F-SECURE ELEMENTS

Più flessibilità, meno complessità.
L'unica piattaforma di sicurezza informatica di cui hai bisogno.

L'ambiente di business di oggi si evolve in modo rapido e costante. Lo stesso fanno le minacce informatiche. Le aziende di ogni settore si stanno spostando sul cloud e stanno adottando nuovi metodi digitali per lavorare. Allo stesso modo, i criminali sfruttano le superfici di attacco estese con metodi più avanzati ed efficienti.

Un modo diffuso per rispondere alle nuove minacce è raccogliere tutta una serie di complesse tecnologie e soluzioni specializzate da vari fornitori. Si tratta di un approccio disordinato da un punto di vista operativo ma anche di una scelta pericolosa per la postura di sicurezza.

- Molte di queste soluzioni richiedono competenze notevoli (e rare) per un utilizzo efficace.
- Le soluzioni frammentate non collaborano né condividono dati l'una con l'altra e questo porta a silos e funzionalità di detection ristrette.

F-Secure Elements offre una piattaforma di sicurezza all-in-one e flessibile che si adatta ai cambiamenti nel panorama aziendale e delle minacce. È una piattaforma unificata e clpoud-native che copre tutte le aree critiche della catena di valore della sicurezza: Vulnerability Management, Endpoint Protection, Endpoint Detection and Response e Protezione di Microsoft 365. Scegli tecnologie complementari stand-alone con flessibilità o ottieni il pacchetto completo: la scelta è tua

- **Un singolo pannello:** ottieni visibilità senza precedenti e piena consapevolezza della situazione.
- **Integrazione perfetta:** le soluzioni condividono un data lake e collaborano su vari vettori di attacco, offrendo eccezionali funzionalità di rilevamento.
- **F-Secure Elements Security Center:** uniforma le operazioni con una gestione centralizzata.
- **Piattaforma SaaS cloud-native:** nessun hardware o middleware. Adattamento e deployment con un click.
- **Servizio completamente gestito o software a gestione autonoma:** collabora con i nostri partner certificati o gestisci in locale. A prescindere dalla scelta, siamo a tua disposizione.

PERCHÉ F-SECURE ELEMENTS?

Flessibile. Modulare. Scalabile.
Scegli funzionalità stand-alone o passa alla suite completa in un solo click. Adattati rapidamente grazie alle opzioni di licenza flessibili.

All-in-one.
Riduci al minimo i rischi con una protezione unificata e all'avanguardia per l'intera catena di valore della sicurezza.

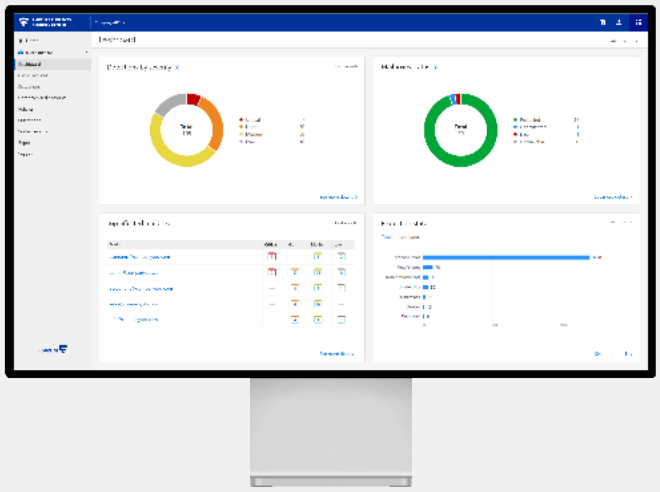
Consapevolezza della situazione.
Ottieni visibilità significativa. Comprendi gli attacchi complessi.

Risposta rafforzata.
Rispondi a più vettori di attacco su endpoint e cloud.

Gestione semplificata.
Migliora la produttività con una gestione semplice e centralizzata.

Leggero come una nuvola.
Riduci i tempi di deployment e i costi operativi con una progettazione pulita e cloud-native.

F-Secure



F-Secure Elements è la piattaforma all-in-one in cui tutto funziona perfettamente insieme:

- **Visibilità dell'intera superficie di attacco** e dei vettori critici, senza silos.
- **Gestione automatizzata delle patch** che protegge dallo sfruttamento delle vulnerabilità.
- **Prevenzione proattiva** da malware e ransomware moderni.
- **Sicurezza cloud avanzata** per l'ambiente Microsoft 365.
- **Contenimento rapido degli attacchi** con azioni di risposta guidate e automatizzate, accompagnate da supporto on-demand 24/7 da parte di esperti threat hunter.
- **Rilevamenti istantanei e chiari** per le minacce più complesse.
- Con threat intelligence in tempo reale e analisi per identificare minacce nuove ed emergenti entro pochi minuti dalla loro creazione.

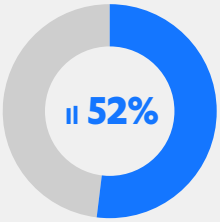
F-SECURE ELEMENTS ENDPOINT PROTECTION

Pionieri della protezione da malware e ransomware moderni.

