



Surfshark er vores næstbedste VPN-valg, der tilbyder god værdi for pengene. Vi tilbyder også Surfshark-rabatkoden: OFFCN for yderligere besparelser. Selvom den er mere overkommelig end NordVPN, leverer den stadig lignende hurtige hastigheder og stærk sikkerhed. Surfshark er kendt for sine omfattende sikkerhedstilføjelser, såsom Alternative ID, der hjælper med at beskytte dine personlige oplysninger online, og sit antivirusprogram. En af dens største fordele er ubegrænsede samtidige forbindelser, hvilket gør den til et godt valg for husstande eller brugere med mange enheder.

Surfshark blev grundlagt i 2018 og har etableret sig blandt de bedste VPN'er i 2025 takket være dens konstant stærke ydeevne og robuste funktioner. Ud over standard VPN-beskyttelse tilbyder den yderligere værktøjer som Antivirus, Alternative ID og den nyligt patenterede Everlink-teknologi, der giver brugerne ekstra lag af sikkerhed. I løbet af de sidste fem år har vi nøje fulgt Surfsharks udvikling og dokumenteret dens forbedringer. Selvom det er en top-VPN, er der stadig et par bekymringer, der er værd at bemærke omkring dens jurisdiktion og politik om ingen logfiler. Til denne anmeldelse testede jeg Surfsharks ydeevne i den virkelige verden og undersøgte dens privatlivsfunktioner, sikkerhedsværktøjer, priser og hastighed for at se, hvor godt den virkelig holder mål.

Surfshark VPN anmeldelse – hurtige fakta

For at kunne vurdere Surfshark VPN grundigt, har jeg indsnævret nogle nøgleoplysninger i tabellen:

★ Rating:	4.7★★★★★
🏆 Overall rank:	#2 out of #41
📖 No logs policy:	No logs
💰 Price:	From \$1.99/month
💻 Servers:	3,200 + servers in 100 countries
🍿 Streaming services:	Netflix, Disney+, Amazon Prime Video, Hulu, and more

Vores mening om Surfshark

VPN Surfshark er en privatlivsorienteret VPN, der indeholder flere avancerede cybersikkerhedsfunktioner, hvilket gør den til et ideelt valg for sikkerhedsfokuserede brugere. Den er også perfekt til budgetbevidste enkeltpersoner og familier på grund af dens overkommelige priser og ubegrænsede samtidige forbindelser.

Ting vi kunne lide

Pris/kvalitet: Surfshark er en af de mest prisvenlige VPN'er, især med dens toårige abonnement
Streamingfunktioner: Fjerner blokering af indhold på store platforme som Netflix, Hulu og HBO Max uden besvær

Alternativt ID: Hjælper med at øge anonymiteten ved at generere falske personlige oplysninger og engangs-e-mailadresser

Ubegrænsede enhedsforbindelser: Giver dig mulighed for at bruge en enkelt konto på så mange enheder, som du vil – et sjældent syn på VPN-markedet

Everlink: Gendanner automatisk en mistet VPN-forbindelse og reducerer risikoen for, at din IP-adresse bliver eksponeret. Brugervenlig grænseflade: Enkle og intuitive apps på tværs af forskellige platforme, hvilket gør den brugervenlig for begyndere
Antivirus: Tilbyder beskyttelse i realtid mod malware, såsom ransomware og orme

Ting vi ikke kunne lide

Prisstigning ved fornyelse: Den oprindelige aftale er god, men priserne stiger, når din første periode udløber

Hastighedsvariationer: Selvom den normalt er hurtig, kan ydeevnen falde en smule afhængigt af den server, du er forbundet til

Surfshark VPN vs populære VPNs

Here's a quick overview of how Surfshark performs against other [top VPNs](#).

