FIREEYE HELIX

SEMPLIFICA, INTEGRA E AUTOMATIZZA LE OPERAZIONI DI SICUREZZA

FireEye Helix è una piattaforma di rilevamento e risposta globale progettata per semplificare, integrare e automatizzare le operazioni di sicurezza. FireEye comprende attacchi informatici meglio di chiunque altro e applica queste conoscenze per eliminare la complessità della sicurezza. Il nostro approccio basato sulle informazioni fonde tecnologie di sicurezza innovative, informazioni FireEye iSIGHT a livello nazionale e la comprovata esperienza di Mandiant in FireEye Helix: la nostra piattaforma per la risposta e le operazioni di sicurezza end-to-end.

Attualmente, l'esperienza delle operazioni di sicurezza è sconnessa, con avvisi generati in decine di prodotti a bassa fedeltà e console di gestione senza il beneficio delle informazioni contestuali o automazione e orchestrazione. Questo fa sì che i responsabili IT e della sicurezza dedicano più tempo a processi manuali inefficienti e alla gestione delle infrastrutture, lasciando l'azienda meno sicura.

Progettato da esperti di sicurezza per esperti di sicurezza, FireEye Helix aiuta le aziende a rendere operativi i programmi di sicurezza e consente ai team di sicurezza di passare dal rilevamento di una minaccia alla sua rapida eliminazione con un basso costo totale di proprietà. Possono visualizzare chiaramente se le risorse sono assegnate effettivamente e se il loro approccio alla sicurezza è migliorato.

FireEye Helix si basa su una piattaforma rivoluzionaria che riunisce il portafoglio di prodotti FireEye e i dati degli eventi provenienti da componenti non-FireEye di un'infrastruttura IT e di sicurezza. Da questa piattaforma centralizzata, i team di sicurezza possono sovrapporre FireEye iSIGHT Intelligence per valutare le minacce nascoste ed eseguire analisi accurate per rilevare movimento laterale, esfiltrazione di dati, usi illeciti degli account e anomalie di comportamento degli utenti. Per tutto il tempo, costruiscono il contesto per automatizzare, definire le priorità e accelerare l'attività di risposta. Queste funzionalità sono disponibili tramite dashboard unificate, moduli di ricerca e di reporting guidati che consentono agli utenti di passare rapidamente dal rilevamento all'indagine alla risposta su ogni componente infrastrutturale.

Vantaggi

Aumenta la tua visibilità

FireEye Helix si avvale del nostro pluripremiato motore MVX che coordina il rilevamento delle minacce alla rete e agli endpoint. Raccoglie e combina in modo intelligente i metadati di rete e gli avvisi provenienti da tutta l'infrastruttura di sicurezza e li invia a una console unificata. E sovrappone le informazioni, le regole e gli strumenti di analisi FireEye iSIGHT per dare alla tua azienda una consapevolezza della situazione senza precedenti, e rimanere così sempre un passo avanti rispetto agli attacchi.

Accelera la risposta e riduci al minimo l'impatto di una violazione

Per bloccare le minacce ti servono le informazioni giuste al momento giusto. Helix offre agli analisti avvisi convalidati con analisi contestuali e la possibilità di passare rapidamente dal rilevamento alla risoluzione sia sulla rete che su un endpoint. Questo contribuisce a risolvere gli attacchi in modo rapido ed efficace e fornisce dashboard e report utili alle verifiche di conformità e ai briefing di gestione.

FireEye Helix accelera e semplifica il rilevamento delle minacce end-to-end e il processo di risposta, riunendo gli investimenti tecnologici esistenti e i processi di gestione degli incidenti in flussi di lavoro automatizzati, in grado di offrire risposte in tempo reale, ridurre l'esposizione al rischio e mantenere la coerenza del processo in un programma di sicurezza. Ogni distribuzione viene fornita con playbook pre-costruiti che codificano anni di esperienza FireEye per combattere le violazioni più consequenziali al mondo. Questi playbook affinano i tuoi processi per rilevare, indagare e rispondere in modo efficace alle minacce.

Migliorare gli investimenti di sicurezza esistenti e riduci i costi operativi

Molte aziende dispongono di strumenti di sicurezza che sono scollegati e richiedono una più lenta elaborazione manuale, soggetta a errori. FireEye Helix si integra e potenzia gli strumenti di sicurezza esistenti con la correlazione automatica, playbook pre-costruiti e contesto FireEye iSIGHT Intelligence per aiutarti a definire la priorità degli avvisi più rilevanti e indagare e rispondere alle minacce più velocemente che mai.

Scala le tue operazioni in modo flessibile

Le aziende cambiano e crescono nel tempo e FireEye Helix è progettato per evolversi insieme a loro. Utilizza l'elasticità del cloud per scalare rapidamente il consumo e la distribuzione e può sempre includere gli strumenti e le tecnologie le più recenti a disposizione per ottenere la miglior difesa cibernetica possibile. FireEye Helix funziona in locale e in ambienti cloud privati, pubblici e ibridi.

Ottieni la conformità

Per molte aziende, la rendicontazione della conformità è spesso un compito del team di sicurezza, perché ha accesso alle attività di conformità e l'esperienza necessaria per proteggere i sistemi critici. FireEye Helix contiene dashboard pre-configurate per fornire visibilità nel tuo programma di conformità e una capacità di ricerca programmata per raccogliere dati non elaborati nel corso del tempo. Aiuta il tuo team a soddisfare le richieste di revisione rapidamente, in modo che possa concentrarsi sulla protezione della rete.

