utilizzando un software di analisi interno in base a tre categorie: protezione, prestazioni e fruibilità. I fornitori possono guadagnare 6

3 https://www.av-comparatives.org/test-methods/

Come funziona un test AV?

Anche se ogni test ha le proprie caratteristiche, in genere, per un gruppo di piattaforme selezionate, tutti i test seguono un processo simile:

1. Installare la piattaforma nell'ambiente di test con impostazioni predefinite. Molti test funzionano su piattaforma Windows, ma vengono eseguiti anche test specifici per Mac, Android e Linux.

2. Introdurre i vettori della minaccia. Un campione di migliaia di file con percentuali note di file dannosi o danneggiati da database attentamente gestiti.

3. Eseguire il test per un determinato periodo di tempo. Ciò consente di effettuare una valutazione per la ricerca di falsi positivi e falsi negativi.

4. Segnalare i risultati a ciascun fornitore, lasciando il tempo per eventuali domande o contestazioni.

5. Pubblicare i risultati.

punti per categoria, con un punteggio perfetto pari a 18 punti. Qualsiasi fornitore che supera con successo un ciclo di test completo riceve l'approvazione e la certificazione di AV-Test per un anno. Per verificare come si è comportato un determinato fornitore nel corso della cronologia, è sufficiente fare clic sul nome del fornitore e visualizzare la cronologia completa dei punteggi per una determinata categoria di test.[4]

MITRE

In sintesi

- Ha sviluppato la knowledge base ATT&CK, fornendo accesso gratuito a "informazioni del mondo reale su tattiche e tecniche di attacco".
- Opera negli Stati Uniti in una partnership pubblica-privata tramite la FFRDC (centri di sviluppo e ricerca finanziati a livello federale).

Come risorsa pubblicamente disponibile, la piattaforma ATT&CK è stata lanciata nel 2015 ed è diventata rapidamente una risorsa molto preziosa per i professionisti della sicurezza informatica, concentrandosi su test e valutazioni da parte di team interni che si coordinano tra red team, difensori e manager.

La MITRE ATT&CK Matrix for Enterprises fornisce una mappa accessibile di tattiche e tecniche osservate durante gli attacchi informatici, una risorsa che da allora molti fornitori di sicurezza hanno iniziato a usare. Infatti, molti fornitori attualmente considerano la terminologia della piattaforma ATT&CK uno standard del settore per descrivere gli attacchi informatici. Nel 2018, MITRE ha annunciato il primo gruppo di valutazioni dei prodotti basato su ATT&CK, che è rapidamente diventato lo standard nei test dei prodotti Endpoint Detection and Response. Tutti i risultati sono stati resi pubblici, in linea con la missione di MITRE di "fornire una visione oggettiva". Tuttavia, vale la pena notare che le valutazioni non sono certificazioni ma piuttosto analisi indipendenti delle capacità di rilevamento di ciascuna piattaforma. I risultati non vengono valutati, classificati o giudicati, né le piattaforme vengono confrontate tra loro.

Usando ciò che MITRE chiama "adversary emulation" o testando "nello stile di un determinato adversary", le valutazioni di ATT&CK concentrano il test su sottoinsiemi di tecniche consolidate. Più di recente, MITRE APT 29 ha testato i prodotti rispetto al gruppo di minacce APT 29 emulate. Per ogni fornitore testato, le minacce rilevate vengono annotate durante ogni

4 https://www.av-test.org/en

fase dell'attacco. Questa valutazione distingue tra i tipi di rilevamento: i rilevamenti di telemetria e MSSP sono intrinsecamente ritardati e spesso è difficile per un reparto IT aziendale medio agire senza l'aiuto di un team SOC. Invece le categorie Generale, Tattiche e Tecniche identificano un'azione sospetta e determinano ciò che l'aggressore sta cercando di ottenere (come guadagnare la persistenza), e come sta tentando di ottenerlo.[5, 6]

NSS LABS

In sintesi

- Lanciata come startup in Texas per integrare i test di terze parti disponibili
- Nota per i test avanzati di protezione degli endpoint con l'inclusione dei calcoli del costo totale di esercizio per ogni soluzione testata

In qualità di uno dei più recenti laboratori di test, NSS si concentra sulla ricerca di minacce e vulnerabilità, cercando di capire "i molti modi in cui gli aggressori possono aggirare i prodotti di sicurezza". Di conseguenza, è ben attrezzato per misurare l'efficacia e le prestazioni di una piattaforma di sicurezza informatica, esaminando anche stabilità, fruibilità e costi di esercizio.