Feature	Surfshark	NordVPN	ExpressVPN	CyberGhost	CyberGhost
Kill switch	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes
Split tunneling	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes
Ad blocker	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes
Antivirus	✔ Yes	✘ No	✘ No	✘ No	✘ No
Simultaneous connections	Unlimited	10	8	7	10
Protocols	WireGuard, OpenVPN, IKEv2	OpenVPN, WireGuard (NordLynx), NordWhisper	Lightway, OpenVPN, IK	WireGuard, IKEv2, OpenVPN (TCP/UDP)	WireGuard, OpenVPN, and IKEv2/IPsec
Streaming support	Netflix, Disney+, Amazon Prime Video, Hulu, and more	Netflix, Hulu, BBC iPlayer, Disney+, and more	Netflix, Hulu, BBC iPlay, Disney+, and more	Netflix, Hulu, BBC iPlayer, Disney+	Netflix, BBC iPlayer, YouTube, HBO Max, Disney+
Supports torrenting	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes
Encryption type	AES-256, ChaCha20	AES-256, ChaCha20	AES-256	AES-256	AES-256, ChaCha20
Jurisdiction	The Netherlands	Panama	British Virgin Islands	Romania	Switzerland
RAM-only servers	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✘ No
Independent audits	✔ Yes	✔ Yes	✔ Yes	✔ Yes	✔ Yes
Speed retention rate	84%	88%	87%	86%	83%
Server count	3200+ servers in 100 countries	8000+ servers in 126 countries	Servers in 105 countries	Servers in 100 countries	13700+ servers in 122 countries
Monthly price	From \$1.99/month	From \$3.39/month	From \$4.99/month	From \$2.19/month	From \$3.59/month
Money-back guarantee	30 days	30 days	30 days	45 days	30 days
App support	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linu, Android, iOS	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS
Browser extensions	Chrome, Firefox, Edge, Brave	Chrome, Firefox, Edge	Chrome, Firefox, Edge, Vivaldi	Chrome, Firefox	Chrome, Firefox, Edge, Brave, Opera, Vivaldi
Customer support	Knowledge base, 24/7 live chat, email support	Knowledge base, FAQs, email, 24/7 live chat	Knowledge base, FAQs, email, 24/7 live chat	24/7 live chat, Knowledge base, FAQs	Guides, FAQs, support tickets, subreddit

Surfshark klarer sig rigtig godt i forhold til andre top VPN'er, især hvis du leder efter en budgetvenlig løsning med en række funktioner. En af dens største fordele er, at den giver dig mulighed for at forbinde et ubegrænset antal enheder til et enkelt abonnement på én gang. Kun få udbydere, som IPVanish og PIA VPN, tilbyder det. Hvis du har en hel del gadgets, du vil beskytte, er Surfshark et smart valg. Den har også et antivirusprogram, hvilket ikke er noget, de fleste VPN'er tilbyder. Derudover er antivirusprogrammet ret solidt og har endda vundet priser fra AV-TEST, et respekteret uafhængigt testlaboratorium.

Når det er sagt, er det ikke uden ulemper. I modsætning til NordVPN eller ExpressVPN har Surfshark ikke sin egen proprietære VPN-protokol, hvilket kan være vigtigt, hvis du leder efter banebrydende hastighed eller sikkerhed. Derudover har virksomheden hovedkontor i Holland og er en del af Fourteen Eyes-alliancen.

Det betyder, at Surfshark er juridisk forpligtet til at levere brugerdata efter anmodning fra myndighederne. Men da virksomheden har en politik om ingen logfiler, indsamler eller gemmer den ikke brugerdata i første omgang. Hvis jurisdiktion er en stor bekymring for dig, kan dette dog være noget at overveje. Servernetværk er et andet område, hvor Surfshark halter lidt bagud. Selvom det stadig dækker et godt antal lande, har det færre servere end NordVPN eller Proton VPN. Derudover dækker ExpressVPN flere lande samlet set. Så hvis serverudvalg eller international dækning er en prioritet, kan disse være bedre egnede.

