IBM Security
Thought Leadership White Paper

Ottobre 2016.

Combattere le minacce di sicurezza con il controllo e la security intelligence applicata agli endpoint

Prioritizzare le vulnerabilità e accelerare gli interventi di remediation con IBM QRadar e e IBM BigFix

Sommario

Introduzione

Dal malware customizzato agli attacchi 0-day, le minacce avanzate di sicurezza stanno aumentando vertiginosamente in tutto il mondo e la sofisticazione di questi attacchi ha raggiunto proporzioni senza precedenti. I criminali informatici di oggi sono abili nell'individuare le vittime da colpire via e-mail o con attacchi via Web, oltre a sfruttare le vulnerabilità degli endpoint stessi. Attualmente, vengono sferrati attacchi di vaste proporzioni, coordinati e sofisticati sul piano operativo, che si estendono in ampie aree della rete, bypassando i meccanismi di sicurezza tradizionali. E il numero di malware continua a crescere.

In che modo un'organizzazione può stare al passo con queste minacce avanzate di sicurezza? E' assolutamente necessario e importante mantenere un livello elevato di sicurezza di base, implementando costantemente politiche di sicurezza e livelli di patch su endpoint e server. Tuttavia, quando le reti sono esposte a diverse vulnerabilità per ogni indirizzo IP nella fase di scansione, la lentezza del processo di attenuazione e patching di queste debolezze può provocare varchi insidiosi per la sicurezza. Il personale IT di oggi è chiamato a prendere decisioni difficili, basate sul rischio, sulle quali concentrare il proprio effort, spesso senza avere un quadro completo dell'ambiente di sicurezza. Questo è ancora più critico quando il numero di vulnerabilità nell'intero ambito aziendale è in aumento, mentre l'organizzazione dispone di risorse e competenze limitate per risolvere le vulnerabilità. Oltre ad essere in grado di rilevare le vulnerabilità in modo efficiente, le organizzazioni devono anche prendere in considerazione il contesto più ampio di tali vulnerabilità e associarle ai livelli di rischio, in modo da poter concentrare i propri interventi di rimedio sulle aree di maggior rischio.

Questo white paper illustra come contrastare le minacce avanzate di sicurezza attraverso l'adozione di un approccio integrato, intelligente e automatizzato per la sicurezza degli endpoint. Spiega come ampliare il contesto e le capabilities di IBM® QRadar Security Intelligence Platform con il controllo e la security intelligence applicata agli endpoint di IBM BigFix allo scopo di identificare, assegnare priorità e rimediare ad una condizione di rischio individuata. Il paper esamina il valore strategico legato all'uso combinato di queste soluzioni per combattere le più recenti modalità di attacco.

IBM QRadar Security Intelligence Platform

QRadar Security Intelligence Platform è una soluzione che aiuta le organizzazioni a combattere efficacemente gli attacchi sempre più sofisticati per salvaguardare gli ambienti di rete, proteggere la proprietà intellettuale ed evitare interruzioni dell'attività. La piattaforma non si limita a monitorare i log e i dati del flusso di rete; raccoglie dati e attività da una grande varietà di fonti di dati ed esegue la correlazione in tempo reale con le regole e la threat intelligence per identificare rapidamente le offense contro la sicurezza che potrebbero richiedere un intervento immediato.

IBM QRadar Risk Manager, integrato a QRadar Security Intelligence Platform, permette alle aziende di gestire in modo proattivo le configurazioni dei dispositivi di rete e di correlarle alla topologia della rete, al fine di analizzare e identificare i rischi per la sicurezza e i possibili percorsi di attacco.

IBM QRadar Vulnerability Manager, anch'esso integrato a QRadar Security Intelligence Platform, fornisce una soluzione efficace per rilevare le vulnerabilità nei dispositivi presenti sulla rete. Consente inoltre di acquisire e consolidare i risultati della scansione da vari scanner di vulnerabilità. Sfruttando i dati della piattaforma QRadar Security Intelligence e di QRadar Risk Manager, QRadar Vulnerability Manager può agire da punto di controllo centralizzato per il reporting e la prioritizzazione della vulnerabilità nell'intero ambito aziendale.