Le sue metodologie di test sono basate su briefing pubblici gratuiti con utenti, analisti e fornitori. In base alle informazioni raccolte in questi dialoghi ricorrenti, l'azienda ha aggiornato le sue procedure, che sono state poi vagliate da un consiglio d'amministrazione. Mentre i prodotti vengono valutati, sono classificati come Consigliato, Neutro o Cautela. È importante notare che tutti i prodotti iniziano con una valutazione di Cautela e ottengono la valutazione finale esclusivamente sulla base dei risultati dei test e dei dati empirici.

I fornitori sono invitati a partecipare ai nostri test di gruppo in base alla loro presenza sul mercato o su richiesta dei clienti aziendali. Anche se la partecipazione a un gruppo di test NSS è sempre gratuita, i costi vengono sostenuti vendendo i risultati del test ai clienti interessati tramite un abbonamento e vendendo i diritti di marketing ai fornitori interessati al termine del test.[7]

5 https://www.mitre.org/news/press-releases/mitre-releases-results-of-evaluations-of-21-cybers ecurity-products
6 https://attackevals.mitre-engenuity
7 https://www.nsslabs.com/about/

Lo standard del protocollo di test AMTSO

Nel 2018, L'Anti-Malware Testing Standards Organization (AMTSO) ha creato "un insieme concordato di regole per la trasparenza, l'equilibrio e la chiarezza" tra i laboratori di test.

1. I test non devono mettere in pericolo il pubblico [creando nuovi malware].
2. I test devono essere imparziali.
3. I test dovrebbero essere ragionevolmente accessibili e trasparenti.
4. L'efficacia e le prestazioni dei prodotti anti-malware devono essere misurate in modo equilibrato.
5. I tester devono prestare la dovuta attenzione per confermare se i campioni o i casi da esaminare siano stati classificati accuratamente come dannosi, innocui o non validi.
6. La metodologia di un test deve essere coerente con la sua finalità.
7. Le conclusioni di un test devono essere basate sui risultati del test.
8. I risultati dei test dovrebbero essere statisticamente validi.
9. Fornitori, tester ed editori devono avere un punto di contatto attivo per la corrispondenza relativa ai test.

Quali risultati ha ottenuto Bitdefender nei test AV indipendenti?

Bitdefender Endpoint Security ha ottenuto costantemente la prima posizione in materia di protezione o rilevamento nei test EDR e AV condotti dalle organizzazioni indipendenti di test più rinomate. Dal giugno 2016 a oggi, Bitdefender ha ottenuto un punteggio massimo di 6 per la protezione in tutti i 26 test aziendali di AV-TEST. Bitdefender ha anche dominato il test di rilevamento migliorato proposto da AV-Comparatives nel 2019, ottenendo un risultato perfetto nella prova di protezione in pre-esecuzione. Inoltre, è stato l'unico fornitore a ottenere un punteggio perfetto contro le minacce avanzate nel 2020. Nella valutazione MITRE APT 29, pubblicata nell'aprile del 2020, Bitdefender ha ottenuto il maggior numero di rilevamenti contestuali e una copertura completa degli attacchi con rilevamenti utilizzabili.

La soluzione Bitdefender Security for Mail Servers, basata sulla tecnologia antispam, è l'unico prodotto ad aver ricevuto una certificazione in tutti i test VBSpam mai eseguiti e l'unica soluzione ad aver conquistato 24 riconoscimenti VBSpam+ consecutivi, la più importante certificazione assegnata nei test di VBSpam eseguiti da Virus Bulletin.

Scopri maggiori informazioni sui test indipendenti e le tecnologie comportamentali e basate sull'IA che hanno dato un tale vantaggio a Bitdefender.

