Tjänstebeskrivning och villkor IT-säkerhetspaket

InfraCom erbjuder omfattande IT-säkerhetstjänster som täcker alla aspekter av NIST Cybersecurity Framework: Identifiera, Skydda, Upptäck, Svara och Återställ.

Den här bilagan beskriver de tjänster som ingår i våra IT-säkerhetspaket Bas, Premium och Platinum SOC. I tjänstebeskrivningarna ingår även ansvarsfördelning mellan InfraCom och er som kund.

	Bas	Premium	Platinum SOC
Antivirus	Ja	Ja	Ja
Klienthantering på distans (RMM)	Ja	Ja	Ja
InfraCom Backup för Microsoft 365*	Ja	Ja	Ja
Mailskydd*		Ja	Ja
Ransomwareskydd		Ja	Ja
IT-säkerhetsträning (inkl. nätfisketester)*		Ja	Ja
Endpoint Detection & Response (EDR)		Ja	Ja
24/7/365 Security Operation Center			Ja

* Ej applicerbart för servrar eller industriella datorer.

Färgerna i diagrammet representerar de olika delarna av NIST Cybersecurity Framework:

Identify Protect Detect Respond Recover

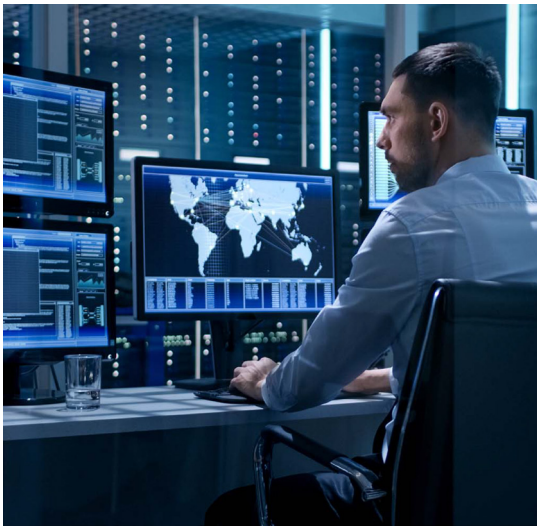
Åtgärdsnivåer för våra IT-säkerhetspaket

För att säkerställa att er verksamhet är skyddad mot IT-hot och attacker, erbjuder vi olika åtgärdsnivåer anpassade efter era behov. Nedan följer en beskrivning av åtgärdsnivåerna som ingår i våra tre IT-säkerhetspaket.

IT-säkerhet Bas

Åtgärdsnivån i Bas-paketet innebär att systemenställs på autopilot och agerar utifrån sin egen logik. Dessutom finns möjlighet att skicka automatiserade rapporter till er som kund där det är möjligt.

Med Bas-paketet ställs högre krav på er egen kunskap för att bedöma eventuella IT-hot och attacker.



IT-säkerhet Premium

Utöver det som ingår i Bas-paketet, så hanteras ärenden av erfarna IT-säkerhetstekniker och en noggrann granskning av ärendet eller larmet sker under kontorstid (8-17).

Med den här nivån kan ni som kund överlåta en stor del av den aktiva hanteringen av er IT-säkerhet, vilket ger er mer tid att fokusera på er egen verksamhet.

IT-säkerhet Platinum SOC

I vårt mest omfattande IT-säkerhetspaket ingår allt som ingår i Premium-paketet, med skillnaden att ärenden hanteras av erfarna IT-säkerhetstekniker dygnet runt, alla dagar om året.

Insatser vid kritiska åtgärder, såsom risk för intrång eller attack, som sker under helgdagar och utanför ordinarie kontorstider debiteras löpande med 1995 kr/h. Under ordinarie kontorstid debiteras enligt IT-taxa nivå 5 (all tid debiteras per påbörjad timme).

Med nivå Platinum SOC får er verksamhet ett IT-säkerhetsteam tillgängligt dygnet runt, året om, vilket ger er tryggheten att sova gott på natten och veta att er IT-miljö är i säkra händer.

Stöd för användare och olika typer av enheter

IT-säkerhetspaketen kan anpassas för tre olika kategorier av enheter: användare, servrar och industriella datorer (IPC). Varje kategori har olika förutsättningar och behov, vilket påverkar vilka tjänster som inkluderas. Det framgår av tjänstens namn i avtalet vilken enhetstyp som avses.

