VIRKSOMHEDER TVUNGET TIL STÆRK DIGITAL GRÆNSEKONTROL

WHITEPAPER

wingmen

GRÆNSEKONTROL ER NØGLEN I NYT TRUSSELSLANDSKAB

Digital data er kernen i moderne virksomheders forretning. Men data lever i stigende grad en udsat tilværelse. For det første er data underkastet det hybride arbejdsmarked, hvor fjernarbejde og hjemmearbejde er normen. For det andet ser danske virksomheder ind i en virkelighed med en voldsom vækst i cyberkriminalitet, hvor ransomware, phishing og DDoS-angreb er en del af dagens digitale uorden. Det er grunden til at EUs medlemslande er gået sammen om et nyt it-sikkerhedsdirektiv NIS2, der skærper kravene til it-sikkerheden blandt samfundskritiske virksomheder og organisationer.
Men hvordan sikrer almindelige virksomheder sig i dette trusselslandskab?

Nyt trusselslandskab kræver grænsekontrol
Når vi arbejder hjemme og på farten, er vi uden for virksomhedens firewall. Derfor er der behov for nye sikkerhedsløsninger. Løsninger, der beskytter virksomhedens "grænser", inden cyberkriminelle kommer ind i virksomhedens systemer. Cisco Umbrella er en løsning skabt til at yde denne type beskyttelse. Umbrella et "first line of defense", der blokerer trusler, før de når netværket. Sikkerheden håndhæves på DNS-niveau forud for etablering af forbindelse med virksomhedens netværk. Samtidig rummer Umbrella en suite af værktøjer, der sikrer, at virksomheden lever op til de højeste standarder inden for it-sikkerhed. Umbrella hjælper virksomheden til at udvikle en *state of the arts* it-sikkerhedspolitik.

NIS2

NIS2 er et nyt Net- og Informationssikkerhedsdirektiv fra EU-kommisionen, der træder i kraft i 2023. Direktivet skærper kravene til en række samfundskritiske virksomheders it-sikkerhed indenfor bl.a. forsyningskæden, affaldshåndtering og fødevareproduktion. Direktivet skal imødegå stigningen i cyberangreb - bl.a. fra ondsindede stater -, som vi har set i de senere år. Det indeholder krav om, at de omhandlede virksomheder skal forholde sig til risikostyring, kontrol og tilsyn. Desuden skal it-sikkerhed have større synlighed i organisationen, og der skal etableres nødberedskab og procedurer for rapportering til myndighederne.

"Halvdelen af virksomhedens it-sikkerhed handler om at overholde reglerne. Compliance og lovgivning som NIS2 betyder mere og mere, og her skal systemerne hjælpe. De fleste mangler værktøjer til dette. Normalt kræver det højt specialiseret viden, men med Umbrella får man et værktøj, der på en enkelt måde kan hjælpe til med at sikre, at man lever op til de højeste standarder for it-sikkerhed."

- Nicolai Hannen, Senior System Engineer, Wingmen Solutions

BESKYTTER DATA OVERALT

Umbrella beskytter data ved grænsen til virksomheden, når de cyberkriminelle forsøger at opnå forbindelse til virksomhedens netværk. Det sker ved en rekursiv DNS-beskyttelse, der beskytter klienter og data, uanset hvor de befinder sig.

Grænsekontrol

Umbrella beskytter al data på DNS-niveau og beskytter brugerne ved at stoppe trusler via alle porte og protokoller, før de når virksomhedens netværk og endepunkter. Informationen om evt ondsindede forespørgsler har Umbrella fra verdens største ikke-statslige it-sikkerhedsorganisation Cisco Talos. Umbrella påvirker ikke netværkets performance og beskytter altid - også når brugerne ikke benytter netværket.