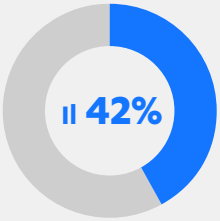
I criminali analizzano costantemente i dispositivi connessi alla ricerca di vulnerabilità non corrette e non si lasceranno scappare alcuna opportunità. La maggior parte delle minacce informatiche può essere bloccata con una soluzione di protezione degli endpoint efficace e un'applicazione rigorosa delle patch.

F-Secure Elements Endpoint Protection ti offre una protezione pluripremiata per bloccare le minacce moderne, da ransomware e malware mai visti prima fino ad exploit di vulnerabilità "zero day". Ottieni una copertura di sicurezza completa per dispositivi mobili, desktop, laptop e server. Una maggiore precisione significa meno interruzioni di business e meno lavoro richiesto all'IT per il ripristino. Gli avvisi con filtri e gli elevati livelli di automazione assicurano la massima efficienza. Risparmia risorse per le attività più importanti.

- **Protezione autonoma** sempre disponibile per ridurre il lavoro manuale o le competenze richieste.
- **Blocca le minacce e gli exploit invisibili** con analisi euristica e comportamentale, machine learning avanzato e threat intelligence in tempo reale.
- **Distribuisci patch di sicurezza quando vengono rilasciate** con una gestione completamente automatizzata.
- **Blocca l'esecuzione di applicazioni e script** in base alle regole create dai nostri penetration tester o definite dal tuo amministratore.
- **Impedisci agli utenti di cadere vittima delle minacce online,** incluso l'accesso a siti web pericolosi.
- **Rileva il ransomware e impedisci distruzione** e manomissione dei dati con le tecnologie DeepGuard e DataGuard.
- **Impedisci alle minacce di introdursi nei sistemi o di estrarne dati** tramite dispositivi hardware.
- **Impedisci alle applicazioni pericolose di accedere a file e** risorse di sistema senza autorizzazione.



delle aziende ha subito un data breach negli ultimi due anni.

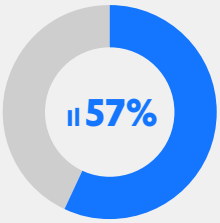


dei data breach nel 2020 si è verificato per la mancata applicazione di una patch disponibile.

F-SECURE ELEMENTS ENDPOINT DETECTION AND RESPONSE

Più veloce dei criminali. Resilienza contro gli attacchi avanzati.

Nessuno è immune alle minacce informatiche e la prevenzione perfetta non esiste. Gli attacchi moderni più sofisticati possono oltrepassare anche i controlli preventivi più robusti. Inoltre, possono essere difficili da rilevare, permettendo così ai criminali di prendersela comoda mentre causano disastri e utilizzi impropri dei dati.



delle organizzazioni non sa quali siano le vulnerabilità più pericolose.

F-Secure Elements Endpoint Detection and Response ti permette di respingere gli attacchi informatici avanzati e mirati con funzionalità di rilevamento leader di settore. Garantisci la resilienza e riassumi rapidamente il controllo con informazioni pratiche e linee guida chiare.

- **Ottieni visibilità in tempo reale** su ciò che sta accadendo negli endpoint. Telemetria per Windows, macOS e Linux.
- **Rileva le minacce in modo rapido e preciso** con Broad Context Detection. Rileva tutti i comportamenti sospetti, anche se sembrano sicuri. Ricevi tutti gli avvisi necessari.
- **Scova le minacce in modo efficiente** con la ricerca e i filtri per gli eventi.
- **Comprendi le catene di eventi correlati** con visualizzazioni semplificate.
- **Reagisci istantaneamente alle minacce con azioni di risposta automatizzate** incluso l'isolamento degli host basato sui rischi.
- **Contieni gli attacchi** con linee guida chiare e pratiche e la possibilità di inoltrare i casi complessi ai nostri esperti 24/7.
- **Soddisfa i requisiti normativi** PCI, HIPAA e GDPR che richiedono la segnalazione di violazioni entro 72 ore.

F-SECURE ELEMENTS FOR MICROSOFT 365

Protezione multi-livello per rilevare e bloccare le minacce avanzate e gli attacchi di phishing.

I dati oggi sono tutto. Le email aziendali contengono numerose informazioni riservate e confidenziali. Gli storage in cloud come Microsoft SharePoint sono una miniera d'oro di proprietà intellettuale. Gli account email aziendali sono spesso collegati a varie applicazioni business critical. Le credenziali degli utenti che finiscono in mano ai criminali aprono le porte a furti di identità e accesso ai sistemi dell'azienda.

Microsoft 365 è il servizio email più usato al mondo. La sua popolarità spinge i criminali a progettare metodi per oltrepassare i controlli di sicurezza standard di Microsoft. La sicurezza email di base di Microsoft non offre difese adeguate contro gli attacchi avanzati o i tentativi di phishing più complessi.