IBM BigFix per la sicurezza degli endpoint

La migliore protezione contro le minacce agli endpoint consiste nell'individuazione delle vulnerabilità del software o della configurazione e nel proteggere gli endpoint prima che un exploit possa procurare danni nella rete. BigFix offre una soluzione di gestione degli endpoint e di sicurezza che consente ai clienti di monitorare costantemente la configurazione degli endpoint, il software installato, il sistema operativo o le patch delle applicazioni e di segnalare la conformità alle politiche su tutti i dispositivi basati su policy, sia preconfigurate che personalizzate. BigFix è anche in grado di risolvere prontamente la non conformità utilizzando i messaggi di IBM Fixlet per modificare lo stato di configurazione degli endpoint, applicare patch appropriate, rimuovere i file di malware o arrestare i processi sospetti. Questo ciclo continuo di monitoraggio, segnalazione e risoluzione consente di eliminare efficacemente le finestre di opportunità degli attacchi.

Secondo il rapporto di un'indagine sulla violazione dei dati condotta nel 2015, quasi la metà delle vulnerabilità scoperte di recente sono state sfruttate nelle prime quattro settimane dopo la segnalazione, in quanto gli hacker sanno che molte organizzazioni non sono in grado di risolvere in modo efficace le nuove vulnerabilità.[1] Il patching efficace si conferma ancora l'approccio migliore per attenuare il rischio di malware che sfrutta le nuove vulnerabilità. BigFix fornisce un processo di patching automatico, semplificato ed efficiente in tutti gli endpoint, all'interno o all'esterno della rete aziendale, per i vari sistemi operativi e applicazioni. Il patching che utilizza BigFix consente di ridurre significativamente i tempi del ciclo di patching e di abbattere notevolmente i costi operativi.

Per le vulnerabilità che non hanno ancora patch disponibili (vulnerabilità 0-day), BigFix offre alle aziende una funzionalità di quarantena in remoto che consente di isolare dalla rete gli endpoint colpiti in modo che possano essere protetti contro gli attacchi e non infettino altri endpoint fino a quando non sarà disponibile una patch o un altro rimedio.

Colmare i divari in materia di gestione delle vulnerabilità

Per difendersi contro le minacce di sicurezza, le aziende hanno bisogno di un approccio globale per identificare e attenuare i rischi ad alta priorità in un ambiente IT in continuo cambiamento. Questo approccio deve includere le seguenti attività:

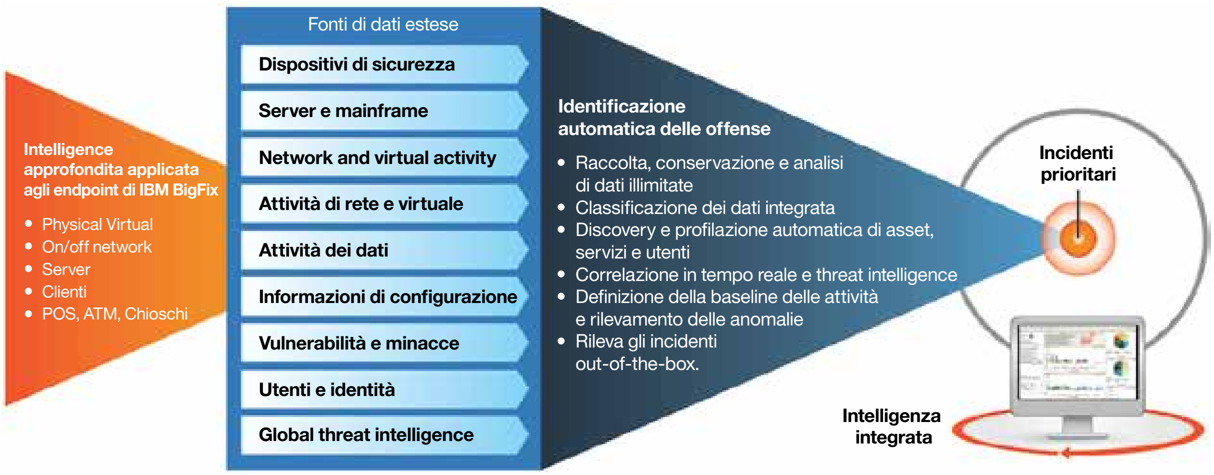
- Capire lo stato aggiornato al minuto dei diversi endpoint
- Identificare le vulnerabilità di ciascun endpoint
- Attribuire priorità alle vulnerabilità
- Agire rapidamente per porre rimedio o attenuare le vulnerabilità degli endpoint ad alta priorità o per mettere in quarantena i dispositivi
- Confermare che l'azione correttiva abbia effettivamente ripristinato un maggiore stato di sicurezza dell'endpoint.