Lukker huller i synlighed og kontrol

Policy på højeste niveau

Umbrella guider virksomheden til at lave en state of the art sikkerhedspolitik, både hvad angår overholdelse af lovgivning og stillingstagen til de nødvendlige policies, der skal sikre compliance. Dermed løftes virksomhedens sikkerhedsniveau til det højeste niveau, uanset om man ønsker et "set & forget" eller vil bruge Umbrella som et aktivt værktøj til at sikre alle virksomhedens digitale procedurer.

Compliance på højeste niveau

Ensartet sikkerhedspolitik

Umbrella sikrer implementering af virksomhedens sikkerhedspolitik, så den håndhæves på samme måde alle steder, hvor virksomhedens klienter og servere befinder sig.

Gennemtvinger ensartet politik

Overblik over aktivitet

Umbrella leverer et fuldstændigt overblik over internetaktiviteten omkring virksomhedens netværk på tværs af alle brugere og enheder uanset deres placering. Løsningen giver værdifuld viden om, hvad der foregår på netværket og tilvejebringer information til it, ledelse og andre afdelinger om bekymrende adfærd. Information, der kan have forretningsmæssig værdi.

Konsolidérer virksomhedens forskellige systemer

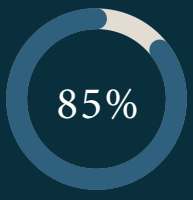
CISCO TALOS.
VERDENS STØRSTE PRIVATEJEDE SIKKERHESCENTER

Cisco Talos er verdens største ikke-statslige it-sikkerhedscenter. På Talos overvåger forskere, analytikere og ingeniører den globale web-aktivitet og indsamler, analyserer og filtrerer DNS-forespørgsler i realtid. TALOS opdeler forespørgsler i tre typer — sikre, ondsindede og risikable. Sikre forespørgsler sendes igennem, ondsindede blokeres, og risikable anmodninger underkastes yderligere analyse, inden de klassificeres. Det sker ved at omdirigere forespørgslerne til en Cisco Proxy.

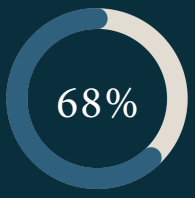
Umbrella giver et globalt overblik over it-trusler i realtid. På baggrund af information fra Talos stopper Umbrella dagligt 170 mio. ondsindede DNS-forespørgsler hos mere end 24.000 virksomheder.

DIN HYBRIDE VIRKSOMHED

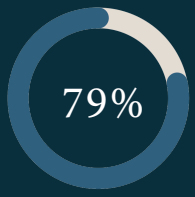
Det er primært fjernbrugere og hjemmebrugere, der er årsag til at virksomheders systemer kompromitteres.



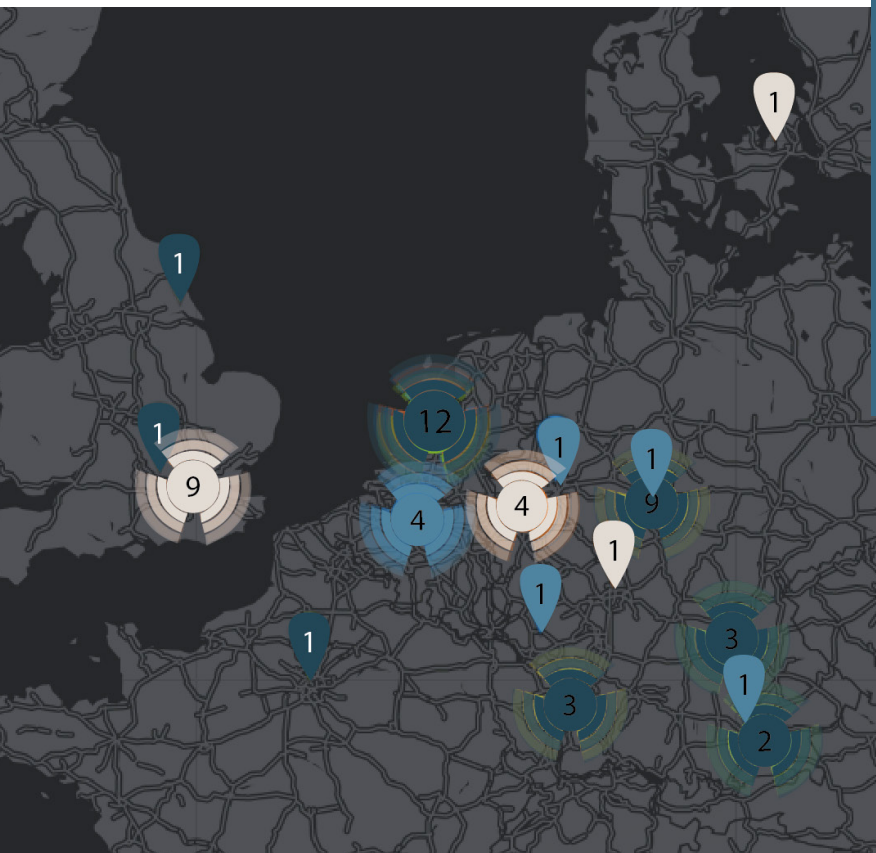
85% af fjernbrugerne rapporterer, at de til tider går direkte på internettet



