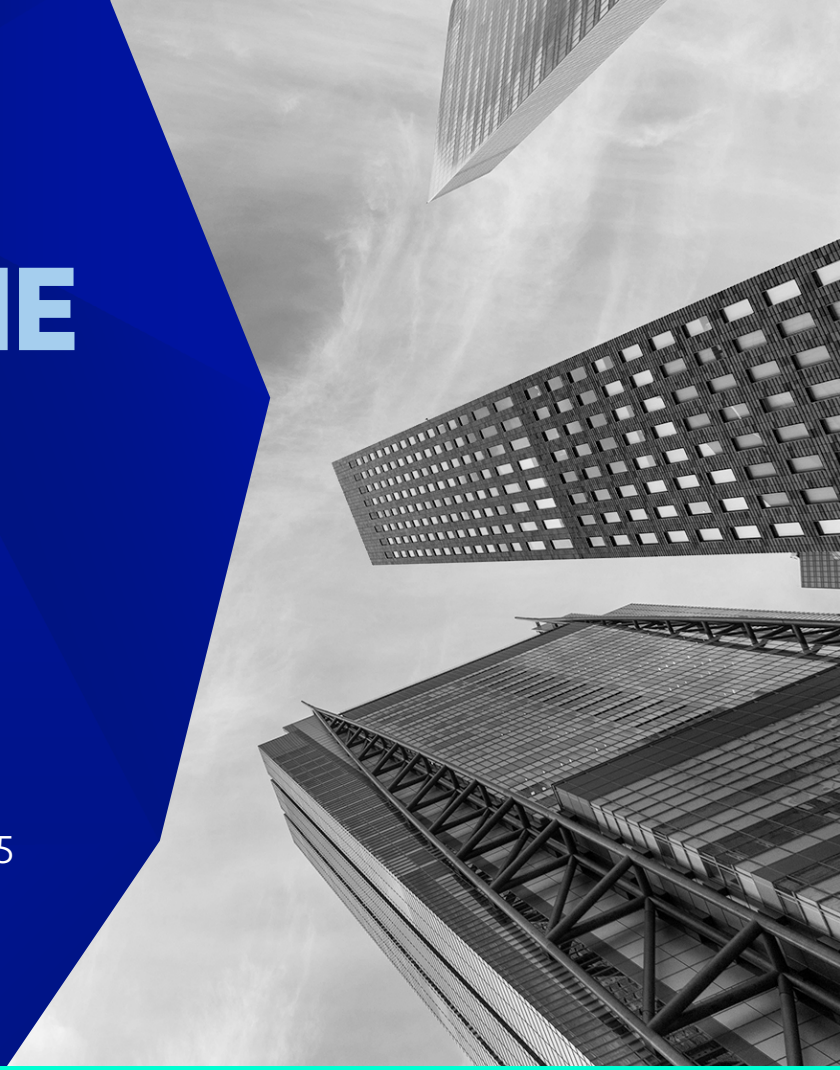
F-Secure

PROTEZIONE CONTRO PHISHING E MINACCE VIA EMAIL

F-Secure Elements for Microsoft 365



PANORAMICA

È responsabilità di un'organizzazione verificare che la propria soluzione di email in cloud offra meccanismi di difesa contro raggiri, social engineering, contenuti malevoli e attacchi mirati. Tuttavia, identificare e gestire queste potenziali lacune è una sfida complessa per qualsiasi azienda.

Per ridurre i rischi delle email in cloud, è importante utilizzare una soluzione specifica che offra i tassi di rilevamento più alti possibile per proteggere gli utenti dalle minacce. Inoltre, una soluzione che fornisce sicurezza dagli endpoint al cloud è più conveniente e facile da gestire.

La crescita costante del numero di utenti che si affidano alla posta elettronica di Microsoft 365, sta attirando l'attenzione dei criminali, che progettano e testano i loro attacchi in modo da non essere rilevati dalla sicurezza standard di Microsoft.

Microsoft 365

Microsoft 365 è il servizio cloud più diffuso, con 180 milioni di caselle postali aziendali

I metodi di attacco sono testati e progettati espressamente per non essere rilevati dalle misure di sicurezza Microsoft standard

Tramite Microsoft 365 vengono lanciate campagne di phishing insolitamente convincenti ai danni di aziende di qualsiasi dimensione

VANTAGGI PRINCIPALI

INTERRUZIONI DI BUSINESS RIDOTTE AL MINIMO

Offre sicurezza basata sulla tecnologia di threat intelligence di F-Secure, leader di settore, con protezione da contenuti malevoli non rilevati dalla protezione standard dell'email di Microsoft 365.

