CYBERSECURITY

UN NUOVO APPROCCIO STRUTTURALE

ALFACOD®


ALFACOD
ALFACOD®
sistemi di identificazione automatica
mobile computing

FORTINET

INTRODUZIONE

È normale per le aziende espandere i propri networks digitali per stare al passo con le crescenti richieste del mercato. Come naturale conseguenza di questa crescita, aumentano di pari passo le esigenze di sicurezza delle reti stesse. Ma il panorama della sicurezza odierno è molto diverso da quello che era anche solo pochi anni fa, poichè i rischi si sono accumulati.

I seguenti fattori di cambiamento rendono questo argomento molto rilevante quando si pensa all'espansone strategica di un'impresa:

- rischi associati e il peso delle prestazioni dei dati crittografati in SSL
- Potenziamento del Cloud
- Le vulnerabilità derivanti dall'Internet of Things (IoT)
- L'aumento dei ransomware
- L'attuale carenza di competenze relative alla sicurezza IT

Mettere in sicurezza ambienti dinamici e distribuiti in queste condizioni, difficili richiede tecnologie di sicurezza fortemente integrate che condividano le informazioni, lavorino insieme per rilevare le minacce e sincronizzino risposte automatizzate in tempo reale.

01
COMPRENSIONE DELLA TENDENZA DELLE MINACCE PER L'IMPRESA

Per proteggere le imprese, dobbiamo innanzitutto capire cosa sta succedendo oggi nel panorama delle minacce e cosa è previsto per il futuro. Ci sono diverse questioni da prendere in considerazione quando si tratta di definire e progettare una strategia di sicurezza per un network di classe enterprise.

Dati crittografati in SSL: molte aziende devono crittografare determinati tipi di dati sensibili in transito, utilizzando il Secure Sockets Layer (SSL) per conformarsi alle normative di settore. Il traffico SSL occupa dal 35 al 50% del traffico di rete attuale, continuando a crescere ogni anno. Ma i criminali informatici possono anche usare la crittografia SSL per nascondere malware e ransomware alle tradizionali soluzioni di sicurezza aziendali. La decodifica SSL e il controllo del traffico con un sistema di sicurezza della rete tradizionale può sperimentare latenze e degrado delle prestazioni, che inficiano le attività aziendali. Di conseguenza, molte organizzazioni scelgono di non crittografare il traffico critico oppure di non ispezionare il traffico che viene crittografato.

Cloud: anche se la maggior parte dei fornitori di servizi cloud può offrirti una qualche sorta di protezione, le loro misure di sicurezza sono quasi certamente fuori dal controllo della tua azienda. La principale sfida per la sicurezza diventa quindi quella di stabilire e mantenere coerenti la policy e il rinforzo della sicurezza, mentre i dati vanno e vengono tra reti locali e ambienti cloud di terze parti. Dal momento che sempre più dati aziendali vengono archiviati in cloud unificati e spesso multi-proprietari, specialmente big data raccolti da dispositivi IoT, una attività fondamentale dovrebbe essere quella di fare in modo che quegli endpoints, quei dispositivi IoT e altri dispositivi periferici non diventino un condotto per l'iniezione di malware nel cloud.

IoT: molti prodotti IoT non sono assolutamente stati progettati pensando alla sicurezza. Spesso hanno protocolli di autenticazione e di autorizzazione deboli, software e firmware facilmente strumentalizzabili, sistemi di comunicazioni mal progettati e poche, o addirittura nessuna, configurazione di sicurezza. Una violazione del sistema IoT può diffondere malware, rubare dati sensibili e interrompere le attività aziendali. Nell'ambito di servizi ospedalieri, sistemi industriali importanti o servizi pubblici, non si può scendere a compromessi perchè le conseguenze potrebbero essere disastrose.