Användare: Avser skydd för företagets användare och deras datorer. För användare med fler än en dator går det att lägga till extra klientdatorer.

Server: Avser skydd för företagets servrar, både fysiska och virtuella.

Industriell dator (IPC): Avser datorer med särskilda krav, exempelvis i produktionsmiljöer där enheter inte alltid är uppkopplade.

För servrar och Industriella datorer ingår allt utom de användarfokuserade tjänsterna InfraCom Backup för Microsoft 365, Mailskydd och IT-säkerhetsträning.

Övergripande villkor för IT-säkerhetspaket

InfraCom använder fysiska, tekniska och administrativa skyddsåtgärder som är utformade för att hjälpa till att säkra tjänsten mot oavsiktlig eller obehörig förlust, åtkomst eller avslöjande. Dock kan inget system för dataöverföring, lagring eller hämtning göras helt ogenomträngligt och trots de åtgärder som används, garanterar inte tjänsten skydd mot alla säkerhetshot eller andra sårbarheter. Kunden godkänner att tjänsten används på egen risk.

Under inga omständigheter ansvarar InfraCom för fysiska, administrativa eller tekniska kontroller som ligger under Kundens ansvar, inklusive men inte begränsat till hantering av åtkomstuppgifter (t.ex. lösenord), nätverksanslutning och internetanslutning.

Kunden åtar sig att:

1. Regelbundet ändra lösenord och andra åtkomstuppgifter till tjänsten samt omedelbart vidta åtgärder vid misstanke om obehörig åtkomst eller annan kompromettering.
2. Omedelbart tillämpa alla uppdateringar, uppgraderingar, ändringar eller förbättringar som InfraCom bedömer som nödvändiga eller lämpliga för att upprätthålla säkerhet, sekretess, integritet, tillgänglighet eller prestanda för tjänsten.

För att säkerställa korrekt debitering för antal användare och klientenheter förbehåller sig InfraCom rätten att justera eventuella avvikelser om dessa inte överensstämmer med det faktiska antalet i kundens miljö.

Villkor tredjepartsapplikationer

Delar av tjänsten tillhandahålls genom en tredjepartsapplikation som licensieras från tredje part. InfraCom förvärvar en licens till mjukvaran och förmedlar denna vidare till Kunden. InfraCom hanterar driften av mjukvaran och säkerställer att de senaste uppdateringarna är installerade.

Mjukvaran utgörs av en insticksmodul som installeras som en plugin i Kundens dator. Vid en attack mot insticksmodulen påbörjas omedelbart försök att identifiera och avbryta aktiviteten. Enheten isoleras och ett ärende registreras i ärendehanteringssystemet som hanteras av InfraComs Support.

För att tjänsten ska fungera krävs att Kunden godkänner de villkor som framgår av Kaseya Subscription End User License Agreement (EULA):
https://www.kaseya.com/legal/kaseya-end-user-license-agreement-eula/

Kunden är medveten om och accepterar att InfraCom, utöver ovan nämnda åtgärder, inte ansvarar för eventuell skada hänförlig till tredjepartsapplikationer. Kaseyas ansvar i förhållande till slutanvändare framgår av EULA.

Antivirus - Skydda er IT-miljö

Med ett antivirusprogram säkrar ni datorn från skadlig programvara.

Vad gör ett antivirusprogram?

Antivirusprogram är nödvändiga för att skydda enheter från kända hot. De upptäcker och reagerar på skadlig programvara på en infekterad dator eller server. Antivirusprogrammet uppdateras regelbundet för att skydda från nya kända hot.

Krav för integration med övriga tjänster

- Tjänsten är ett tillägg till InfraComs övriga supporttjänster eller ingår som en del i InfraComs säkerhetspaket
- Tjänsten aktiveras på samtliga enheter i kundens miljö och kan inte installeras på enskilda enheter.
- Tjänsten kräver installation av InfraComs RMM (Remote Monitoring and Management)-klient

Teknisk beskrivning av tjänsten

Tjänsten hanterar virus och stoppar kända virushot. Detta gör den dygnet runt, 365 dagar om året.

InfraCom konfigurerar och installerar antivirusprogramvaran mot en kostnad.

Uppdatering av antivirusprogramvaran sker löpande.