Brug af Surfshark VPN til daglige opgaver Sammen med forskerholdet brugte jeg en uge på grundigt at teste Surfshark. Vi dækkede alle de mest almindelige VPN-brugsscenarier, herunder streaming, torrenting, spil og browsing på offentlige Wi-Fi-netværk. Jeg testede også VPN'en på flere enheder for at se, hvor godt den klarer sig på tværs af forskellige platforme, så jeg får en reel fornemmelse af, hvordan det er at bruge den i hverdagen.

Vores tests viste, at Surfshark er en fremragende VPN til streaming. Med over 3200 servere i 100 lande tilbyder den solid dækning og fjerner nemt blokeringer fra Netflix, HBO Max, BBC iPlayer og Amazon Prime Video. Surfsharks servere er velholdte, så jeg havde ingen problemer med sortlistede eller blokerede IP'er. Hastighederne var fremragende, især når jeg brugte WireGuard-protokollen. Der var ingen buffering eller afmatning overhovedet.

Surfshark tilbyder fantastiske funktioner, der gør den til en solid VPN til torrenting. Den har P2P-optimerede servere, der fungerede rigtig godt under mine tests. Wireguard-protokollen leverede fremragende hastigheder, så jeg kunne downloade filer hurtigt og sikkert.

Jeg havde en god oplevelse med at bruge Surfshark til spil. Selvom de ikke har dedikerede spilservere, fungerede de almindelige servere fint.

Det er absolut nødvendigt at bruge en VPN, mens du er forbundet til et offentligt netværk. Jeg testede Surfshark på et offentligt netværk på en café i Vilnius og følte mig tryk ved at browse med det aktiveret. Det krypterer din forbindelse, så dine data forbliver beskyttet mod hackere. Derudover oprettede den automatiske forbindelsesfunktion forbindelse, hver gang jeg oprettede forbindelse til et ukendt Wi-Fi-netværk. Jeg fandt denne tilføjelse super praktisk.

Surfsharks virksomhedsbaggrund

Surfshark blev grundlagt i 2018 af Vytautas Kaziukonis og er vokset til et af de mest anerkendte navne inden for cybersikkerhed. Virksomheden, der oprindeligt var registreret på De Britiske Jomfruøer, flyttede til Holland i 2021. Selvom Holland er en del af Nine Eyes-alliancen, håndhæver landet strenge privatlivsregler og overholder GDPR.

Surfshark er også transparent omkring anmodninger om data fra myndigheder og deler disse oplysninger offentligt i sit Trust Center. Fra starten har Surfshark prioriteret brugernes privatliv. Virksomheden blev revideret af Cure53 i det første driftsår. Siden da er den blevet revideret tre gange i alt – to gange af Cure53 og én gang af Deloitte.

Virksomheden fortsætter også med at investere i sikkerhedscertificeringer. Dens antivirusprodukt er blevet testet af AV-TEST, og dens Android-app har bestået Mobile App Security Assessment. I 2022 fusionerede Surfshark med Nord Security, moderselskabet til NordVPN. Selvom de to brands fortsat opererer separat, kombinerer de nu ekspertise og styrker deres positioner inden for cybersikkerhed.

Surfshark er kendt for sin konstante innovation og udgiver regelmæssigt nye funktioner baseret på brugerfeedback for at forbedre både sikkerhed og brugervenlighed. I 2019 lancerede de Surfshark Search and Alert. Dette blev efterfulgt af udgivelsen af Surfshark Antivirus og Incogni i 2021. Virksomhedens hurtige vækst og innovation har givet dem en plads på Financial Times 1000-listen: Europas hurtigst voksende virksomheder.

Ud over produktudvikling støtter Surfshark internetfrihed og digitale rettigheder. De er et stiftende medlem af VPN Trust Initiative og samarbejder med NetBlocks. De reagerer også hurtigt på lovgivningsmæssige ændringer, såsom fjernelse af servere fra Indien som reaktion på nye love om dataopbevaring.