Ransomware: gli attacchi ransomware sono più che raddoppiati lo scorso anno. È probabile che le aziende continueranno a vedere aumentare gli attacchi contro obiettivi di importanza strategica (es. data center e sistemi di comunicazione) finalizzati a rubare e tenere in ostaggio proprietà intellettuali e dati sensibili. L'impatto non è solo economico, ma anche di immagine, legato all'esposizione pubblica negativa associata a questo tipo di incidenti, che può minare la fiducia dei consumatori e diminuire il valore del marchio. Per alcune organizzazioni, il fallimento nel prevenire adeguatamente attacchi

simili, può persino portare a cause legali.

Mancanza di competenze: attualmente stiamo affrontando a livello globale una grave carenza di professionisti specializzati in sicurezza informatica. Si stimano più di un milione di richieste di cybersecurity inevase in tutto il mondo. Oltre il 50% degli IT managers affermano che la carenza di personale dedicato alla cybersecurity ha aumentato il carico di lavoro sul personale esistente e il 35% è sceso a compromessi per riempiere ruoli con il giusto livello di abilità ed esperienza. Più della metà ha rivelato che le proprie aziende hanno sperimentato almeno un episodio spiacevole di sicurezza informatica dovuto alla mancanza di formazione sulla sicurezza e alla mancanza di personale dedicato.

02 L'APPROCCIO INFRASTRUTTURALE ALLA SICUREZZA

Un sistema di sicurezza aperto, end-to-end (scalabile e in grado di adattarsi alle mutevoli esigenze della rete) consente alle organizzazioni di affrontare l'intero spettro di sfide che affrontano attualmente durante tutto il ciclo di vita dell'attacco informatico. L'integrazione e l'interoperabilità dovrebbero non solo essere requisiti fondamentali di tutte le parti dell'infrastruttura, ma anche essere parte di qualsiasi politica o strategia di sicurezza di base.

Questa soluzione di security sarebbe in grado di distribuire in maniera coerente, orchestrare e rinforzare le policy attraverso domini diversi - inclusi lavoratori fuori sede, filiali/uffici commerciali, data center distribuiti geograficamente e reti cloud private o pubbliche. Dovrebbe:

- Coprire abbondantemente tutte le parti dell'azienda, seguendola nella propria crescita e nelle proprie mutazioni
- Fornire una protezione potente, senza compromettere le prestazioni della rete
- Intraprendere, come un unico sistema coeso, un'azione automatizzata e intelligente

Un approccio infrastrutturale alla sicurezza raggiunge sia in profondità che in estensione l'intera rete distribuita. Funziona come un sistema unificato che condivide elementi tra i componenti. La sua elevata interoperabilità tra tutte le varie soluzioni che proteggono questi domini distribuiti, fornisce una visibilità dettagliata anche nel contesto di reti che variano in maniera repentina.

Come risultato di questa accresciuta consapevolezza, il sistema può quindi fornire risposte rapide e coordinate alle minacce - permettendo a tutti gli elementi di scambiarsi rapidamente informazioni sui pericoli e coordinare azioni. Esso lancia, contro gli attacchi, difese sincronizzate basate sull'informazione in real-time di minacce globali o locali - isolando i dispositivi infetti, rimuovendo i malware, segmentando la rete, aggiornando le regole e generando nuove politiche.

03
LA SOLUZIONE SECURITY DI FORTINET

La soluzione di Security di Fortinet connette le principali tecnologie di sicurezza e networking - dai firewall ai contenuti e alle applicazioni di security atte a mettere in sicurezza gli access points - per la sicurezza integrata dell'intero network, sia esso locale o remoto, fisico o virtuale, cablato o wireless, nel dominio dell'azienda o in cloud. Si basa su tre attributi principali:

Ampiezza: la nostra soluzione di Security copre l'intera superficie a rischio di attacco. Gli amministratori hanno visibilità dell'intera infrastruttura, inclusi endpoints, dispositivi IoT, access points, elementi del network, data center, cloud e perfino applicazioni e dati stessi. Questo consente di mettere in sicurezza tutti i potenziali punti d'entrata, così come i segmenti interni al network dinamico. Una tale ampiezza e una visibilità così profonda garantiscono l'ottemperanza agli standard, aiutano a monitorare il traffico interno e i dispositivi connessi, prevengono accessi non autorizzati a dati e risorse riservati e controllano la diffusione di intrusi e malware.