F-Secure Elements for Microsoft 365 rafforza le funzionalità di sicurezza native di Microsoft per proteggere dagli attacchi di phishing complessi e dai contenuti malevoli presenti in email, calendari, attività e SharePoint. Le funzionalità avanzate di detection includono il rilevamento di anomalie nelle caselle postali e compromissione degli account email. Questa soluzione cloud-native è progettata per Microsoft 365 e rappresenta un'estensione perfetta delle soluzioni di sicurezza degli endpoint Elements.

- **Assicura la continuità di business in modo conveniente** con un approccio multi-livello.
- **Protezione costante** a prescindere dal dispositivo di accesso dell'utente finale. Nessuna interruzione o disservizio del gateway email.
- **Semplifica i flussi di lavoro** con una gestione di sicurezza unificata per endpoint e cloud.

ELEMENTI DISTINTIVI DELLA PIATTAFORMA:

Proteggi endpoint e ambienti cloud

Blocca malware e ransomware

Rileva e correggi le vulnerabilità

Rileva e scova le minacce

Blocca phishing e minacce avanzate su Microsoft 365

Rileva gli account aziendali violati

Rispondi rapidamente agli attacchi con automazione, linee guida e supporto 24/7

- **Deployment senza problemi** con una perfetta integrazione cloud-to-cloud. Nessuna **necessità di middleware o configurazioni estese.**
- **Blocca i contenuti malevoli** inclusi malware, ransomware e tentativi di phishing.
- **Rileva anche il malware più complesso** eseguendo e analizzando file sospetti in un ambiente sandbox isolato.
- **Rileva se gli account aziendali sono stati compromessi** con informazioni complete su come, cosa, quando e gravità.
- **Fidati della tua casella postale. Rileva anomalie comportamentali** come regole di inoltro malevole.
- **Accelera l'efficienza** con le scansioni automatizzate.

> "
> Abbiamo scelto le soluzioni F-Secure anziché una soluzione SIEM perché il loro sistema di rilevamento comportamentale delle applicazioni basato su machine learning ha ridotto drasticamente il numero di falsi allarmi e presentava gli avvisi che facilitavano molto analisi e decisioni.
>
> **Jeovane Monteiro Guimarães, IT Supervisor, Móveis Itatiaia**

F-SECURE ELEMENTS VULNERABILITY MANAGEMENT

Visualizza e conosci la tua reale superficie di attacco.

Gli ambienti IT aziendali, dinamici e complessi, portano a superfici di attacco più ampie. I criminali cercano sempre opportunità per sfruttare sistemi senza patch e cercare di accedere senza autorizzazione per carpire informazioni preziose. Ogni giorno vengono rilasciate nuove patch di sicurezza e l'applicazione tempestiva è fondamentale per proteggere i dati e la continuità di business. Il miglioramento della postura di sicurezza informatica inizia dalla conoscenza di asset e configurazioni.

F-Secure Elements Vulnerability Management identifica gli asset dell'organizzazione, rileva le vulnerabilità e le lacune più critiche. Riduci al minimo superficie d'attacco e rischi. Trova i punti deboli interni ed esterni prima degli altri.

- **Visibilità olistica** e mapping preciso di tutti gli asset, i sistemi, le applicazioni e lo shadow IT.
- **Riduci la superficie di attacco** identificando i sistemi gestiti e non gestiti, i software e le configurazioni errate vulnerabili.
- **Riduci i rischi** prendendo misure predittive e preventive prima che si verifichino incidenti.
- **Uniforma i flussi di lavoro** con analisi pianificate automatizzate. Assegna le priorità alla remediation con i punteggi di rischio integrati.
- **Espandi l'analisi delle vulnerabilità ai dispositivi remoti** al di fuori della rete con l'agent per endpoint Windows.
- **Mostra e giustifica il tuo valore** nel mantenere la continuità di business con report standard e personalizzati su postura e rischi di sicurezza.
- **Soddisfa i requisiti di conformità normativa** con una soluzione di scansione delle vulnerabilità certificata PCI ASV e report personalizzati.

F-Secure

SERVIZI DI SUPPORTO:

HEADLINE	ADVANCED	PREMIUM
Supporto nelle ore lavorative locali (inglese, finlandese, francese, tedesco, giapponese e svedese)	✓	✓
Accesso prioritario al supporto tecnico	✓	✓
Strumenti online per ticket e follow-up	✓	✓
Telefonata e ricontatto	✓	✓
Chat e supporto remoto		✓
Supporto 24/7 (inglese)		✓
Risposta agli incidenti critici entro un'ora		✓
Escalation a livello di management		✓
Consulenza per upgrade		✓
Consigli sulla rimozione del malware		✓

Siamo a tua disposizione. I pacchetti di supporto aggiuntivi offrono servizi completi e fluidi per garantire l'operatività. Disponibili come Advanced e Premium.

Conosciamo la sicurezza informatica: 30 anni di esperienza nella lotta alla criminalità informatica con un approccio basato su ricerca, comprovati da una consolidata storia di valutazioni indipendenti.

PCI MITRE | ATT&CK AV-TEST AWARD

Prova tu stesso

f-secure.com/elements | twitter.com/fsecure_it | linkedin.com/f-secure

F-Secure