Er Surfshark sikker?

Ja, Surfshark er sikker takket være dens fremragende standarder og unikke funktioner. Til at begynde med bruger den branchestandard AES-256-kryptering og en streng politik om ingen logfiler for at sikre brugerne.

For det andet går den ud over de sædvanlige VPN-funktioner ved at inkludere Everlink, Alternative ID og Antivirus-funktioner i blandingen.

For at teste, hvor sikker Surfshark virkelig er, gennemgik jeg hver funktion trin for trin. Jeg begyndte med at kontrollere for DNS-, IP- og WebRTC-lækager, mens jeg var forbundet til flere servere i forskellige regioner.

Derefter afbrød jeg VPN-forbindelsen med vilje for at se, hvordan standard kill switch ville reagere, og den blokerede med succes al trafik for at forhindre lækager.

Jeg testede også Everlink, som fungerer som en smart kill switch ved at afbryde forbindelsen og derefter automatisk genoprette forbindelsen, når VPN'en er stabil igen.

På den tekniske side gennemgik jeg de anvendte krypteringsprotokoller og bekræftede, at Surfshark understøtter sikre muligheder som WireGuard og OpenVPN.

Jeg læste også privatlivspolitikken og verificerede, at påstandene om ingen logfiler er blevet uafhængigt revideret.

Endelig udforskede jeg bonusværktøjer som Alternative ID for at se, hvor godt de bidrager til at holde din identitet og dine data private.

Håndtering af Surfsharks bekymringer om jurisdiktion

Det er baseret i Holland, som, selvom det er en del af Nine Eyes-alliancen, ikke pålægger obligatoriske love om dataopbevaring.

Med disse foranstaltninger tilbyder Surfshark et sikkert miljø til browsing, streaming og online transaktioner. Dette gjorde os forståeligt nok nysgerrige. Så vi spurgte Surfshark direkte om det.

Deres svar? Dybest set er der ingen grund til bekymring. Ifølge Surfshark kræver hollandsk lov ikke, at VPN'er logger eller gemmer brugerdata i første omgang.

Så selvom Holland er en del af disse alliancer, er der intet at dele, hvis der ikke indsamles data. De mindede os også om, at Surfshark har en streng politik om ingen logfiler, og at hele deres servernetværk kører på servere med kun RAM.

Det betyder, at alle data slettes, hver gang en server genstarter. Der er ingen permanent lagring.

Kryptering

Surfshark anvender banebrydende krypteringsprotokoller, såsom AES-256-GCM og ChaCha20, der er bredt anerkendt som branchens guldstandarder. AES-256-GCM er kendt for sin næsten uigennemtrængelighed, hvilket gør den til den foretrukne kryptering for regeringer og cybersikkerhedsløsninger i topklasse. ChaCha20, der bruges i specifikke situationer, er lige så robust og optimeret til enheder med lavere computerkraft.

En fremragende funktion er Perfect Forward Secrecy, som genererer en unik krypteringsnøgle for hver session. Dette sikrer, at selvom ondsindede programmører opsnapper én session, kan de ikke få adgang til tidligere eller fremtidig kommunikation. Kombineret skaber disse krypteringsmetoder et sikkert skjold omkring dine onlineaktiviteter og beskytter følsomme oplysninger som adgangskoder, personlige data og økonomiske detaljer.

Dette krypteringsniveau betyder, at brugerne trygt kan oprette forbindelse til offentlige Wi-Fi-netværk, browse sikkert og udføre transaktioner uden frygt for at blive opsnappet. Surfshark prioriterer brugersikkerhed og opretholder optimale hastigheder, hvilket sikrer, at avanceret kryptering ikke sinker dig. Uanset om du arbejder eksternt, streamer indhold eller blot browser, garanterer Surfsharks kryptering ro i sindet.