Ansvarsfördelning

För att tjänsten ska fungera optimalt krävs det att både InfraCom och ni som kund samarbetar, tabellen visar hur ansvaret fördelas baserat på olika uppgifter som behöver utföras.

Uppgift	InfraCom	Kunden
Justering av antal prenumerationer för antivirus		Ja
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter för konfigurering av antivirus		Ja
Uppsättning av tjänsten	Ja	
Se till att antivirusprogrammen är i drift på avtalade datorer och servrar samt kontakta er som kund vid eventuella avbrott	Ja	
Informera InfraCom vilka klienter som ska ha tjänsten installerad samt när en dator tas ur bruk och tjänsten ska avinstalleras		Ja
Tillhandahålla en teknisk kontakt på plats för grundinstallation		Ja

Klienthantering på distans (RMM)

Genom att installera RMM-programvaran på användarnas datorer skapas en miljö för effektiv IT-support och säkerhetsarbete.

Vad är RMM?

RMM betyder Remote Monitoring and Management. Det är en programvara som kontinuerligt övervakar alla anslutna enheter. Genom att identifiera och åtgärda problem innan de påverkar verksamheten hjälper RMM till att minimera avbrott och säkerställer att systemen är tillgängliga när de behövs.

RMM gör det möjligt för InfraCom att agera proaktivt, vilket betyder att problem ofta kan lösas innan de ens märks av kunden. Kontinuerlig övervakning och automatiska uppdateringar säkerställer att kundens IT-system är skyddade mot säkerhetshot och virus, vilket är särskilt viktigt i en tid med ökande cyberhot.

Krav för integration med övriga tjänster

- Tjänsten är ett tillägg till InfraComs övriga supporttjänster eller ingår som en del i InfraComs säkerhetspaket.
- Tjänsten skall aktiveras på samtliga enheter kundens miljö, och kan inte installeras på enskilda enheter.

Teknisk beskrivning

RMM övervakar kontinuerligt servrar, datorer, nätverksutrustning och andra system. Den samlar in data om prestanda, säkerhet, och andra kritiska parametrar, och larmar om till exempel en klient inte har genomfört rätt uppdateringar och därmed utgör en säkerhetsrisk för verksamheten.

Programvaran används också av InfraComs support för att utföra underhåll, felsökning och uppdateringar på distans utan att behöva vara på plats hos kunden. InfraCom konfigurerar och installerar RMM mot en kostnad. Behövs hjälp på plats för att installera RMM hos användarna tillkommer timkostnad för detta.

Ansvarsfördelning uppgifter	InfraCom	Kunden
Justering av antal prenumerationer för RMM		Ja
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter samt åtkomst för konfiguration av tjänsten		Ja
Uppsättning av tjänsten	Ja	
Se till att RMM är i drift på avtalade klienter	Ja	
Informera InfraCom vilka klienter som ska ha tjänsten installerad samt när en dator tas ur bruk och tjänsten ska avinstalleras		Ja
Tillhandahålla en teknisk kontakt på plats för grundinstallation		Ja

InfraCom backup för Microsoft 365

Skydd för e-post, filer, OneDrive och SharePoint från virus och ransomware samt felaktigt borttagna filer. Tjänsten lagrar er data ”för evigt” så länge ni har tjänsten aktiv!

Varför behövs en backuptjänst?

När organisationer flyttar mer data till molnapplikationer, tror många att traditionella rutiner som datasäkerhetskopiering inte längre behövs. Molntjänster är ju alltid tillgängliga, så varför säkerhetskopiera?

Svaret är enkelt: de flesta dataförluster beror på användarfel, som oavsiktlig radering eller dataintrång. InfraCom Backup för Microsoft 365 skyddar och återställer er organisations e-post, kalendrar, kontakter, OneDrive och SharePoint-filer från virus och ransomware. Det säkerställer också att felaktigt borttagna filer eller data som förstörts av angripare kan återställas och användas som vanligt.

Er organisations data sparas så länge ni prenumererar på tjänsten!

Krav för integration med övriga tjänster

- Tjänsten kräver en av backuptjänsten supporterad licens för Microsoft 365.
- Tjänsten kräver att InfraCom ges korrekta administratörsrättigheter till kundens Microsoft 365-miljö.
- Tjänsten installeras på hela Microsoft 365-tenanten, inte på enskilda användare.

Teknisk beskrivning av tjänsten

InfraCom konfigurerar backuplösningen mot en kostnad och backup körs 3 ggr dagligen.