68% af hændelserne sker for disse brugere



79% af alle organisationer skifter til direct internet access (DIA)



Datasikkerhed handler basalt om, at man er bevidst om og har overblik over de de data, der flyder ind og ud af virksomheden. Det lyder simpelt - og det er det også med Umbrella."

- Nicolai Hannen, Senior System Engineer, Wingmen Solutions

UMBRELLA I FLERE STØRRELSER

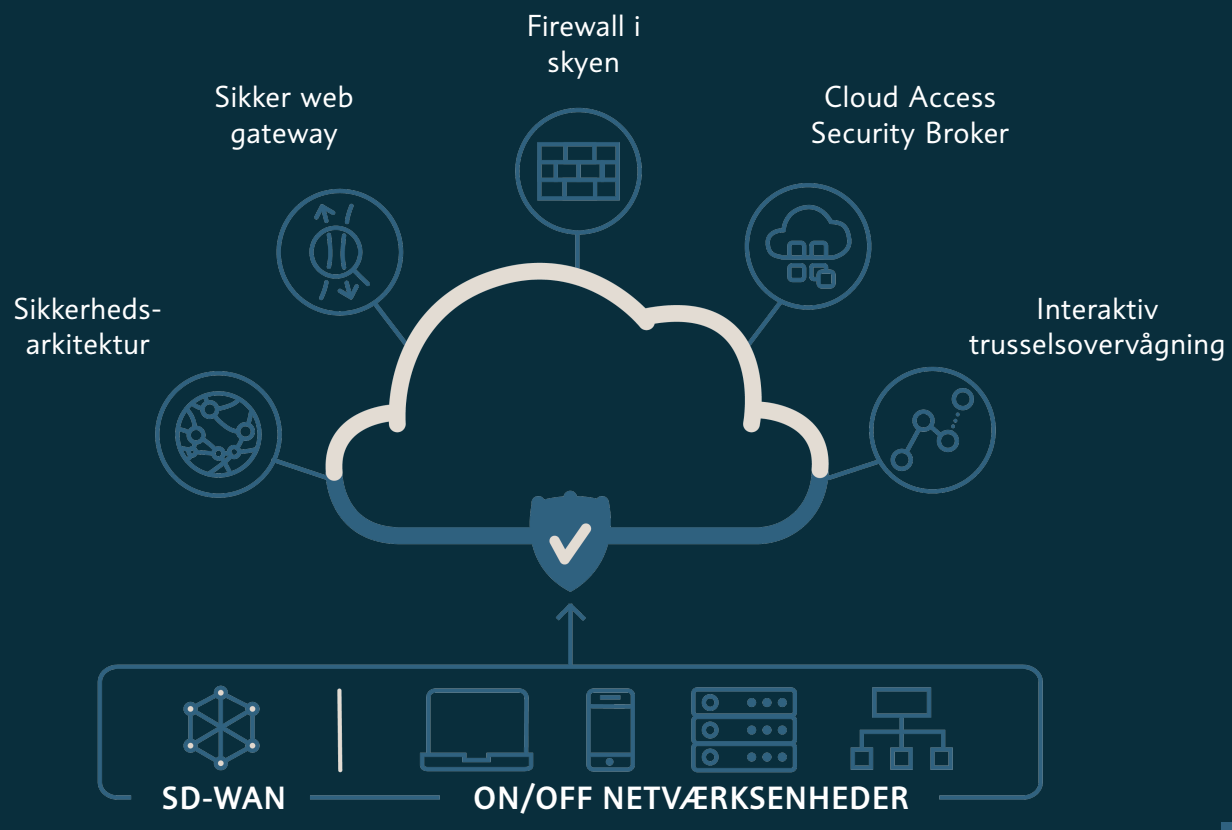
Ønsker man en "set & forget-løsning" er Umbrellas DNS-beskyttelse det rigtige valg. Her opnår virksomheden optimal beskyttelse via Umbrella, uden at det trækker ressourcer fra organisationen.