Potenza: al giorno d'oggi le aziende non possono permettersi di sacrificare la protezione in cambio delle performance. La nostra soluzione di Security è stata progettata sulla tecnologia "Security Processor Unit" (SPU) di Fortinet - i processori più veloci e specifici dell'intero settore della Security. L'utilizzo di applicazioni specificamente rivolte alla Security aumenta drasticamente le performance e la scalabilità, per garantire che la protezione non ostacoli la produttività in nessun punto della rete. La soluzione di Security fornisce, in maniera perfettamente integrata, una grande sicurezza, dai dispositivi endpoint ai livelli di accesso al network, siano essi cablati o wireless. Questa soluzione può scalare da network molto piccoli e poco ramificati a data center e data campus più grandi, complessi e ad alta intensità di dati, garantendo inoltre protezione per cloud privati, ibridi e pubblici. Una tale potenza consente alle aziende di essere sempre in anticipo rispetto ai requisiti di larghezza di banda che aumentano sempre più rapidamente, evitando così che le attività di security impattino negativamente sulle performance del network.

Automatizzazione: dal momento che un attacco può compromettere un network in pochi minuti, la sola visibilità non è sufficiente. La nostra soluzione di Security compie azioni veloci e coordinate contro le minacce, consentendo agli elementi giusti all'interno dell'infrastruttura di scambiarsi rapidamente informazioni sulle minacce e sincronizzare le risposte. Il nostro approccio permette al network di individuare automaticamente e isolare in maniera dinamica i dispositivi e i segmenti della rete coinvolti, aggiornare le regole, rilasciare nuove procedure e rimuovere i malware. Questa struttura di Security, inoltre, fornisce soluzioni in grado di adattarsi dinamicamente ai cambiamenti di configurazioni del network, stabilisce e aggiorna le politiche all'interno del network man mano che i bisogni aziendali cambiano. Le misure e le contromisure di sicurezza sono erogate automaticamen-

te nel momento in cui vengono distribuiti lungo la rete nuovi dispositivi, carichi di lavoro e servizi. La soluzione di Security supporta anche le interfacce di programmazione di applicazioni (APIs) aperte e questo permette alle organizzazioni di integrare investimenti in sicurezza e networking all'interno della struttura di Security di Fortinet.

04
COME LE SOLUZIONI FORTINET AFFRONTANO LE MINACCE DI OGGI

Le differenti componenti della nostra soluzione di Security sono progettate per lavorare in sinergia al fine di affrontare le nuove minacce in cui le aziende di oggi si imbattono.

Firewall Enterprise: la nostra soluzione di Security prevede processi altamente performanti di de-crittografia SSL e di ispezione delle comunicazioni sia in entrata che in uscita lungo l'intero spettro di attacchi possibili. La soluzione è costruita attorno ai Firewalls Enterprise di Fortinet - per filiali, campus, data center e segmenti interni - il tutto interconnesso da un solo, unificato sistema operativo per un controllo e una distribuzione semplificati e coordinati.

Queste capacità forniscono le performance più elevate del settore, la difesa più sicura contro le minacce e supportano i codici cifrati imposti dal settore. La nostra soluzione Firewall Enterprise consente la segmentazione degli elementi del network, la gestione del traffico, dei dispositivi e la separazione dei dati per un controllo più intenso. Quindi, se un malware crittografato con SSL entra nel perimetro del network, non andrà lontano prima di essere individuato ed eliminato. Il Firewall Enterpise esegue anche l'ispezione SSL, decifrando il traffico per applicare i controlli di prevenzione delle minacce.