Uppsättningen konfigureras på ett smart sätt och lägger automatiskt till backup för nya användarkonton och delade resurser. Alla backuper avseende användarkonton arkiveras även vid borttagning av Microsoft 365-licens, borttagning av arkiverad backup beställs manuellt.

Återläsningen är designad att på ett snabbt, enkelt och säkert sätt återställa filer utan risk för problem med namnkonflikter eller oavsiktlig borttagning av filkopior under återläsningens gång.

Vid en eventuell begäran av återläsning kontaktar kunden InfraComs support. Återläsning och användaradministration faktureras löpande.

Konfiguration för backuplösningen dokumenteras i InfraComs dokumentationssystem.

Backupperioder och utfasning av data

Backup tas som en ögonblicksbild 3 gånger om dagen. Om ni skapar och tar bort en fil under tiden mellan backuperna kommer filen inte bli sparad i en backup.

- När en backup är 30 dagar sparas 1 av de 3 dygnsbackuper som gått den första månaden.
- När en backup är 90 dagar sparas 1 backup per vecka.
- När en backup har sparats i ett år går backupen över till att spara 1 gång per månad.

Ansvarsfördelning uppgifter	InfraCom	Kunden
Justering av antal prenumerationer för tjänsten		Ja
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter för konfigurering av tjänsten		Ja
Uppsättning av tjänsten	Ja	
Se till att backuptjänsten är i drift för kundens Microsoft-tenant	Ja	
Tillhandahålla en teknisk kontakt på plats för grundinstallation		Ja

InfraCom mailskydd

InfraCom mailskydd är en avancerad hotskydds- och spamfiltrerande lösning som upptäcker okända skadliga malwareprogram vid dess första attack mot Microsoft 365, vilket förkortar tiden för upptäckt och hjälper till att stänga hot.

Robust analysfunktion och rapportering med InfraCom mailskydd

Vi kan snabbt och enkelt analysera detaljerna om varje skadligt objekt; e-post, fil eller länk som skyddet har flaggat. Från denna rapportering kan vi som leverantör beskriva vad som har hänt. Vi kan analysera varför objektet flaggades som skadligt, flödet och de tekniker som används för att försöka kringgå skyddande lösningar.

Exempel på hot som stoppas:

Det finns olika kategorier av information för varje skadligt objekt beroende på typen av attack och de specifika tekniker som används.

- **Skadlig lösenordsskyddad fil**: filer som kräver ett lösenord för att komma åt dem (främst PDF eller ZIP-filer).
- **Skadlig nyttolast**: finns främst i e-postbilagor och kan vara ofarlig under en tid tills den utlöses.
- **Macro Malware**: utnyttjar VBA-programmering (visuell basic för applikationer) i Microsoft 365-makron för att sprida virus, maskar och andra former av skadlig kod.
- **WMI-kommando**: kan användas för att interagera med lokala och fjärranslutna system för att utföra farliga funktioner, såsom att samla information för upptäckt och fjärrkörning av filer som en del av lateral rörelse.
- **Ladda ner en fil från webben**: kommer att visa om någon internetanslutning gjordes och om en nyttolast laddades ner och varifrån, så domänen och/eller IP-adressen kommer att vara synlig för användaren.
- **Excel4Macro**: Excel4Macro använder inbyggda funktionsanrop som EXEC för att köra filer. Tjänsten visar vilka API:er som används, vilket ger användaren insikt i vad Excel4Macro försöker göra.

Krav för integration med övriga tjänster

- Tjänsten är ett tillägg till InfraComs övriga supporttjänster eller ingår som en del i InfraComs säkerhetspaket.
- Tjänsten aktiveras på hela Officemiljön, och kan inte installeras på enskilda användare.
- Tjänsten kräver installation av InfraCom backup för Microsoft 365.

Teknisk beskrivning av tjänsten

InfraCom hanterar driften av mjukvaran samt säkerställer att de senaste uppdateringarna är installerade om en attack inträffar påbörjas direkta försök till att identifiera aktiviteten, objektet sätt i karantän och ett ärende skickas till ärendehanteringssystemet som hanteras av InfraComs Support. Åtgärder och felavhjälpning och rapport efter eventuell attack debiteras löpande och sker kontorstid om inget annat har avtalats.