Ønsker man derimod, at Umbrella skal bidrage til den løbende udvikling og overvågning af virksomhedens interne sikkerheds-setup og compliance, bør man supplere med overbygningen Umbrella SIG. SIG er en Secure Internet Gateway, der supplerer DNS-beskyttelsen ved også at yde sikkerhed på "indersiden" af organisationen.

SIG kræver mere engagement men yder til gengæld en mere omfattende og avanceret sikkerhed. SIG er især valget for virksomheder, der har behov for en stram sikkerhedspolitik.

SIKKERHEDSARKITEKTUR

Umbrella leverer omfattende cloud-baseret sikkerhed til alle virksomhedens klienter - overalt og altid.



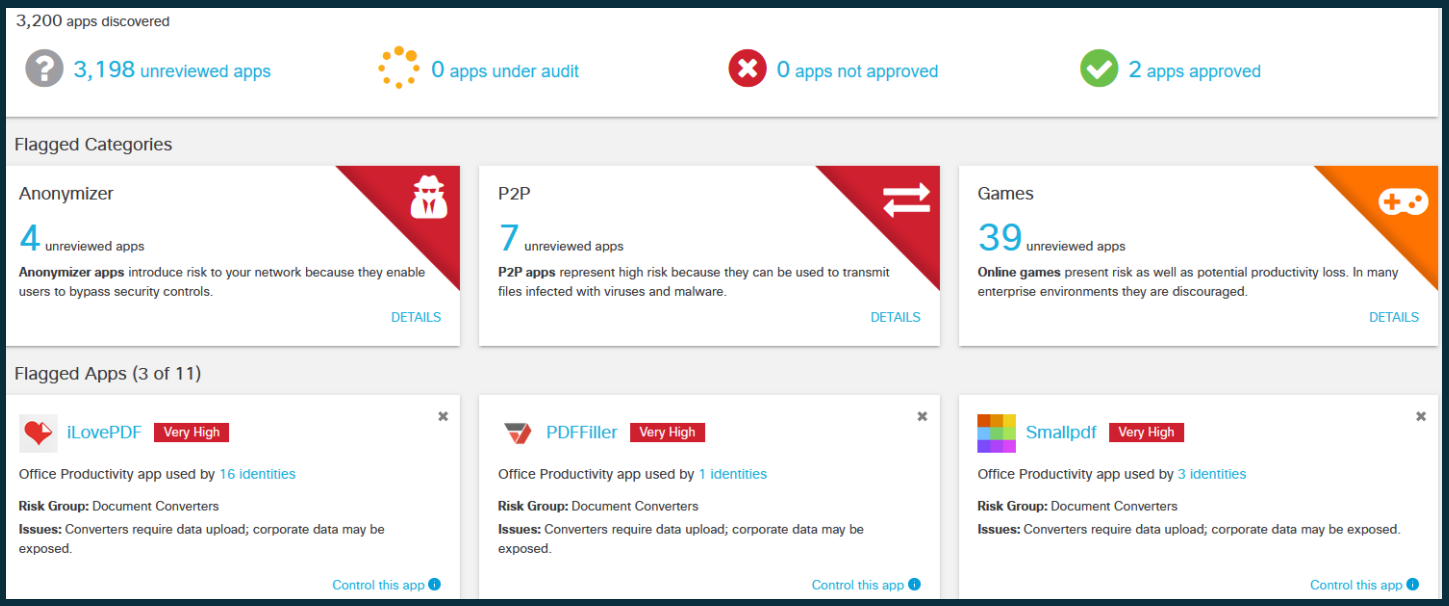
UMBRELLA SECURE INTERNET GATEWAY (SIG) BESKYTTER MOD RISIKABEL OMGANG MED DATA

Når DNS-grænsekontrollen har hvidlistet en service eller applikation på baggrund af det globale trusselsbillede, kan den frit bevæge ind i virksomheden. Men den kan stadig udgøre en trussel mod virksomhedens data fx ved brug af eksterne services.

SIG tilbyder endnu et lag af sikkerhed. SIG logger og undersøger webtrafik for fuld visibilitet, URL og applikationskontrol og beskytter mod malware. SIG giver samtidig et detaljeret overblik over, hvilke risikable services og applikationer, der anvendes i virksomheden.

Virksomheder kan bl.a. overvåge brugen af sociale medier og peer-to-peer services og oprette specifikke regler, der regulerer og begrænser medarbejdernes brug af disse. I SIG er det let for it-afdelingen at se og blokere applikationer, services og funktioner og adfærd, der er forbundet med en sikkerhedsrisiko. Det er fx. muligt at tillade, at medarbejderne læser indhold på Facebook fra virksomhedens enheder, men blokere at de poster.

UMBRELLA OVERSIGT
Overblik over applikationstyper. Umbrella SIGs kontrolpanel giver bl.a. overblik over hvilke apps, der anvendes, og advarer, rådgiver, når der anvendes særlige typer af app, som kan indebære risici. Her er også mulighed for at blokere risikable apps.