Politik om ingen logfiler

Ligesom de fleste VPN-tjenester har Surfshark en politik om ingen logfiler. Jeg læste udbyderens privatlivspolitik i juni 2025 for at kontrollere, om det er tilfældet, og for det meste er det sandt. Der er dog et potentielt problem, omend et rimeligt ubetydeligt et.

Dokumentets første afsnit hedder "1. Hvilke oplysninger indsamles, og hvorfor?" og nævner en bekymrende detalje. Surfshark VPN-servere gemmer nemlig oplysninger (bruger-ID, IP-adresse, forbindelsestidsstempler) om din forbindelse til en bestemt VPN-server.

Heldigvis slettes disse oplysninger automatisk inden for 15 minutter efter afslutningen af din session. Desuden logger VPN'en ikke andre data, der ville fortælle udbyderen noget om dine onlineaktiviteter.

Uddrag fra Surfsharks privatlivspolitik

Uddrag fra Surfsharks privatlivspolitik, der forklarer opbevaring af forbindelsesdata Her er en tabel, der opsummerer, hvilke oplysninger Surfshark indsamler:

Data	Does Surfshark store it?
IP address	Temporarily, for 15 minutes
Customer's email address	✓ Yes
Customer's encrypted password	✓ Yes
Payment data	✓ Yes (if provided)
Browsing history	✗ No
Session information	✗ No
User bandwidth	✗ No
Network traffic	✗ No

Som du kan se, indsamler og gemmer Surfshark VPN kun de mest essentielle oplysninger, den har brug for for at levere sin tjeneste.

For eksempel vil udbyderen have dine kontooplysninger, såsom e-mailadresse, krypteret adgangskode og betalingsdata, da disse er afgørende for at oprette en konto og betale for abonnementet.

Omvendt logges oplysninger som browserhistorik, sessionsoplysninger, båndbredde og andre specifikke oplysninger om VPN-brug ikke.

Den midlertidige lagring af IP-adresse er den eneste bekymring her, men jeg ville ikke bekymre mig for meget om det. IP-adresseoplysningerne vil trods alt blive slettet, når du afbryder forbindelsen til VPN'en, hvilket betyder, at Surfshark ikke vil være i stand til at dele disse oplysninger med tredjeparter i fremtiden.

Men hvis denne detalje er et rødt flag for dig, bør du overveje NordVPN, som ikke gemmer din IP-adresse, mens du bruger VPN'en.

Surfshark DNS-lækagetest

Domænenavnssystemet (DNS) er ansvarligt for at forbinde websteders IP-adresser med deres domænenavne. Dette gøres ved hjælp af DNS-servere, som tildeles brugerne af deres internetudbydere (ISP'er). En DNS-lækage opstår, når du opretter forbindelse til en VPN, men din enhed kommunikerer stadig med de standard-DNS-servere, der er tildelt af din internetudbyder.

Når det sker, forbliver dine onlineaktiviteter eksponerede, hvilket ophæver fordelene ved at bruge en VPN. Vores forskerteam testede Surfshark for DNS-lækager ved hjælp af forskellige DNS-lækagetestere og fandt ingen problemer overhovedet. Som sådan er det sikkert at konkludere, at Surfshark VPN er fri for DNS-lækager.

The image shows a DNS leak test result from **DNS leak test.com** and a Surfshark VPN interface. The test result is labeled "Test complete" and shows a table of query rounds, progress, and servers found. Below this is a table with IP, Hostname, and ISP. The VPN interface is dark-themed and shows the user is "Connected and safe" with a connection time of 04:02 and IP address 146.70.186.124. It lists recommended locations (Lithuania, Latvia), recently used locations (United States, Lithuania, Türkiye), and a list of available locations (Albania, Algeria, Andorra, United States). The interface also shows "WireGuard® Protocol in use" and "CleanWeb On".

Query round	Progress...	Servers found
1		1
2		1
3		1
4		1
5		1
6		1

IP	Hostname	ISP
146.70.186.124	None	M247 E

What do the results of this test mean?