Cloud Security: la soluzione di Sicurezza di Fortinet è stata progettata per estendersi in profondità in diversi ambienti cloud, al fine di garantire politiche coerenti e rinforzare le risorse con accesso. All'interno dell'architettura di sicurezza unificata, i firewall virtuali possono essere distribuiti tra i cloud privati, pubblici e ibridi per creare una micro-segmentazione di tipo "nord-sud" e "est-ovest".

La soluzione di Security integra le applicazioni cloud in un ambiente più ampio, regolato da policy di sicurezza e conformità universali e gestito in totale trasparenza su tutta la superficie di attacco. Combinando il Cloud Security al firewall aziendale preesistente si estende la medesima potente sicurezza su vasta scala, nonché la stessa intelligenza e la mitigazione del rischio dinamico sia per le applicazioni situate nel cloud che per quelle installate in locale.

Secure Access: la nostra soluzione di Security va ben oltre la mera integrazione di sistemi di sicurezza. Il Secure Access di Fortinet estende le policy di sicurezza coordinate fino al limite della rete, sia cablata che wireless, dove risiedono dispositivi IoT altamente vulnerabili. Poiché i dispositivi IoT vengono distribuiti in modo pervasivo, è difficile garantire la gestione e la visibilità trasparente degli stessi. Molte soluzioni di tipo "point" e "platform" sono semplicemente incapaci di integrare tutti i device in una visione di gestione centralizzata, compreso il controllo dell'accesso e la risposta. Invece, la soluzione di Security di Fortinet può integrare tutti i diversi punti di accesso di una rete (endpoint, applicazioni, cloud e dispositivi IoT), indipendentemente dalla loro distribuzione, in una soluzione

end-to-end che copre tutte le diverse superfici di attacco.

Advanced Threat Protection (ATP): la lotta agli attacchi ransomware richiede una struttura di sicurezza che copra i diversi canali che i cybercriminali utilizzano per guadagnarsi l'entrata: link e allegati di posta elettronica, download di siti web, applicazioni aziendali, condivisione di social media e persino dispositivi IoT vulnerabili. In quanto parte dell'infrastruttura di Security, la soluzione Advanced Threat Protection di Fortinet può essere implementata in alcuni solamente o in tutti i punti di ingresso, con un rapido scambio di informazione globale, per impedire l'aumento dei ransomware, e uno scambio dinamico di informazioni locale, per contrastare le ultime campagne. Inoltre, l'interfaccia API rende possibile la condivisione di queste informazioni tra le componenti Fortinet e quelle non Fortinet, per una difesa senza soluzione di continuità tra i diversi elementi di sicurezza presenti all'interno dell'organizzazione.

I nostri componenti ATP lavorano insieme per scambiarsi reciprocamente oggetti e dati in modo automatico e costante, al fine di prevenire, rilevare e mitigare attacchi nell'intero ambiente e tra tutti i portatori di attacchi. Inoltre, sono in grado di monitorare le comunicazioni in uscita di comandi ransomware crittografati e comunicazioni di controllo, così come sofisticati malware che tentano di passare inosservati.