Ansvarsfördelning uppgifter	InfraCom	Kunden
Justering av antal prenumerationer för tjänsten		Ja
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter för konfigurering av tjänsten		Ja
Uppsättning av tjänsten	Ja	
Kontinuerlig objektscanning	Ja	
Tillhandahålla en teknisk kontakt på plats för grundinstallation		Ja

InfraCom Ransomwareskydd

Minska spridning av ransomware genom isolering av klienten.

Vad är ransomware?

Ransomware, eller utpressningsprogram, är en typ av skadlig programvara som krypterar filer eller låser tillgången till en dator eller ett nätverk och sedan kräver en lösensumma för att återställa åtkomsten. Den som drabbas får vanligtvis ett meddelande som informerar dem om att deras data har blivit krypterade eller att deras system är låst och att de måste betala en viss summa pengar, oftast i kryptovaluta som Bitcoin, för att få tillbaka information.

Hur fungerar Ransomware detection?

När ransomware har upptäckts kommer tjänsten att påbörja ett stopp av attacken genom att automatiskt stoppa processen och isolera den berörda enheten från nätverket. Tjänsten isolerar klienten vid eventuell attack som skyddar mot spridning i företagets miljö. Detta gör den 24/7 365 dagar om året.

Krav för integration med InfraComs IT-tjänster

- Tjänsten är ett tillägg till InfraComs övriga supporttjänster eller ingår som en del i InfraComs säkerhetspaket.
- Tjänsten aktiveras på samtliga enheter i ovan nämnda tjänster, och kan inte installeras på enskilda enheter.
- Tjänsten kräver installation av InfraComs RMM-klient (Remote Monitoring and Management).

Krav för integration med kundens IT-miljö

- Tjänsten kräver internetåtkomst med lämpligt brandväggsskydd.
- Tjänsten kräver operativsystem som supporteras av Microsoft.

Teknisk beskrivning av tjänsten

InfraCom hanterar driften av mjukvaran samt säkerställer att de senaste uppdateringarna är installerade. Om en attack inträffar påbörjas direkta försök till att identifiera och avbryta aktiviteten, enheten isoleras sedan och ett ärende skickas till ärendehanteringssystemet som hanteras av InfraComs Support.

Åtgärder och felavhjälpning efter eventuell attack debiteras löpande och sker kontorstid om inget annat har avtalats

Ansvarsfördelning uppgifter	InfraCom	Kunden
Justering av antal prenumerationer för tjänsten		Ja
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter för konfigurering av tjänsten		Ja
Uppsättning av tjänsten	Ja	
Löpande uppdatering av ransomewareskyddet	Ja	
Informera InfraCom vilka klienter som ska ha tjänsten installerad samt när en dator tas ur bruk och tjänsten ska avinstalleras		
Tillhandahålla en teknisk kontakt på plats för grundinstallation		Ja

IT-säkerhetsträning för organisationen

Stärk er organisations förmåga att hantera och förebygga IT-säkerhetshot.

Vad är utbildning inom IT-Informationssäkerhet?

Utbildning inom IT-Informationssäkerhet är en lösning som kombinerar en phishing/nätfiskesimulator med en dynamisk utbildningsplattform. Med denna lösning kan ni testa och träna era anställda i att känna igen och hantera olika typer av phishing/nätfiske-attacker, som är ett av de vanligaste och farligaste hoten mot er organisations IT-säkerhet. Phishing/nätfiske är en metod som kriminella organisationer använder för att lura mottagare att klicka på skadliga länkar, dold kod inbäddat i media, öppna infekterade bilagor eller lämna ut känslig information. Phishing kan leda till dataintrång, ransomware, identitetsstöld, bedrägerier och andra konsekvenser som kan skada er verksamhet, era kunder och leverantörer.

En av de största utmaningarna med att skydda sig mot phishing är att det inte räcker med att ha tekniska lösningar, som antivirusprogram, brandväggar eller kryptering. Det krävs även att de som använder IT-systemen har kunskap och medvetenhet om hur man undviker att bli lurad av falska meddelanden. Mänskliga faktorn är ofta den svagaste länken i säkerhetskedjan, och därför är det viktigt att investera i utbildning och träning av era anställda.

Hur fungerar utbildning inom IT-Informationssäkerhet?