Molte soluzioni di gestione delle vulnerabilità si concentrano sull'identificazione o sull'attribuzione delle priorità alle vulnerabilità, ma non dispongono di intelligence e capabilities in grado di porre rimedio alle vulnerabilità in modo efficiente secondo le priorità attribuite. IBM può aiutare le organizzazioni a colmare questo gap associato alla gestione delle vulnerabilità, combinando BigFix con QRadar Security Intelligence Platform. Questa soluzione integrata consente all'organizzazione di identificare e prioritizzare le vulnerabilità dei sistemi operativi o del software applicativo che gli aggressori possono sfruttare per poi sanare tali vulnerabilità al fine di prevenire un attacco o ridurre al minimo l'impatto che esercita sull'organizzazione.

Definire una gestione del rischio a circuito chiuso con l'intelligence applicata agli endpoint

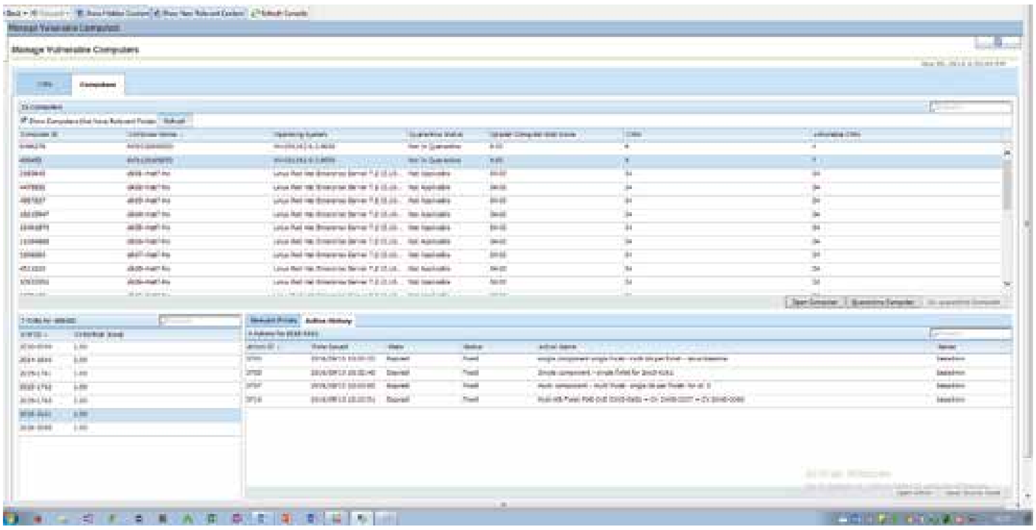
Oggi, le minacce avanzate diventano sempre più sofisticate, dinamiche e dannose, ecco perché l'esigenza di risorse integrate, intelligenti e automatizzate non è mai stata così grande. L'utilizzo di una soluzione integrata che combina sia Security Intelligence Platform QRadar che BixFix consente di potenziare le operazioni IT e i team di sicurezza affinché cooperino per proteggere gli assets da attacchi sempre più sofisticati.

BigFix può fornire informazioni approfondite sullo stato degli endpoint, quasi in tempo reale, segnalando le patch applicate, le modifiche di configurazione recenti, e molto altro ancora, alla QRadar Security Intelligence Platform, al fine di migliorare la precisione dell'analisi del rischio del sistema. Più nello specifico, l'agente BigFix in esecuzione su un endpoint, all'interno o all'esterno della rete dell'organizzazione, valuta continuamente la conformità alle policy di configurazione e di patching e comunica lo stato più recente a QRadar che, in tal modo, può correlare lo stato degli endpoint con altri eventi di sicurezza o attività di rete per individuare gli incidenti sospetti.