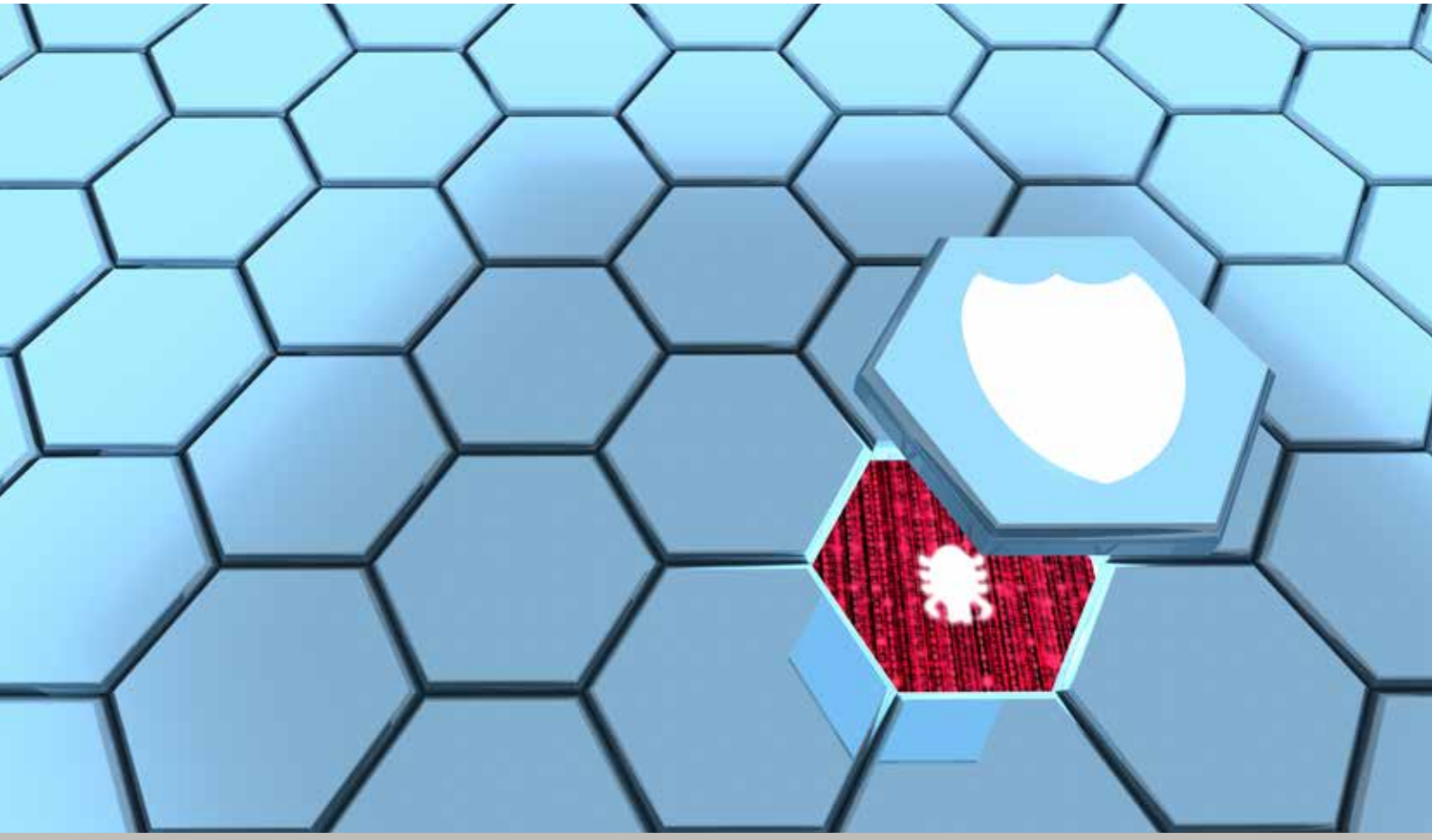
Security Operations: la visibilità flessibile della struttura di Security di Fortinet è un requisito importante per il team dedicato alle operazioni di sicurezza, incaricato di monitorare e reagire agli attacchi all'interno dell'organizzazione. Lo strumento Security Operations della soluzione di Security di Fortinet aiuta a gestire, monitorare e raccogliere analytics sui diversi componenti della rete da un solo punto di controllo - sia che essi includano diversi elementi dello stesso prodotto Fortinet, diversi prodotti Fortinet o diversi prodotti di altri costruttori. I report predefiniti aiutano a gestire la conformità agli standard attraverso l'infrastruttura aziendale.