Utbildning inom IT-Informationssäkerhet fungerar genom att skicka ut simulerade phishing-mejl till era anställda, som ser ut som riktiga meddelanden från trovärdiga avsändare. Dessa mejl innehåller olika typer av lockbeten, som erbjudanden, fakturor, varningar eller uppmaningar att logga in på någon tjänst. Om en anställd klickar på en länk, öppnar en bilaga eller svarar på ett mejl, registreras detta som ett misstag och användaren får omedelbar feedback och utbildning om hur man undviker att göra om det i framtiden.

Utbildningen består av korta, interaktiva och engagerande lektioner som varar mellan 3-6 minuter och som behandlar olika aspekter av IT-säkerhet, som phishing, lösenordshantering, dataskydd, fysisk säkerhet och mer. Utbildningen anpassar sig efter varje användares kunskapsnivå och prestation, så att de får den mest relevanta och effektiva inlärningen. Vi rekommenderar att denna tjänst kompletteras med återkommande kvartalsgenomgångar som grundas på rapporterna.

Vilka är fördelarna med utbildning inom IT-Informationssäkerhet?

- Utbildning inom IT-Informationssäkerhet ökar era anställdas kunskaper och medvetenhet om IT-säkerhet, vilket minskar risken för att de blir offer för phishing och andra hot.
- Utbildning inom IT-Informationssäkerhet förbättrar er organisations IT-säkerhetskultur, genom att skapa en positiv och kontinuerlig inlärningsprocess som främjar en skeptisk och ansvarsfull inställning till säkerhet.
- Utbildning inom IT-Informationssäkerhet hjälper dig att efterleva GDPR-kraven om att era anställda ska ha kunskap om IT-säkerhetsfrågor och hur de ska hantera personuppgifter på ett säkert sätt.
- Utbildning inom IT-Informationssäkerhet ger dig insikt och översikt över er organisations säkerhetsstatus, genom att generera rapporter och statistik om era anställdas beteende, framsteg och resultat.

Krav för integration med InfraComs tjänster

- Tjänsten aktiveras på samtliga användare och kan inte aktiveras på enskilda användare.

Krav för integration med Kundens IT-miljö

- Tjänsten kräver internetåtkomst med lämpligt brandväggsskydd.
- Tjänsten kräver att InfraCom ges korrekta administratörsrättigheter till kundens IT-miljö.

Teknisk beskrivning av tjänsten

Phishing-simuleringar skickas med viss frekvens till anställda. Ni kan spåra vilka anställda som har klickat på länkar i phishing-mejlet, öppnat en bilaga eller gett bort sitt lösenord. När riskabla beteenden identifieras levererar vår plattform engagerande utbildningsvideor till användarna. Varje video åtföljs av en quiz för att testa behållandet av utbildningsinnehållet. Automatisk rapportering låter dig övervaka pågående framsteg samt analysera och demonstrera värdet av IT-säkerhetsutbildningen.

Anpassade IT-säkerhetsutbildningar eller kundanpassade uppsättningar/rapporter kan skapas och faktureras i dessa fall löpande.

Ansvarsfördelning uppgifter	InfraCom	Kunden
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter samt åtkomst för konfigurering av tjänsten		Ja
Uppsättning av tjänsten	Ja	
Utskick av Phising-mail, kvartalsvis eller enligt överenskommelse	Ja	

Endpoint Detection & Response (EDR)

Det enda sättet att skydda sig mot AI-drivna attacker är att identifiera anomalier i er organisations IT-miljö.

Vad är EDR?

Endpoint Detection and Response (EDR) är en avancerad säkerhetslösning för datorer och servrar. Den övervakar kontinuerligt enheterna, samlar in data och analyserar den för att upptäcka och reagera på hot. EDR kan avsluta skadliga processer och isolera angripna enheter vid behov.

Vad är skillnaden mellan Antivirus och EDR?

Antivirusverktyg skyddar enheter från kända hot genom att upptäcka och reagera på skadlig programvara. Men eftersom de förlitar sig på att känna igen tidigare identifierade hot, kan nya eller okända attacker undgå upptäckt. Detta gör organisationer sårbara för ransomware, skadlig programvara, stöld av inloggningsuppgifter och andra IT-attacker.