Virus Bulletin

In sintesi

- Noto per la sua conferenza annuale e le sue certificazioni bimestrali
- Un laboratorio di test con sede nel Regno Unito e decenni di esperienza

Operando da oltre 30 anni, Virus Bulletin è noto per il suo riconoscimento VB100. Per molti anni, questa certificazione di fatto è stata considerata uno standard minimo di qualità per il rilevamento dei malware per la sua semplicità: "dimostrare se un prodotto è in grado di rilevare il 100% dei campioni di malware elencati nella WildList senza generare falsi positivi."

Virus Bulletin non è un'analisi comparativa delle prestazioni tra piattaforme, né è relativa al mondo reale nelle sue metodologie. Tuttavia, è uno standard statico di prima linea per stabilire le capacità di rilevamento in modo uniforme su qualsiasi piattaforma di sicurezza informatica nel mondo.

Il test della certificazione VB100 utilizza un "insieme di campioni quasi standard, che cambia da test a test" per misurare le prestazioni tramite l'esposizione a una serie nota di campioni di malware per diversi giorni sia in modalità "su accesso" che "su richiesta". In genere, questi test includono gli elenchi WildList e AMTSO RTTL.

Il successivo Diversity Test ha esposto la piattaforma a una più ampia selezione di campioni. Tuttavia, non viene considerato una parte del processo di certificazione ed è semplicemente una serie di dati complementari per scopi contestuali. Il test VB100 determina anche i falsi positivi usando un set pulito di oltre 400.000 file gestiti da VB.[8]

8 https://www.virusbulletin.com/testing/vb100/vb100-methodology/vb100-methodology-ver1-1/

Come posso sapere di chi fidarmi?

Prima di tutto, sbarazziamoci di un luogo comune, ovvero che i test degli antivirus non siano altro che pubblicità "Pay to play" sotto mentite spoglie. Anche se ci sono sicuramente molte "certificazioni" che possono essere acquistate, i test indipendenti analizzati in questo white paper sono assolutamente reali e affidabili. Se la realtà fosse questa, i risultati la mostrerebbero subito, perché le piattaforme con i maggiori budget otterebbero sempre il miglior riconoscimento! Il fatto che si possa guardare nel tempo e alla diversa gamma di test disponibili e trovare costantemente piccoli innovatori della sicurezza informatica riconosciuti per il loro contributo sul campo dovrebbe dimostrare che questi test riguardano più la convalida che la monetizzazione.

Ecco tre suggerimenti chiave che ti aiuteranno a capire come valutare la validità di qualsiasi test antivirus, anche se non è trattato in questo white paper.

Segui il denaro - I finanziamenti per i principali test AV ed EDR sono trasparenti ed è un parametro che vale la pena considerare quando si valuta l'affidabilità dei risultati. Come regola generale, i test privati, sponsorizzati da un singolo fornitore, tendono a essere considerati meno affidabili rispetto a quelli in cui i fornitori contribuiscono in egual modo o il finanziamento proviene da altre fonti.

Considera le tendenze - Con un numero sufficiente di test, in particolare test commissionati da privati, qualsiasi prodotto può ottenere un ottimo risultato almeno una volta. Perciò cerca di andare oltre a un singolo risultato o momento temporale, valutando una gamma più ampia di test, in grado sicuramente di stabilire una tendenza di prestazioni comprovate e coerenti con un periodo di tempo più lungo.

Non fidarti di un solo risultato - Se consideri un solo test per confermare il tuo acquisto, probabilmente ti mancheranno delle informazioni. Invece, cerca conferma attraverso più test indipendenti prima di prendere qualsiasi decisione. Come abbiamo mostrato in precedenza, ogni test enfatizza punti di forza, punti deboli e modalità di reportistica differenti. Questo ci riporta al punto in cui abbiamo iniziato: conosci la tua attività meglio di chiunque altro. Ora che hai a disposizione questa serie di valutazioni approfondite, hai molte più informazioni per prendere ogni decisione sul partner di sicurezza informatica giusto per proteggere le tue risorse digitali. Anche se non esiste un test perfetto, né probabilmente ci sarà mai in futuro, ma i test indipendenti per le piattaforme software sono un indicatore prezioso dell'efficacia della protezione del mondo reale, oltre che uno strumento utile per i leader IT occupati che necessitano di una conferma affidabile della protezione scelta per la propria azienda.