NON SOLO PROTEZIONE EMAIL

Tutti i tipi di contenuti, inclusi email, inviti del calendario e attività, vengono analizzati alla ricerca di contenuti pericolosi.

SCELTA CONVENIENTE

Offre una scelta conveniente per funzionalità di sicurezza avanzate come il sandboxing.

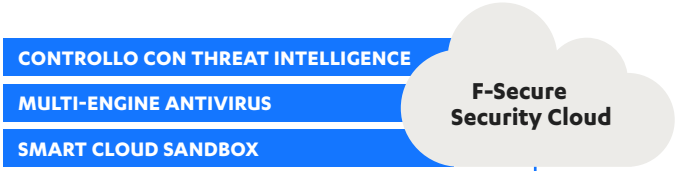
DEPLOYMENT IN CLOUD IN POCHI MINUTI

Sfrutta l'integrazione cloud-to-cloud che non richiede l'installazione di middleware o software ed è estremamente veloce da implementare e facile da gestire.

UNA SOLUZIONE INTEGRATA

Insieme alle funzionalità EDR e di protezione degli endpoint di F-Secure, offre una protezione più completa rispetto a qualsiasi soluzione dedicata unicamente alla sicurezza della posta elettronica.

F-SECURE SECURITY CLOUD



F-Secure Security Cloud è il nostro servizio di analisi e rilevamento delle minacce basato su cloud. Utilizza un sistema di threat intelligence in tempo reale che raccoglie dati 24/7 da decine di milioni di sensori di sicurezza nel mondo. Rappresenta il fulcro dei nostri prodotti innovativi e pluripremiati*.

CONTROLLO CON THREAT INTELLIGENCE
Grazie alla threat intelligence in tempo reale raccolta da decine di milioni di sensori, possiamo identificare le minacce nuove ed emergenti entro pochi minuti dall'esordio, garantendo una protezione eccezionale dalle minacce in continua evoluzione.

ANTIVIRUS MULTIMOTORE
Quando un file è sconosciuto, F-Secure Security Cloud lo sottopone a un'analisi più approfondita. Vari motori antimalware, comportamentali ed euristici, si completano a vicenda nella ricerca di malware, exploit "zero day" e modelli di minacce avanzate e attacchi mirati.

SMART CLOUD SANDBOX
I file sospetti sono sottoposti a ulteriori analisi in Smart Cloud Sandbox, che li esegue in diversi ambienti virtuali e monitora il comportamento per rilevare attività malevole.

*AV-Test e AV-Comparatives 2010-2019

SICUREZZA PER L'UTENTE

ANALIZZA
I contenuti vengono sottoposti a varie fasi di analisi in base al profilo di rischio.

FILE E URL
I file e gli URL malevoli vengono inviati e ricevuti da M365 in varie forme, come email, inviti e note.

O365 EXCHANGE
F-Secure Elements for Microsoft 365 è connesso e autorizzato a monitorare tutte le attività di Exchange senza impatto sull'utilizzo dell'email.

M365
La soluzione, quindi, sottopone attività e contenuti sospetti a un processo brevettato di analisi e rilevamento delle minacce supportato da F-Secure Security Cloud.

RILEVA
I contenuti non sicuri vengono automaticamente eliminati o messi in quarantena, il loro utilizzo viene bloccato e gli utenti ricevono linee guida sul da farsi.

Rileva gli account email compromessi con informazioni complete su come, cosa, quando e gravità.

INTERVIENI
Grazie a reporting dettagliato, analisi di sicurezza e audit trail completi, gli amministratori possono rispondere agli incidenti in modo efficace.

SANDBOXING

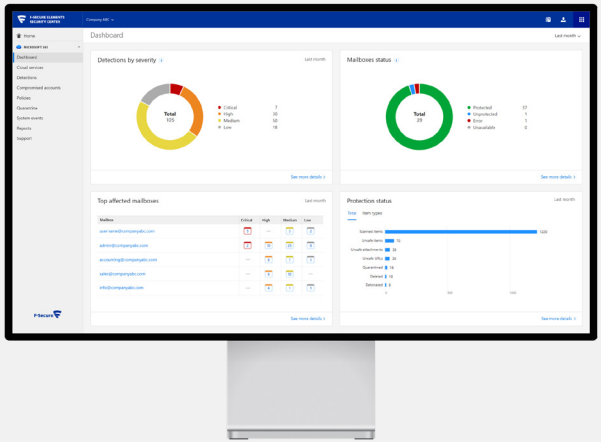
F-Secure Security Cloud utilizza un'analisi dei contenuti in più fasi in un processo sequenziale generato in base al profilo di rischio del contenuto. Inoltre, i file ad alto rischio vengono sottoposti a un'analisi più approfondita con la nostra tecnologia di sandboxing cloud.