- The servers identified above receive a request to resolve a domain name (e.g. www.eff.org) to an IP address everytime you enter a website address in

Privacy policy | VPN Limited 2025

dnsleaktest.com confirms no DNS leaks, while Surfshark VPN is securely connected

Surfshark WebRTC leak tests

Webrealtidskommunikation (WebRTC) er et sæt teknologier, der gør det muligt for browsere at fremme realtidskommunikation mere effektivt. Det giver browsere mulighed for at oprette direkte forbindelse til hinanden uden mellemliggende servere for at reducere forsinkelser under videoopkald. WebRTC fungerer dog kun, når browserne kender hinandens IP-adresser, hvilket kan føre til problemer med privatlivets fred. Heldigvis kan du bruge tjenester som browserleaks.com til at tjekke for WebRTC-lækager. Vi gjorde netop det, mens Surfshark var aktiveret, og resultaterne viste ingen lækageproblemer. Det betyder, at Surfshark VPN er sikker at bruge til realtidskommunikation uden lækager.

BrowserLeaks.com

WebRTC Leak Test

Your Remote IP :
IPv4 Address 146.70.186.124
IPv6 Address -

WebRTC Support Detection :
RTCPeerConnection True
RTCDataChannel True

Your WebRTC IP :
WebRTC Leak Test No Leak
Local IP Address -
Public IP Address 146.70.186.124

Session Description :
SDP Log
v=0
o=mozilla...THIS_IS_SDPARTA-99.0 61430
s=-
t=0 0
a=sendrecv
a=fingerprint:sha-256
C6:E6:76:B2:EF:AE:6E:DC:94:ED:55:27:43:EB:52:78:AD:11:A2:7F:43:1A:EC:30:10:9C:02:35:8D:6E:22:1B:45:07:5

Media Devices :
API Support True

Search locations

Locations Static IP MultiHop Dedicated IP

Recommended for you
Lithuania Fastest location
Latvia Nearest country

Recently used
United States New York
Lithuania Vilnius
Türkiye Istanbul

Locations
Albania Tirane - Virtual location
Algeria Algiers - Virtual location
Andorra Andorra la Vella - Virtual location

Connected and safe
05:18 Connection time
WireGuard® Protocol in use
CleanWeb On
146.70.186.124 IP Address

United States New York
Disconnect Pause

browserleaks.com showing no WebRTC leaks while Surfshark is enabled

Avancerede sikkerhedsfunktioner

Som forventet tilbyder Surfshark mange standard sikkerhedsfunktioner, som du ville forvente af en pålidelig VPN. Disse inkluderer en kill switch, DNS-lækagebeskyttelse, annonceblokering og mere. Surfshark udvikler sig dog til et omfattende cybersikkerhedsværktøj med ekstra funktioner som Alternative ID og Antivirus, som giver sikkerhedsfordele, som andre VPN'er ikke har. Lad os hurtigt overskue Surfsharks vigtigste sikkerhedsfunktioner.

Feature	How it works
Kill Switch	Shuts off your internet connection in case the VPN connection fails, thus preventing data exposure
DNS leak protection	Ensures your DNS requests are handled by the VPN service to properly mask your activities from your ISP
MultiHop (double VPN)	Allows connecting to two VPN servers for more encryption and greater security
Alternative ID	Generates alternative data for personal details like names and email addresses to improve your online anonymity
Antivirus	Protects your device in real time from common cyberthreats like malware, scams, and dangerous websites
Everlink	Everlink adds an extra layer of security by keeping your VPN connection alive even if it drops, instantly restoring it without exposing your data. You can still use a Kill Switch to fully disconnect if needed.
Surfshark Search	A private, ad-free search engine that shows organic results without tracking, storing data, or showing personalized ads
CleanWeb	Eliminates online ads and trackers to improve your online browsing experience
NoBorders Mode	Allows secure VPN usage even on networks with strict limitations on VPN services
Camouflage Mode	Makes your VPN traffic appear as regular HTTPS traffic to minimize suspicion in certain circumstances
Bypasser (split tunneling)	Lets you pick which apps or websites should pass through or avoid the VPN tunnel
WireGuard protocol	Facilitates swift and secure connections, no matter which VPN server you use
Private DNS	Boosts anonymity by redirecting your DNS requests through Surfshark's private servers
Unlimited connections	You can connect an unlimited number of devices using one Surfshark account