Con l'aumento del numero e dell'aggressività delle minacce e l'incremento della complessità delle architetture di sicurezza, l'approccio della nostra soluzione di Security alle operazioni di sicurezza offre un'alternativa seria alle soluzioni di tipo "point" e "platform", che richiedono personale di cybersecurity addestrato e esperto su più prodotti e componenti di soluzioni. In questo modo si alleggerisce l'urgente bisogno di assumere specialisti di Security IT e, al tempo stesso, si consente al personale dedicato alla cybersecurity di dare il proprio contributo in maniera forte. La capacità di individuare automaticamente elementi collegati al network porta alla creazione di un database dinamico di gestione centralizzata (CMDB).

CONCLUSIONI

Le imprese si trovano ad affrontare cambiamenti senza precedenti in termini di tendenze nell'evoluzione della rete e un insieme di minacce che tendono a mimetizzarsi. Tuttavia, una soluzione di Security offre ai responsabili della sicurezza informatica una risposta coordinata e trasversale che può difendere, da un capo all'altro, tutte le infrastrutture.

La soluzione di Security di Fortinet presenta un approccio unico, che collega più soluzioni per formare un'ossatura di sicurezza unificata. Aiuta le aziende di oggi ad adattare dinamicamente le proprie infrastrutture IT in continua evoluzione, per difendere una superficie di attacco in rapida evoluzione.



WI-FI ENTERPRISE PERCHÉ FORTINET È DIVERSA DAGLI ALTRI

Per Fortinet, il coordinamento fra tuti gli attori che operano all'interno dell'infrastruttura radio è l'elemento chiave per un Wi-Fi di classe Enterprise. Vediamo di seguito quali sono le caratteristiche principali che differenziano il Wi-Fi Enterprise di Fortinet da tutti gli altri.

Singola cella virtuale (access point coordinati): tutti gli access point vengono configurati sul medesimo canale; i client sincronizzati non si disturbano; gli access point non comunicano tra di loro, la gestione è lasciata tutta alla controller. Analizzando una rete Fortinet si noterà che esiste un solo punto di accesso Wi-Fi, anche in presenza di tanti access point. La controller Fortinet, nel momento in cui si accorge che un device mobile si sta muovendo, sposta la virtual port da un access point all'altro, in maniera automatica, evitando che il segnale degradi. Il device che riceveva le risposte da un primo access point immediatamente, su decisione della controller, riceve le risposte da un altro access point.

Air Time Fairness (massima copertura, massima sicurezza): il Wi-Fi di Fortinet assegna la stessa quantità di tempo a tutti i client, dando ai dispositivi la capacità di trasmettere alla massima potenza. Nel Wi-Fi tradizionale questo non avviene. Spesso si verifica una sorta di contesa tra i client per cercare di avere accesso al mezzo. Il Wi-Fi di Fortinet, invece, utilizzando sempre il protocollo standard 802.11 fornisce in sostanza la stessa quantità di tempo a tutti i client, alcuni dei quali saranno in grado di andare molto veloce e in quel dato tempo trasmetteranno un'elevata quantità di dati, altri invece andranno più lentamente, trasmettendo nello stesso tempo un minor numero di dati, ma senza che si verifichino mai prevaricazioni.

PORTA VIRTUALE (roaming controllato): ogni client che si connette alla rete Fortinet ha a disposizione un access point virtuale dedicato, che viene generato su qualsiasi access point fisico in cui il client passerà. Sarà la controller a sincronizzare tra di loro tutti i virtual access point assegnati.

SCALABILITÁ (capacità di crescita in base alle necessità): è un altro punto di forza di Fortinet. Modificare o ampliare una rete Fortinet è molto semplice: si posiziona nel punto più appropriato un nuovo access point, che viene riconosciuto immediatamente dalla controller. Con la stessa facilità è possibile spostare un'intera rete Wi-Fi da un'azienda ad un'altra.

NOC & SOC PRESIDIO E ASSISTENZA ALFACOD

Un Network Operations Center (NOC) è un luogo in cui i tecnici IT monitorano e gestiscono costantemente da remoto infrastrutture ICT 24 ore al giorno, 365 giorni all'anno. In tal modo è possibile accorgersi di qualsiasi evento o criticità si verifichi sull'intero network e intervenire nella maniera più tempestiva per la risoluzione del problema.