Perché Bitdefender

Servire con orgoglio i nostri clienti

Bitdefender offre soluzioni e servizi per piccole e medie imprese, fornitori di servizi e integratori di tecnologia. Siamo orgogliosi della fiducia che aziende come **Mentor, Honeywell, Yamaha, Speedway, Esurance o Safe Systems** ripongono in noi.

Leader nel Forrester's Inaugural Wave™ per la sicurezza dei carichi di lavoro cloud

Valutazione "Consigliato" da NSS Labs nel NSS Labs AEP Group Test

Premio SC Media Industry Innovator per Hypervisor Introspection, per il secondo anno di fila

Fornitore rappresentativo di Gartner® di piattaforme per la protezione del carico di lavoro cloud

Al servizio dei nostri oltre 20.000 partner nel mondo

Come fornitore di canale esclusivo, Bitdefender è lieta di condividere i successi con decine di migliaia di rivenditori e distributori al mondo.

Partner a 5 stelle di CRN per 4 anni di fila. Riconosciuto nell'elenco Security 100 di CRN. Partner cloud di CRN per il secondo anno di fila

Più soluzioni integrate per MSP rispetto a qualsiasi altro fornitore

3 programmi per i partner di Bitdefender diversi, per consentire a tutti i nostri partner, rivenditori, fornitori di servizi e partner ibridi di concentrarsi sulla vendita delle soluzioni Bitdefender che corrispondono meglio alla propria specializzazione.

Un'autorità di sicurezza affidabile

Bitdefender è un fiero partner di alleanza tecnologica con i principali fornitori di virtualizzazione, contribuendo direttamente allo sviluppo di ecosistemi sicuri con **VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS e Pivotal.**

Tramite il suo team di esperti forensi, Bitdefender si impegna anche nella lotta contro il crimine informatico internazionale con le principali forze dell'ordine come FBI ed Europol, in iniziative come NoMoreRansom e TechAccord, oltre all'eliminazione di black market, come Hansa. A partire dal 2019, Bitdefender è anche una fiera CVE Numbering Authority approvata nella partnership MITRE.

RICONOSCIUTA DAI PRINCIPALI ANALISTI E ORGANIZZAZIONI DI TEST INDIPENDENTI

CRN AVTEST AV Gartner 451 Research FORRESTER IDC GLOBAL

ALLEANZE TECNOLOGICHE

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

Bitdefender

Fondata nel 2001, in Romania
Numero di dipendenti Oltre 1.800

Sedi principali
Enterprise HQ – Santa Clara, California, Stati Uniti
Technology HQ – Bucarest, Romania

UFFICI NEL MONDO
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europa: Copenaghen, DANIMARCA | Parigi, FRANCIA | Monaco, GERMANIA | Milano, ITALIA | Bucarest, Iasi, Cluj, Timisoara, ROMANIA | Barcellona, SPAGNA | Dubai, UAE | Londra, Regno Unito | Hague, PAESI BASSI
Australia: Sydney, Melbourne

SOTTO IL SIMBOLO DEL LUPO

Quello della sicurezza dei dati è un comparto brillante dove solo la visione più chiara, la mente più acuta e l'intuito maggiore possono vincere. È una partita senza margine di errore. Il nostro obiettivo è vincere ogni volta, senza limiti.

E lo facciamo. Eccelliamo nel settore non solo grazie a una visione più chiara, una mente più acuta e un intuito sempre maggiore, ma restando sempre un passo avanti a chiunque altro, siano essi "cappelli neri" o altri esperti di sicurezza. La brillantezza della nostra mente collettiva è come un **luminoso Lupo-Drago** accanto a te, alimentato da intuizioni ingegnerizzate, creato per proteggerti da tutti i pericoli nascosti nelle arcane complessità del regno digitale.

Tale brillantezza è il nostro super potere ed è alla base di tutti i nostri prodotti e soluzioni rivoluzionarie.

Bitdefender-Whitepaper-MSP_SS-haPrint-crea[5]194-it_IT
03/15/21March 15, 2021 9:47 am03/15/21