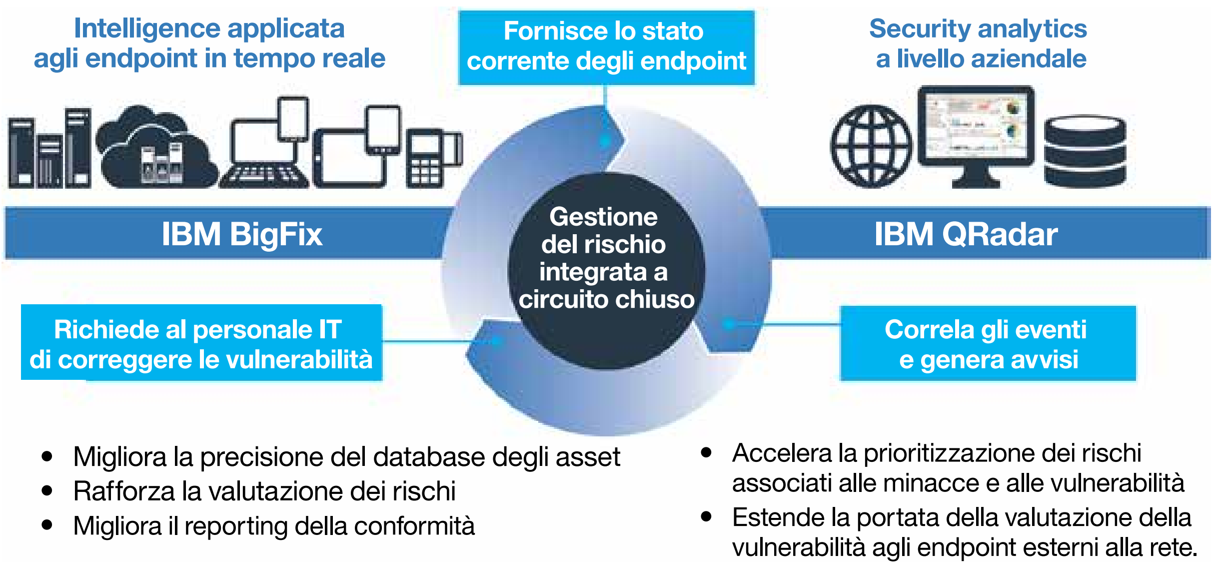
IBM BigFix comunica lo stato più recente dell'endpoint a IBM QRadar che correla tale stato con altri eventi di sicurezza per individuare e prioritizzare gli incidenti sospetti.

QRadar Vulnerability Manager può essere utilizzato per eseguire la scansione delle vulnerabilità o per acquisire le vulnerabilità da BigFix e altri scanner di vulnerabilità degli endpoint, al fine di assegnare un punteggio di rischio a ciascun asset sulla base di una correlazione con un contesto più ampio fornito da QRadar Risk Manager che include la topologia di rete e le attività di comunicazione per poi inviare gli score di vulnerabilità e di rischio degli asset a BigFix. Per ogni vulnerabilità rilevata da QRadar, BigFix è in grado di identificare le azioni correttive appropriate (patching o quarantena) che il personale IT può implementare. Inoltre, il personale IT può utilizzare lo score di rischio dell'asset, il numero di vulnerabilità su ciascun endpoint o l'azione correttiva per attribuire una priorità agli interventi di rimedio, in modo che le vulnerabilità più critiche possano essere sanate prima.



IBM BigFix consente di porre rimedio in modo efficace alle vulnerabilità identificate da QRadar Vulnerability Manager e fornisce diverse metriche che permettono ai clienti di attribuire una priorità agli interventi di rimedio.

Dopo aver implementato l'azione correttiva, lo stato dell'endpoint più recente viene riferito a QRadar, che, a sua volta, è correlato ad altri eventi di sicurezza o alle attività di rete e può aggiornare gli incidenti sospetti precedentemente segnalati. Grazie alla combinazione dell'intelligence applicata agli endpoint e del controllo di BigFix con le funzionalità di security intelligence di QRadar a livello aziendale, l'organizzazione può definire un programma di gestione del rischio in costante esecuzione, a circuito chiuso, in grado di combattere efficacemente le minacce associate alla sicurezza.



IBM BigFix e IBM QRadar, insieme, formano un sistema di gestione integrata dei rischi a circuito chiuso in tempo reale con intelligence applicata agli endpoint e security analytics nell'intero ambito aziendale.