SKYGGE-IT GIVER INDSIGT

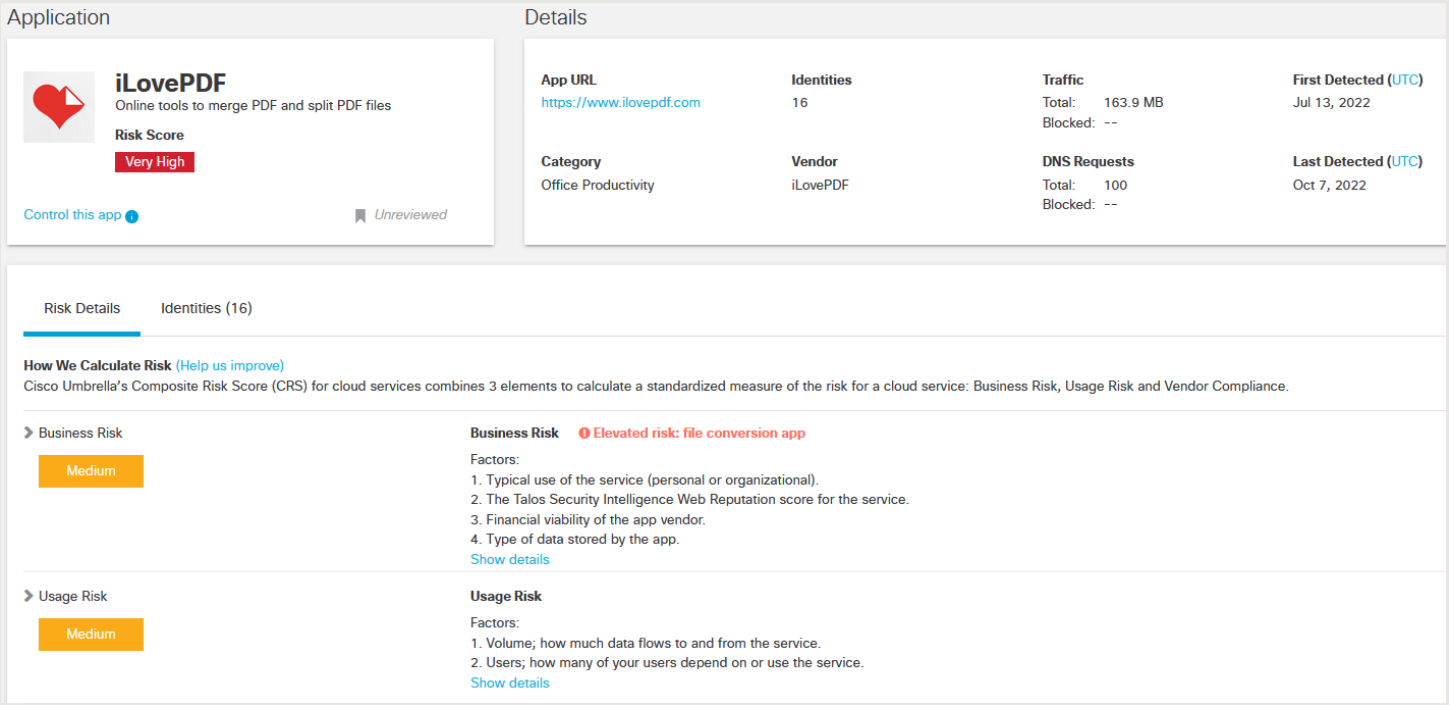
Application discovery er et værktøj i Umbrella SIG, der gør det muligt at overvåge og sikkerhedsvurdere hvilke typer data, medarbejderne downloader. Her får man bl.a. et detaljeret overblik over den skygge-it medarbejderne anvender. Skygge-it er alle de programmer, som medarbejderne bruger på deres arbejds-enheder, som ikke er leveret og autoriseret af virksomheden.

Indsigt om skygge-it er vigtig, fordi den giver viden om sikkerheds- & compliance-problemer."

- Nicolai Hannen, Senior System Engineer, Wingmen Solutions

CASE: I Love PDF

En virksomhed opdagede, at flere brugere på kort tid har benyttet sig af "I love pdf" tjenesten, en applikation der gør det muligt at pdf'e dokumenter. Problemet med at anvende en ekstern applikation til dette er, at det indebærer en risiko for, at følsom data bliver tilgængelig for en ekstern part. Derfor måtte virksomheden undersøge om denne app, havde funktionalitet som ikke var til rådighed internt og beslutte, om den skulle blokeres og man skulle stille tilsvarende funktionalitet til rådighed.



SIG BESKYTTER MOD TAB AF DATA

Sikrer fortrolige dokumenter
Med SIG kan virksomheden se, når data siver ud af virksomheden. Dermed kan virksomheden sikre sig mod datatab og data lækager. Det er fx. muligt at overvåge fortrolige dokumenter ved hjælp af sensitivity tags og dermed hindre deling af disse.

Sikker mod overtrædelse af GDPR
SIG rummer også et GDPR-modul, der kan sikre, at der ikke deles følsomme persondata. Her kan man bl.a. se, når der sker forsøg på at dele navnedata og CPR-numre ud af virksomheden.

Blokerer bestemte services
Virksomheder, der opererer under strenge krav til håndtering af data, har også mulighed for at låse specifikke, lokale miljøer ned. Det kan fx være, at virksomheden ønsker at medarbejderne kun skal have adgang til virksomhedens OneDrive. Så kan man blokere adgangen til deres private OneDrive.