TRACCIAMENTO GLOBALE DEL COMPORTAMENTO DEL MALWARE

I prodotti di sicurezza F-Secure usano servizi di reputazione per il riconoscimento delle minacce. Il software client calcola un hash crittografico per un oggetto ed esegue una query di rete con Security Cloud. Questo processo ci offre una visione granulare della distribuzione globale del software e della diffusione dei programmi malevoli. Security Cloud ci permette di esaminare il comportamento globale dei programmi malevoli sospetti e come si diffondono fra computer, paesi e continenti.

ANALISI AUTOMATIZZATA

Per rimanere al passo con l'odierno panorama delle minacce in rapida evoluzione, sono necessari strumenti come elaborazione automatizzata e analisi del malware. Grazie al feed di analisi, Security Cloud è in grado di classificare una quantità considerevole di nuovo malware in modo veloce ed automatico. Questa automazione ci permette di rispondere rapidamente alle nuove minacce.



AMMINISTRAZIONE

F-Secure Elements for Microsoft 365 offre visibilità completa sull'utilizzo di Microsoft 365. Tutti gli avvisi di sicurezza relativi a contenuti malevoli o sospetti trovati nelle caselle postali degli utenti sono accessibili su F-Secure Elements Security Center in una comoda vista a tabelle. Elements Security Center offre un unico pannello per tutta la piattaforma unificata. Le informazioni vengono presentate in modo chiaro per offrire piena consapevolezza della situazione sui vari livelli di sicurezza.

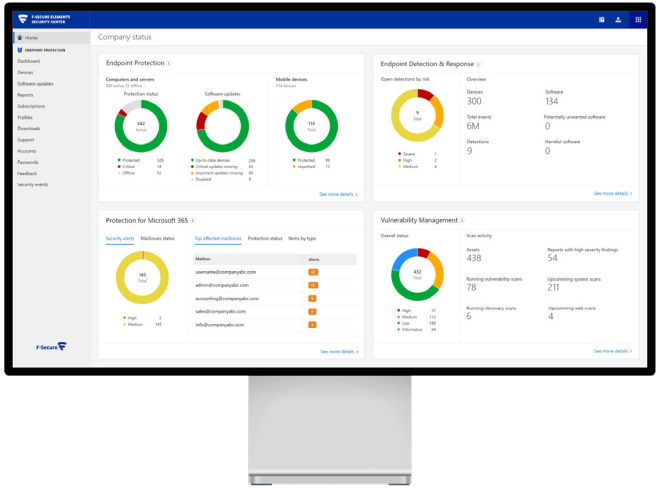
Questa tabella è ricercabile e ordinabile con facilità in base a varie colonne e criteri. La vista di quarantena nel portale di gestione consente agli amministratori di visualizzare, rilasciare o eliminare gli elementi in quarantena in base alla necessità. L'amministratore può anche usare diversi criteri di ricerca e ordinamento per regolare e affinare la vista durante la gestione dell'elenco degli elementi in quarantena per gli ambienti gestiti.

Sono disponibili funzionalità avanzate di reporting per gli amministratori, che possono generare report sullo stato di sicurezza di un ambiente protetto in qualsiasi momento in un formato facilmente condivisibile.

F-SECURE ELEMENTS – PIÙ FLESSIBILITÀ, MENO COMPLESSITÀ. L'UNICA PIATTAFORMA DI SICUREZZA INFORMATICA DI CUI HAI BISOGNO

F-Secure Elements for Microsoft 365 è disponibile come soluzione stand-alone o come funzionalità integrate nella piattaforma di cyber security F-Secure Elements.

Prova tu stesso



INFORMAZIONI SU F-SECURE

Nessuno può vantare una visibilità sui cyber attacchi real-life maggiore di F Secure. Stiamo colmando il divario tra rilevamento e risposta, impiegando l'impareggiabile threat intelligence di centinaia dei migliori consulenti tecnici del settore, milioni di dispositivi che eseguono il nostro pluripremiato software e innovazioni incessanti nell'intelligenza artificiale. Le maggiori banche, compagnie aeree e imprese si affidano a noi per il nostro impegno volto a sconfiggere leminacce più potenti del mondo.

Insieme alla nostra rete costituita dai più importanti partner di canale e da oltre 200 service provider, il nostro obiettivo è fare in modo che ognuno disponga della cyber security di livello enterprise di cui tutti noi abbiamo bisogno.Fondata nel 1988, F-Secure è quotata sul listino NASDQA OMX Helsinki Ltd.

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

F-Secure