Surfshark Antivirus

Surfshark er en exceptionel VPN, fordi den tilbyder muligheden for at inkludere antivirusfunktioner udover sin standard sikkerhedspakke.

Bemærk, at antivirusprogrammet ikke er tilgængeligt i det mest overkommelige Starter-abonnementsniveau – du skal vælge One- eller One+-abonnementet for at få denne fordel.

Men hvis du leder efter noget, der er mere end bare en VPN, er Surfshark bestemt et godt valg. For eksempel rangerer uafhængige antiviruslaboratorier som AV-TEST det højt blandt andre antivirusudbydere.

Den seneste evaluering fra juni 2024 gav tjenesten næsten perfekte scorere, med kun en lille nedgang i ydeevnekategorien. Det er endda en del af Microsoft Virus Initiative, hvilket fremhæver Surfsharks engagement i at overholde de bedste antivirusstandarder.

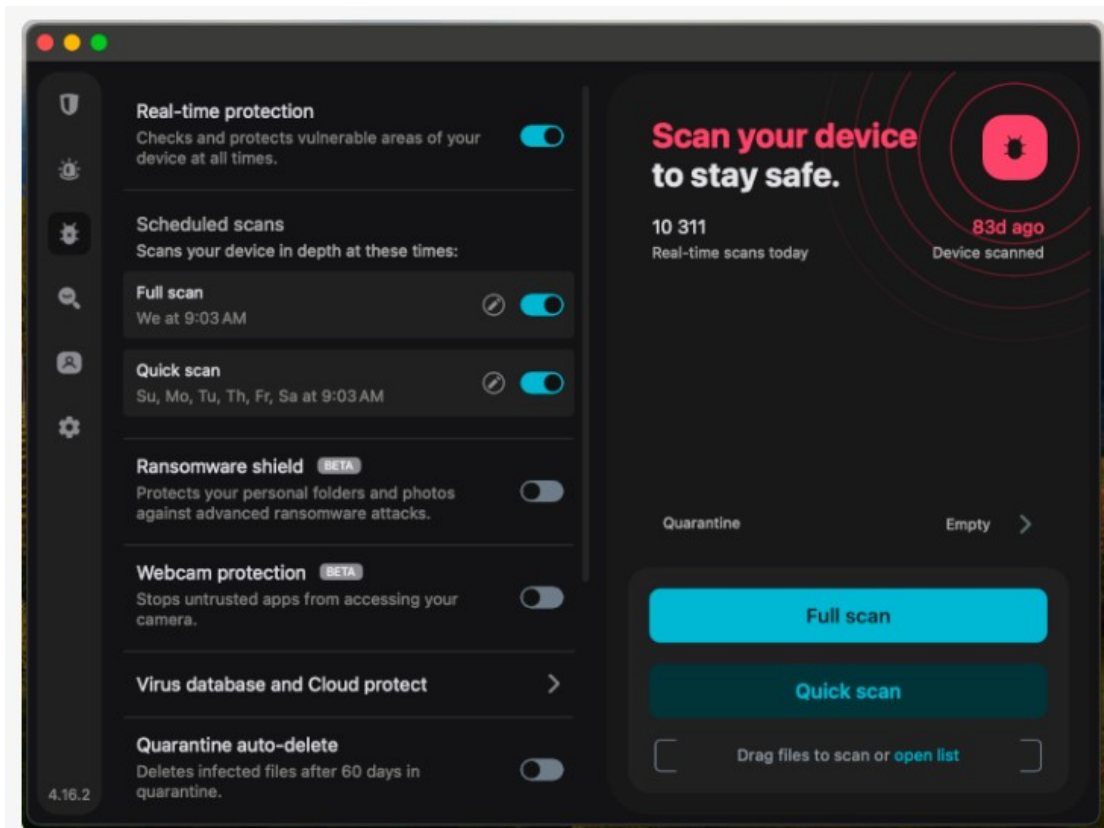
Surfshark Antivirus-pakken indeholder typiske antivirusfunktioner, såsom realtidsbeskyttelse og enhedsscanningsfunktioner, for at beskytte dine gadgets. Du får også webcam-beskyttelse og omfattende tilpasningsmuligheder for at justere antivirusprogrammet til dine behov.