EDR erbjuder ett mer omfattande skydd genom att kontinuerligt övervaka och analysera systembeteenden. Denna lösning kan upptäcka misstänkt aktivitet och automatiskt vidta åtgärder för att neutralisera hot. EDR registrerar och lagrar systembeteenden, analyserar dem för att identifiera avvikelser och svarar på hot som antivirusprogram kan missa. Dessutom fortsätter EDR att analysera, upptäcka, undersöka, rapportera och varna IT-säkerhetsteamet om potentiella hot. EDR inkluderar även skydd mot ransomware.

Vad är ransomware?

Ransomware, eller utpressningsprogram, är en typ av skadlig programvara som krypterar filer eller låser tillgången till en dator eller ett nätverk och sedan kräver en lösensumma för att återställa åtkomsten. Den drabbade får vanligtvis ett meddelande som informerar om att deras data har blivit krypterade eller att deras system är låst, och att de måste betala en viss summa pengar, oftast i kryptovaluta som Bitcoin, för att få tillbaka informationen.

Hur fungerar Ransomwareskyddet?

När ransomware har upptäckts kommer tjänsten att påbörja ett stopp av attacken genom att automatiskt stoppa processen och isolera den berörda enheten från nätverket. Tjänsten isolerar klienten vid eventuell attack som skyddar mot spridning i företagets miljö. Detta gör den 24/7, 365 dagar om året.

EDR Ransomware Rollback - Återställningsfunktion

Ransomware Rollback är en ny, innovativ funktion som ingår i EDR och som ger dig sinnesro när ni vet att ni kan få tillbaka era filer, intakta som de var före incidenten, när en ransomware-attack slår till.

Lösningen fungerar genom att fånga upp filsystemförändringar som görs av applikationer och sedan sparas de ändringar som görs. Om en fil t.ex. byter namn, raderas eller uppdateras registrerar systemet dessa ändringar och lagrar de i en avgränsad katalog på användarens hårddisk.

Till skillnad från andra EDR-applikationer som erbjuder liknande rollback-funktioner, förlitar sig EDR med Ransomware Rollback inte på Windows skuggkopia, som ofta är målet för ransomware-attacker. Detta säkerställer att era filer och data är säkra även från de mest avancerade IT-attackerna.

Här är en sammanfattning av informationen om EDR:s Ransomware Rollback-funktion:

- Återställning av filer: Med ett klick kan man snabbt återställa krypterade filer till deras tidigare tillstånd, vilket gör återställningsprocessen enkel och effektiv.
- Affärskontinuitet: Funktionen säkerställer att verksamheten kan fortsätta som vanligt efter en ransomware-attack.
- Snabb återställning: EDR:s Rapid Rollback-metod tillåter företag att snabbt återställa filer efter större oönskade förändringar.

InfraCom rekommenderar att denna tjänst kompletteras med SOC.

Behövs både Antivirus och EDR?

Vanliga antivirusprodukter fungerar för att stoppa kända hot och bör alltid användas för att skydda enheter, men eftersom de är baserade på kända hot misslyckas de ofta med att upptäcka mer sofistikerade attacker som idag ofta är AI-drivna.

EDR lägger till ett flertal viktiga lager av säkerhetgenom att upptäcka misstänkta beteenden och ge varningar. EDR kan integrera med antivirusprogram och andra säkerhetsfunktioner, vilket ger ett mer fullständigt skydd för er organisation mot de ökade IT-säkerhetsriskerna, som ökar dag för dag.

Krav för integration med InfraComs tjänster

- Tjänsten är ett tillägg till InfraComs övriga supporttjänster eller ingår som en del i InfraComs IT-säkerhetspaket.
- Tjänsten skall aktiveras på samtliga enheter i kundens miljö, och kan inte installeras på enskilda enheter. Tjänsten kräver installation av InfraComs RMM-klient (Remote Monitoring and Management).

Krav för integration med Kundens IT-miljö

- Tjänsten kräver internetåtkomst med lämpligt brandväggsskydd.
- Tjänsten kräver att InfraCom ges korrekta administratörsrättigheter samt åtkomst till kundens IT-miljö.

Teknisk beskrivning av tjänsten

InfraCom konfigurerar och installerar EDR-tjänsten mot en kostnad. Tjänsten skyddar klienten vid eventuell attack och förhindrar mot spridning i företagets IT-miljö 24/7 365 dagar om året!

När en incident inträffar registreras detta per automatik i ett ärendehanteringssystem och hanterasav InfraComs Support. InfraCom supportundersökeroch rapporterar. Åtgärder och felavhjälpning sker kontorstid om inget annat har avtalats. Arbete med återställning från attacken sker mot löpande debitering.