Architettura FireEye Helix

Con le opzioni di distribuzione flessibili, qualsiasi azienda può personalizzare FireEye Helix per soddisfare i requisiti del proprio programma di sicurezza e l'architettura esistente. Un abbonamento annuale comprende il diritto a livello aziendale per:

- Console unificata basata su cloud con orchestrazione e analisi integrate di FireEye iSIGHT Intelligence
- Smart node della sicurezza di rete
- Agenti endpoint

Questo può essere ulteriormente migliorato tramite i componenti opzionali di FireEye iSIGHT Intelligence, la sicurezza email integrata, una maggiore personalizzazione dell'orchestrazione di sicurezza, più playbook pre-costruiti e FireEye come servizio.

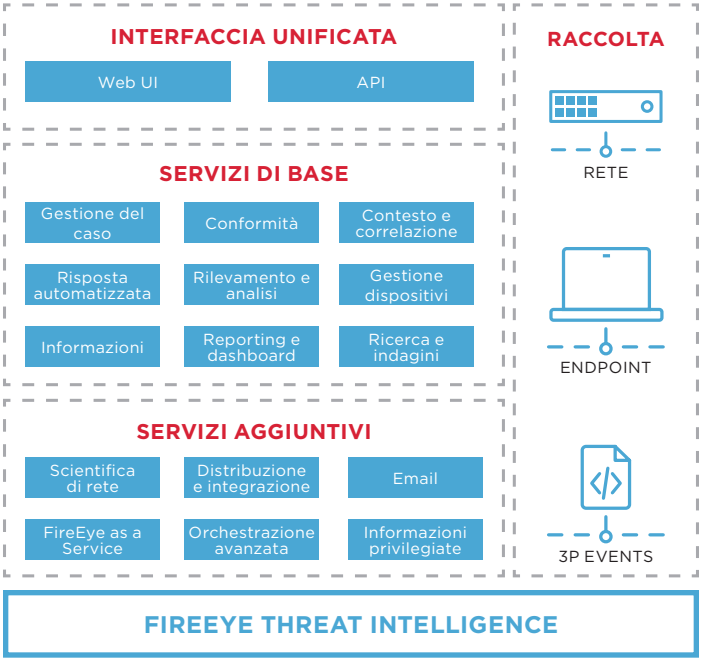

FIGURA 1. HELIX A COLPO D'OCCHIO

FireEye Helix si integra e potenzia gli strumenti di sicurezza esistenti con la correlazione automatica, playbook pre-costruiti e contesto FireEye iSIGHT Intelligence per aiutarti a definire la priorità degli avvisi più rilevanti e indagare e rispondere alle minacce più velocemente che mai.

CARATTERISTICHE

ANALISI Scopri modelli nascosti e anomalie nei tuoi dati per arricchire ulteriormente il rilevamento e fornire contesto per il processo investigativo.	**API** Supporta API aperte e flessibili per l'integrazione in prodotti di terze parti e negli ambienti del cliente.	**CONTESTO** Unisci automaticamente i dati correlati per prendere decisioni più rapide, tra cui contesto su informazioni, avvisi, host e dati degli utenti.
CONFORMITÀ Dashboard predefinite o personalizzate e widget per aggregare, presentare ed esplorare visivamente le informazioni più importanti per un utente, rispettando sempre i requisiti di conformità.	**RILEVAMENTO** Rilevamento multi-vettore con motore MVX; applica regole comprovate FireEye e FireEye iSIGHT Intelligence ai dati esistenti per identificare le minacce che altri non individuano.	**GESTIONE POLITICHE E DISPOSITIVI** Gestisci configurazioni, politiche e stato di integrità di tutto l'ambiente.
CONTROLLO DI ACCESSO BASATO SUI RUOLI Crea gruppi basati sui ruoli e assegna autorizzazioni granulari per accedere alla console.	**INFORMAZIONI** Rileva, arricchisci, esplora e conosci le ultime informazioni sulle minacce da FireEye, con guasti per paese e settore.	**ORCHESTRAZIONE** Automatizza e accelera il processo investigativo e la risposta tramite integrazioni di prodotto e azioni definite per avvisi specifici.
WORKBENCH INVESTIGATIVO Indicizza, archivia, cerca e analizza il malware rispetto agli avvisi e ai dati degli eventi da tutte le fonti in tutta l'infrastruttura per supportare un passaggio flessibile e una soluzione rapida.	**GESTIONE DEL FLUSSO DI LAVORO** Organizza, assegna, collabora e prendi iniziative attraverso il processo di indagine attraverso flussi di lavoro automatizzati e manuali.	**VISIBILITÀ DEGLI ENDPOINT** Proteggiti dalle minacce degli endpoint e dagli exploit che utilizzano la visibilità investigativa, comportamentale e informativa.

Per maggiori informazioni su FireEye, visitate il sito:
www.FireEye.com

A PROPOSITO DI FIREEYE, INC.

FireEye è leader nella sicurezza come servizio basato sulle informazioni. Fungendo da estensione semplice e scalabile delle operazioni di sicurezza del cliente, FireEye offre un'unica piattaforma che fonde tecnologie di sicurezza innovative, informazioni sulle minacce a livello nazionale e i servizi di consulenza Mandiant®, rinomati in tutto il mondo. Con questo approccio, FireEye elimina la complessità e il peso della cybersicurezza per le aziende che hanno difficoltà a prepararsi, prevenire e rispondere agli attacchi informatici. FireEye ha oltre 5.000 clienti in 67 Paesi, tra cui più di 940 dei Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

© 2017 FireEye, Inc. Tutti i diritti riservati. FireEye è un marchio registrato di FireEye, Inc.
Altri marchi, nomi di prodotti e servizi sono o possono essere rivendicati
come proprietà di terzi. DS.FEH.IT-IT.022017