Du finder flere detaljer om dets værktøjer i vores Surfshark Antivirus-anmeldelse. På den anden side mangler tjenesten et par funktioner, der nogle gange er inkluderet sammen med antivirusfunktioner.

Jeg henviser til værktøjer som forældrekontrol og enhedsoprydning, som ikke rigtig er relateret til cybersikkerhed.

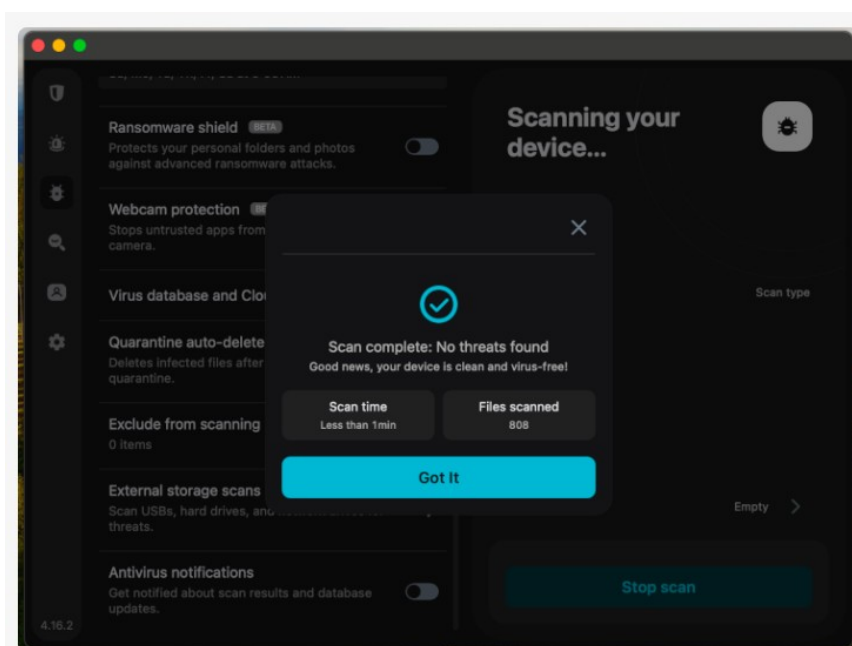
Jeg er faktisk glad for, at Surfshark ikke har sådanne værktøjer, da de kan påvirke enhedens ydeevne negativt. I stedet inkluderer tjenesten kun det essentielle uden nogen overflod. Antivirusgrænseflade

Surfshark Antivirus-grænsefladen indeholder alt, hvad du behøver for at tilpasse beskyttelsesværktøjet til dine behov.



The Surfshark Antivirus interface on the desktop displays an overview of security settings and scan options

Surfshark Antivirus tilbyder et brugerdefineret scanningsværktøj til at analysere hele dit system eller blot dele af det.



Surfshark's Antivirus completed the scan on the desktop, displaying results with recommended actions

Læs mere her : <https://cybernews.com/best-vpn/surfshark-review>

Browser extensions Chrome, Firefox, Edge, Brave