> *Det er fremtidens løsning, uanset hvordan man forholder sig til virksomhedens data. Det er muligt at lave en set & forget, hvor det bare kører i baggrunden på højeste sikkerhedsniveau. Men man kan også bruge det aktivt til at styre data og software i alle virksomhedens afdelinger."*
>
> **- Nicolai Hannen, Senior System Engineer, Wingmen Solutions**

Umbrella yder hurtig og effektiv beskyttelse mod bl.a.:

- Malware
- Ransomware
- Phishing
- Command and Control call backs
- Datatab & Datalækage

Med Umbrella kan virksomheden tillige stoppe ransomware og phishing-forsøg, selv om hackerne skulle være lykkes med at plante deres malware på virksomhedens netværk. Umbrella kan nemlig blokere for, at malware sender data ud af netværket.

SÅ LET KOMMER I I GANG

Cisco Umbrella er den nemmeste og mest effektive måde at beskytte brugerne altid og overalt, og implementeringen er simpel i forhold til den omfattende beskyttelse, der opnås.

Umbrella grundpakken med DNS-beskyttelse kan opsættes i løbet af ½ time. I forbindelse med implementeringen gennemgår Wingmens konsulent de forskellige typer af sikkerhed, som Umbrella opererer med (terror, våben, fildeling etc). Sammen med kunden konfigurerer vi løsningens sikkerhedsindstillinger, så de er på linje med gældende lovgivning og policies.

Vores kunder sætter pris på de overvejelser over sikkerheden, som Umbrella giver anledning til. Min erfaring er, at Umbrella højner bevidstheden om sikkerhedsrisici i virksomheden"

- Nicolai Hannen, Senior System Engineer, Wingmen Solutions

1. **Umbrella SIG**
   Vælger man at supplere med Umbrella SIG er design og implementering mere omfattende.

2. **Installation af agenter**
   Der installeres agenter på virksomhedens klient-pc'er. Installationen foregår i flere tempi, en afdeling ad gangen, så man kan opbygge erfaring afdeling for afdeling.

3. **Design af rapporter**
   Indbyggede rapporter giver et godt overblik over brugers aktivitet på Internettet.

4. **Overvågning og udvikling**
   Medarbejdernes brug af services overvåges og styres. Wingmen Solutions tilbyder at stå for driften. Det indbefatter en kvartals-gennemgang af brugsdata, som danner baggrund for en eventuel justering af policy og indsats.

Umbrella DNS og Umbrella SIG findes i Essentials og Advantage-udgaver. Kontakt os for at høre mere om, hvilken løsning, der passer til jeres organisation og jeres behov.

WINGMEN

Wingmen er et dansk it-konsulenthus med speciale i Ciscos it-sikkerheds-portefølje. Wingmen tilbyder design og implementering af Cisco Umbrella og står for support af løsningen.

Man tilbyder desuden at stå for drift og vedligeholdelse af Umbrella for virksomheder, der ønsker at dette håndteres af en professionel ekstern partner.

Wingmen har mere end 100 Cisco-certificeringer.

Vi ser en stigning i hjemmearbejde på grund af strukturelle forandringer på arbejdsmarkedet og de aktuelle kriser, vi oplever. Men når vi er hjemme, er vi uden for virksomhedens firewall. Derfor er der behov for andre måder at tænke it-sikkerhed. Sikkerhed der griber ind, før truslen er på din computer. Ligesom Umbrella"

- Nicolai Hannen, Senior System Engineer, Wingmen Solutions

Nicolai Hannen

- Senior Systems Engineer
- Tech Lead på sikkerhed
- +25 års erfaring

Certificeringer

- CCNP Enterprise
- CCNP Security

KONTAKT WINGMEN

Kontakt os med dine spørgsmål vedrørende Ciscos sikkerhedsportefølje eller for en udvidet snak om, hvordan vi kan skræddersy den optimale sikkerhedsløsning til dine forretningsbehov

wingmen

+45 70 20 21 10

info@wingmen.dk