Ansvarsfördelning uppgifter	InfraCom	Kunden
Justering av antal prenumerationer för EDR		Ja
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter samt åtkomst för konfigurering av tjänsten		Ja
Uppsättning av tjänsten	Ja	
Löpande uppdatering av EDR-programvaran	Ja	
Tillhandahålla teknisk kontakt för installation		Ja

24/7/365 Security Operation Center

Stoppa avancerade hot idag genom att låta vårt team av avancerade IT-säkerhetsexperter övervaka er verksamhet dygnet runt.

Vad är en SOC?

Ett Security Operation Center, dvs ett säkerhetsoperationscenter, är en omfattande säkerhetslösning som inkluderar en grupp av experter, processer och teknik för att upptäcka, undersöka och svara på säkerhetsincidenter. Det är som att ha ett dedikerat säkerhetsteam som övervakar nätverket och enheterna för tecken på skadlig aktivitet.

Vad får man?

Säkerhet för datorer och servrar - Skydda er organisations datorer och servrar med händelseloggövervakning, avancerad upptäckt av intrångsförsök eller skadliga filer.

Nätverkssäkerhet - Skydda nätverket med brandvägg och EDR (End point Detection & Response) integrerad med skydd för hot i realtid, DNS-information och varningar för eventuella attacker.

Säkerhet för molntjänster - Säkra molnet med Microsoft 365-säkerhetsloggövervakning, Azure AD-övervakning, Microsoft 365-skadlig inloggning och övergripande Secure Score.

IT-Säkerhetsexperter hanterar och spårar hot 24/7

Vårt team av IT-säkerhetsexperter jagar, agerar och samarbetar med dig som kund när hot upptäcks. Tjänsten inkluderar:

- Kontinuerlig övervakning - Dygnet skydd med identifiering och analys av hot i realtid.
- Avancerad plattform - optimerad så att er organisation snabbt kan försvara sig mot förödande cyberhot.
- Intrångsdetektion - Vi fångar sofistikerade och avancerade hot.
- Ett IT-säkerhetsteam - som proaktivt motverkar skadliga aktiviteter så att ni kan fokusera på affären och sova gott om natten.
- Inga hårdvarukrav - Patentansökt, molnbaserad teknik eliminerar behovet av kostsam och komplex lokal hårdvara.

Krav för integration med InfraComs tjänster

- Tjänsten är ett tillägg till InfraComs övriga supporttjänster eller ingår som en del i InfraComs säkerhetspaket.
- Tjänsten skall aktiveras på hela organisationen.

Krav för integration med Kundens IT-miljö

- Tjänsten kräver internetåtkomst med lämpligt brandväggsskydd.
- Tjänsten kräver att InfraCom ges korrekta administratörsrättigheter och åtkomst till kundens IT-miljö.

Teknisk beskrivning av tjänsten

Tjänsten övervakar och varnar om det finns hot eller attacker mot nätverk, moln, användare, klienter och servrar.

Vi identifierar angriparens taktik, tekniker och procedurer så att våra experter kan upptäcka indikatorer på attack innan någon skada sker.

Övervakning i realtid av skadlig och misstänkt aktivitet, identifierar indikatorer så som till exempel anslutningar till kriminella organisationer, obehöriga tjänster, bakdörr till servrar eller datorer.

SOC-experterna undersöker varje varning och vid behov så informeras kunden och det skapas ärende i InfraComs ärendehanteringssystem.

Akuta åtgärder och avvärjning sker 24/7/365. All hantering debiteras mot beredskapstaxa.

Ansvarsfördelning uppgifter	InfraCom	Kunden
Justering av antal prenumerationer för tjänsten		Ja
Ge InfraCom tillgång till nödvändiga inloggningsuppgifter med korrekta administratörsrättigheter samt åtkomst för konfigurering av tjänsten		Ja
Uppsättning av tjänsten	Ja	
Övervakning av kundens IT-miljö 24/7/365	Ja	
Informera InfraCom vilka klienter som ska ha tjänsten installerad samt när en dator tas ur bruk och tjänsten ska avinstalleras		Ja
Dedikerad kontaktperson vid akuta ärenden		Ja
Tillhandahålla teknisk kontakt för grundinstallation		Ja