N-SOC
SECURITY AS A SERVICE

DENIED

SURFING DNS

CHE COS'È

È un servizio cloud-based che non necessita di hardware da acquistare o plugin software da installare. Protegge i PC e dispositivi della rete dalle minacce online ed aiuta a migliorare l'efficienza e la produttività lavorativa dei dipendenti.

COME SI ATTIVA

Grazie alla tecnologia in cloud, N-SOC Surfing DNS è non invasivo e semplice da attivare, senza alcun bisogno di configurazione o installazione sui dispostivi o l'intervento di un operatore, perché gestito interamente da N-SOC.

PERCHÈ ATTIVARLO

Le difese perimetrali tradizionali sono inefficaci per contrastare gli attacchi dinamici, dato che si basano su una serie di analisi che seguono un set predeterminato di regole e i cui risultati emergono dal confronto con signature di comportamento. Il malware e gli attacchi che evadono questi controlli non possono, così, essere individuati: ad esempio è sufficiente che l'attacco si basi su un algoritmo in grado di generare rapidamente nuovi indirizzi non censiti dal sistema di protezione tradizionale per rendere inefficace questi layer di difesa.

Aggiunge un layer alle tradizionali difese perimetrali

Tutte le richieste DNS vengono inoltrate al servizio, che riconosce e blocca l'accesso a destinazioni indesiderate o pericolose, mitigando i rischi e tutelando l'operatività.

COME FUNZIONA

Tutte le richieste DNS vengono inoltrate al servizio N-SOC Surfing DNS che riconosce e blocca l'accesso a destinazioni web inappropriate e insicure. In questo modo si ottiene semplicemente ed efficacemente la protezione e la gestione centralizzata anche per le infrastrutture decentrate.

La piattaforma N-SOC effettua un controllo per ogni richiesta su un database costantemente aggiornato di domini/IP infetti o utilizzati da hackers. Sulla base del controllo effettuato, tutte le richieste dirette a queste destinazioni vengono inibite e l'utente è avvertito con un messaggio di blocco.

Blocca i link di phishing e la pubblicità online in quasi tutte le forme, come gli annunci contestuali, video e annunci audio, banner e pop-up che, il più delle volte, sono il veicolo di infezione preferito dal malware.

Blocca tutti i siti web indesiderati o inappropriati, come la pornografia, la violenza, l'odio o il razzismo, armi, alcol e droghe, gioco d'azzardo e le altre categorie tra cui si può scegliere. Si basa su un database costantemente aggiornato in cui sono censiti oltre 100 milioni di siti web (miliardi di pagine web) suddivisi in più di 55 categorie.

TUTELA LEGALE & CONFORMITA'

Una delle esigenze sempre più sentite sia dalle Imprese che dalla Pubblica Amministrazione è quella di controllare e limitare il traffico verso determinati siti internet per aumentare la produttività dei propri dipendenti, per ridurre gli effetti dannosi indotti (inserimento nelle liste di spamming, download di software pericoloso) e ridurre la probabilità che vengano commessi crimini informatici da dipendenti interni, oltre che ottimizzare l'utilizzo della banda di connessione ad internet.

Filtro dei contenuti evoluto e costantemente aggiornato, in grado di proteggere gli utenti prevenendo le infezioni malware, phishing, conforme alle normative italiane ed europee GDPR sulla privacy ed aderente alle linee guida, in ambito di sicurezza informatica, per la PA. Immediato e semplice da attivare e gestire.

Adatto alle aziende senza una soluzione di protezione navigazione

Il servizio Surfing DNS protegge la navigazione senza introdurre costi di acquisto, implementazione e gestione di hardware o software.

o per chi vuole ridurre i rischi

Il servizio Surfing DNS attiva un ulteriore livello di sicurezza che mitiga il rischio di infezione, incrementa la produttività e preserva l'uso di internet.

I VANTAGGI

Grazie al servizio N-SOC Surfing DNS potrai:

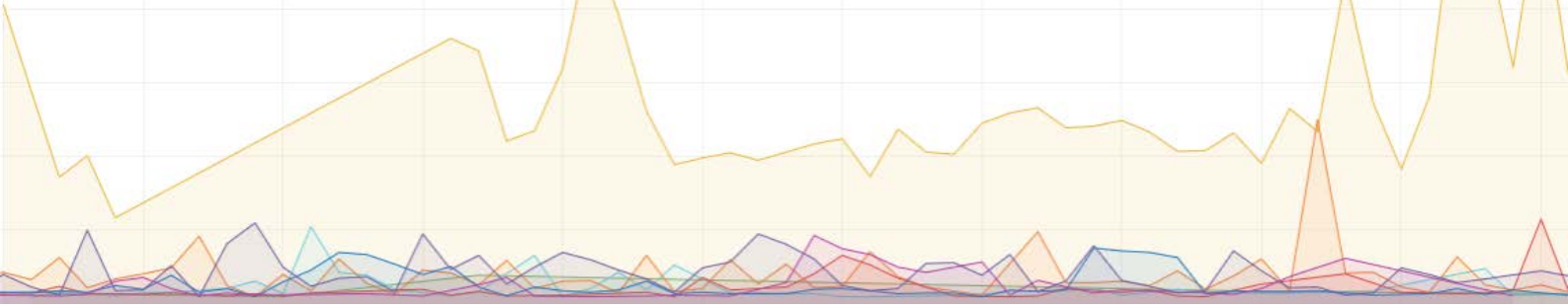
- *visualizzare un report realtime con l'evidenza dei sistemi compromessi nella rete (es: APT, botnet) e i tentativi bloccati di accesso ai domini maligni o non desiderati. N-SOC attinge le informazioni dal proprio network di honeypot e da molteplici fonti real-time di feed per garantire un elevato livello di protezione sempre aggiornato rispetto all'evoluzione delle minacce;*
- *gestire l'accesso degli utenti della tua rete ad internet inibendo l'accesso ai siti pornografici ed in genere a tutti i siti non autorizzati, per evitare la responsabilità dell'azienda in caso di atti illeciti;*
- *migliorare la produttività aziendale;*
- *preservare l'uso della banda per attività lavorative;*
- *prevenire l'infezione dei sistemi degli utenti;*
- *zero impatto sulle performance della rete;*
- *attivare immediatamente una protezione semplice da gestire ed economicamente vantaggiosa;*

NON necessita di installazione di client/agent sui dispositivi client

NON necessita di configurazioni complesse/invasive: è sufficiente "inoltrare" le richieste DNS al servizio N-SOC

Massima tutela della privacy: le richieste sono anonimizzate

Attivazione del servizio semplice, immediata e senza impatto sugli utenti ed amministratori



KEY FEATURES

- Tecnologia Cloud-based - non è necessario installare nessun software o appliance
- Protezione da APT e malware – individua ed interrompe le comunicazioni con i server C&C riducendo il rischio di trasferimento dei dati non autorizzato, bloccando, ad esempio, APT, Ransomware, come il Cryptolocker, phishing, etc
- Threat intelligence feed automatizzato - network proprietario di honeypot e molteplici fonti real-time di feed
- Protezione dagli attacchi veicolati tramite i messaggi pubblicitari
- Database di siti internet continuamente aggiornato
- Clientless - non comporta l'installazione di software sui dispositivi client degli utenti e sui server di rete; Non necessità di installazioni hardware
- Conformità - piena conformità alle normative vigenti in materia privacy e linee guida PA
- Flessibilità - licensing pay per use: la licenza è estremamente flessibile perché paghi con un canone mensile e senza vincoli contrattuali solo l'effettivo utilizzo
- Zero effort - non necessita dell'intervento di un operatore, viene tutto gestito da N-SOC
- Supporto di sicurezza per tutti i dispositivi - protezione di tutti i dispositivi e tutti i sistemi operativi connessi alla rete aziendale
- Trasparenza e semplicità di utilizzo - l'utente riceve un avvertimento nel caso di blocco di accesso al dominio/URL richiesto
- Servizio di security specialist 100% italiano - supporto tecnico sempre raggiungibile e disponibile, perchè gestito da un team di professionisti italiani
- Reporting real time – cruscotto in tempo reale semplice e chiaro per visibilità dei blocchi avvenuti

	max	avg ▾	current	total
DNS connections	41	7	7	406
SDNS queries processed	41	7	0	399
Reverse lookups	6	0	0	6
Non-existent domains	1	0	0	1

PERCHÈ N-SOC

- Team di specialisti della sicurezza di rete
- 100% focus sull'efficacia della soluzione
- 100% Italiani - Supporto tecnico specialistico
- Servizi indipendenti da vendor ed infrastruttura

Evita le conseguenze di un attacco:

PIÙ COSTI
per intraprendere azioni di risposta agli attacchi e bonifica dei sistemi

CLIENTI INSODDISFATTI
più effort per il mantenimento di clienti e partner

RIPERCUSSIONI SUL BUSINESS
impatto sul processo produttivo e sulla reputazione aziendale