Conclusioni

Per rendere più efficace la gestione delle vulnerabilità, le aziende hanno bisogno di un approccio integrato che incorpori sia l'intelligence applicata agli endpoint che il contesto di rete. Il personale IT ha bisogno di sapere quali vulnerabilità sono programmate per essere sottoposte a patching da un sistema di gestione degli endpoint e quali non lo sono, per contribuire a garantire che le priorità degli interventi di rimedio siano definite in modo efficiente. Inoltre, il personale IT deve essere in grado di intervenire rapidamente sul fronte della security intelligence e di eseguire gli aggiornamenti necessari in tutti gli endpoint all'interno dell'organizzazione.

Le soluzioni QRadar e BigFix possono coesistere per aiutare le organizzazioni a tenere il passo con le minacce avanzate. Questo approccio intelligente, automatizzato e integrato può apportare valore strategico, promuovendo la gestione consolidata e l'uso efficiente delle risorse di sicurezza. I tempi di risposta agli incidenti, inclusi i ritardi tra l'esposizione alla vulnerabilità e il rilevamento, possono essere ridotti combinando i dettagli sullo stato degli endpoint forniti da BigFix con la security intelligence delle soluzioni QRadar, riducendo milioni di eventi di sicurezza ad un elenco gestibile e prioritario dei punti di debolezza. In questo modo, le aziende possono adottare un approccio proattivo per potenziare le proprie risorse IT contro le minacce più persistenti, riducendo in modo significativo il rischio.

La sicurezza nazionale richiede la conformità degli endpoint in tempo reale

Le agenzie federali si trovano ad affrontare una moltitudine di minacce per la sicurezza; tale fenomeno ha introdotto dei requisiti normativi per l'implementazione di soluzioni in grado di monitorare, gestire e attenuare continuamente le vulnerabilità. L'integrazione delle soluzioni QRadar e BigFix offre alle agenzie federali un valore straordinario.

Una soluzione informatica di cybersecurity può aiutare le agenzie governative a combattere le minacce ed eliminare le vulnerabilità. A titolo di esempio, oltre 50 agenzie federali degli Stati Uniti si sono standardizzate con BigFix per gestire e proteggere più di tre milioni di postazioni di lavoro, server (fisici e virtuali) e altri endpoint su una vasta gamma di sistemi operativi. Tali soluzioni garantiscono sicurezza e conformità degli endpoint continua e in tempo reale, sfruttando una library di molte migliaia di controlli.

Per ulteriori informazioni

Per saperne di più su IBM QRadar Security Intelligence Platform, IBM BigFix o altre soluzioni IBM Security contattate il rappresentante IBM o il Business Partner IBM di zona, oppure visitate i seguenti siti: ibm.com/security

IBM Security Solutions

IBM Security offre uno dei portafogli più avanzati e integrati di prodotti e servizi per la sicurezza enterprise. Il portafoglio, supportato da una divisione di ricerca e sviluppo di fama mondiale, IBM X-Force, fornisce informazioni sulla sicurezza per consentire alle organizzazioni di proteggere, con un approccio olistico, il proprio personale, infrastrutture, dati e applicazioni, offrendo soluzioni per la gestione dell'identità e degli accessi, la sicurezza del database, lo sviluppo applicativo, la gestione del rischio, la gestione degli endpoint, la sicurezza di rete e molto altro ancora. Queste soluzioni consentono alle organizzazioni di gestire in modo efficace i rischi e di implementare la sicurezza integrata per il mobile, il cloud, i social media e altre architetture di business. IBM gestisce una delle più ampie organizzazioni che operano sul fronte della ricerca, sviluppo e delivery in materia di sicurezza su scala mondiale, monitora 15 miliardi di eventi di sicurezza al giorno in oltre 130 paesi e detiene più di 3.000 brevetti di sicurezza.

Inoltre, IBM Global Financing offre numerose opzioni di pagamento che consentono di acquisire la tecnologia necessaria per far crescere il vostro business. Forniamo la gestione completa del ciclo di vita di prodotti e servizi informatici, dall'acquisizione alla dismissione. Per ulteriori informazioni, visitate: ibm.com/financing

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (MI)
Italia

[1] "2015 Data Breach Investigations Report," *Verizon*, Aprile 2015. https://msisac.cisecurity.org/whitepaper/documents/1.pdf

WGW03051-ITIT-02