Alla stregua del NOC, un Security Operations Center (SOC) consiste in una squadra di specialisti qualificati, che ha il compito di monitorare e migliorare constantemente la sicurezza informatica dell'azienda cliente, prevenendo attacchi e rispondendo prontamente agli episodi critici legati alla sicurezza informatica delle organizzazioni. Una volta adattatosi al contesto di business di cui è al servizio, definito l'obiettivo di sicurezza e il proprio ambito di competenza, il SOC progetta l'infrastruttura tecnologica a sostegno della propria attività.

Attraverso l'utilizzo di strumenti avanzati di monitoraggio, diagnosi e gestione ticketing, ogni operatore del NOC e del SOC è in grado in pochissimi secondi di accedere alla dashboard di controllo di qualsiasi infrastruttura venga gestita da remoto. Affidarsi a un Centro Operativo di monitoraggio e gestione di un network e della sua sicurezza significa avere sempre al proprio fianco un tecnico estremamente specializzato al quale chiedere aiuto o semplicemente conferma che tutto stia funzionando al meglio, in ogni momento.

La squadra di Alfacod dedicata alle attività di NOC e SOC è composta da diversi professionisti qualificati, per garantire fino a 3 livelli diversificati di supporto:

- L1: livello base, per il supporto e la risoluzione dei problemi comuni delle aziende, come semplici questioni di utilizzo, facendo fronte a richieste di help desk. Se la questione necessita di una competenza maggiore, si passa al livello successivo.

- L2: livello approfondito di risoluzione dei problemi, con analisi tecniche e supporto back end. Tecnici esperti e competenti valutano incidenti e problemi, fornendo soluzioni a questioni che non possono essere risolte attraverso il primo livello.

- L3: livello operativo avanzato. La squadra di Alfacod si compone di 8 esperti SME (Subject Matter Expert) multibrand. Questo gruppo si avvale del più alto grado di risorse tecniche, per la risoluzione delle situazioni critiche, riproducendole all'occorrenza in ambiente di laboratorio, per identificarne la causa scatenante.

Alfacod mette a disposizione un servizio di presidio e intervento 24 ore al giorno, 365 giorni all'anno sull'intero territorio nazionale, avvalendosi di collaboratori e stock di parti di ricambio dislocati in tutta Italia. Offre in parallelo un servizio autonomo di intervento e di gestione del risanamento degli assets delle imprese clienti, analizzando costantemente lo stato delle reti e inviando report programmati o su richiesta.

Alfacod amministra diversi data center, utilizzando i più innovativi sistemi di monitoraggio proattivo. Ad oggi arriva a gestire oltre 32.000 nodi di rete tra switch, firewall e router.

Per analizzare la situazione attuale della Tua Azienda o per qualsiasi ulteriore approfondimento, contatta la squadra specializzata di Alfacod.


NOC e SOC di Alfacod


NOC e SOC di Alfacod


ALFACOD
ALFACOD®
sistemi di identificazione automatica
mobile computing

FORTINET

ALFACOD®
sistemi di identificazione automatica
mobile computing

Il Gruppo Alfacod sviluppa soluzioni di identificazione automatica e tracciabilità dal 1986.
É considerato fra i maggiori esperti nella progettazione e realizzazione di architetture WiFi ad alta velocità, sistemi RFid, soluzioni di geolocalizzazione (RTLS e FGS), sistemi di automazione del fine linea, soluzioni di tracciabilità e rintracciabilità e vanta trent'anni di esperienza nel campo della stampa digitale.

GRUPPO ALFACOD

Sede di Bologna
via Cicogna, 83 - 40068 San Lazzaro di Savena (BO)
Tel. 051 4997211 / info-bo@alfacod.it

Sede di Milano
via San Cristoforo, 84 - 20090 Trezzano sul Naviglio (MI)
Tel. 02 90420055 / info-mi@alfacod.it

WWW.ALFACOD.IT