

Patch management

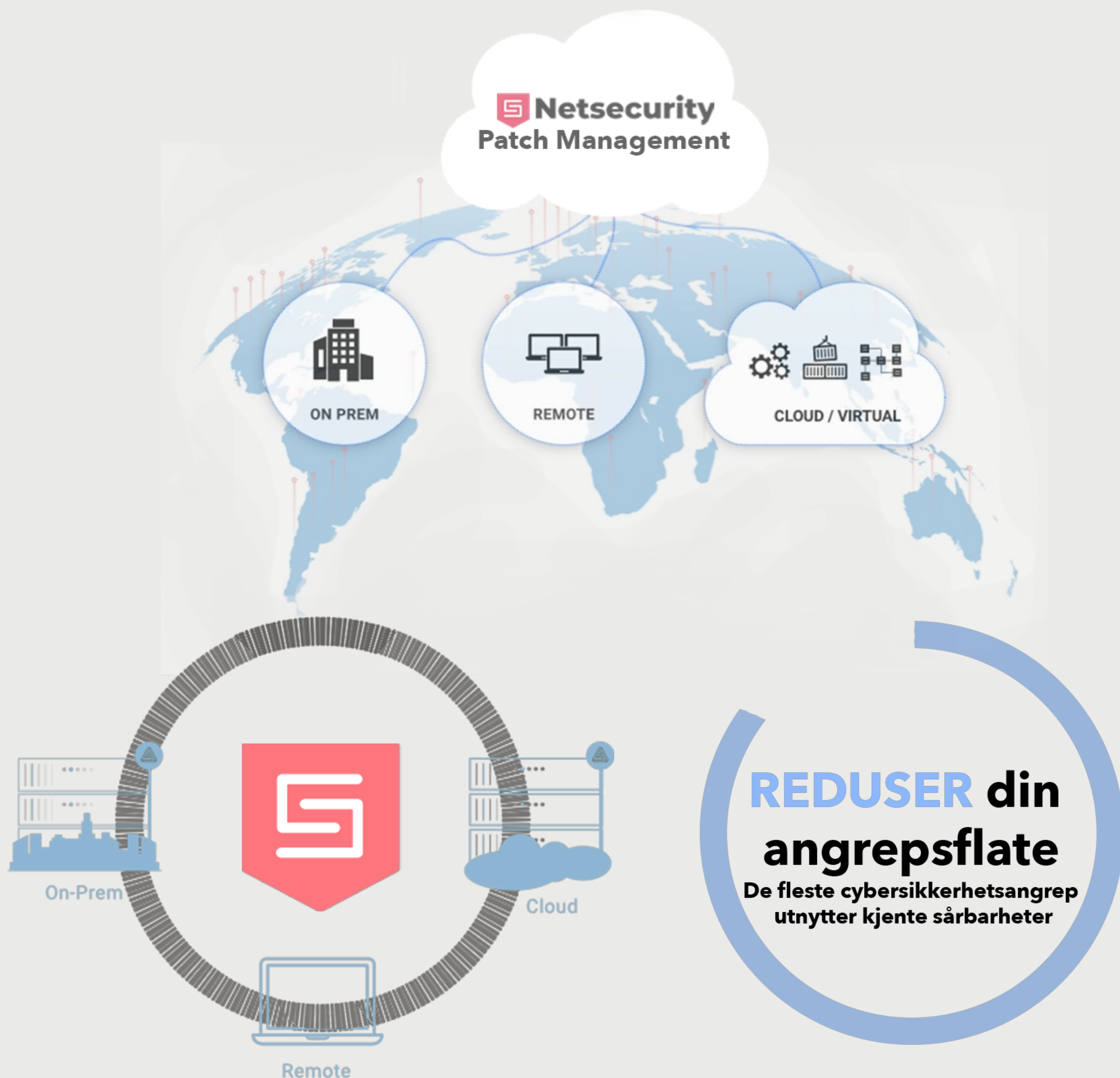
Sikkerhetshåndtering av endepunkt



Hvorfor bruke tjenesten?

Patch management tjenesten fra Netsecurity bistår virksomheter med;

- / Redusere behov for bemanning til å ivareta endepunkter og holde dem oppdatert
- / Redusere behov for spesialiserte verktøy og infrastruktur for å ivareta endepunkt og holde dem oppdatert
- / Redusere behov for arbeid på kvelder og i helger
- / Herding og sikring av endepunkter
- / Ha oversikt over status, sårbarheter og risiko på endepunkter





Hva omfatter tjenesten?

- / Kontinuerlig patching av OS og tredjeparts programmer; Windows, MacOS og Linux.
 - / Automatisk håndheving av patching, basert på forskjellige policyer.
 - / Alltid oppdatert oversikt over endepunkt;
 - Installert programvare og operativsystem
 - Versjons- og oppdateringsnivå for installert programvare og operativsystem
 - Anbefalinger om oppdateringer av programvare og operativsystem
 - / 24/7/365 bemannet overvåking av innrullerte endepunkt med deteksjon av avvik, feil og kritiske sårbarheter.
 - / Varslinger fra Netsecurity
 - ved feil i oppdateringer
 - ved avvik fra policy
 - ved nye kritiske oppdateringer som berører kunden
 - / Månedlige rapporter.
 - / Kontinuerlig oppfølging og dialog rundt status, utfordringer og tiltak.
 - / Rikt API, for integrasjoner med andre systemer og løsninger.
-

Hvordan leveres tjenesten?

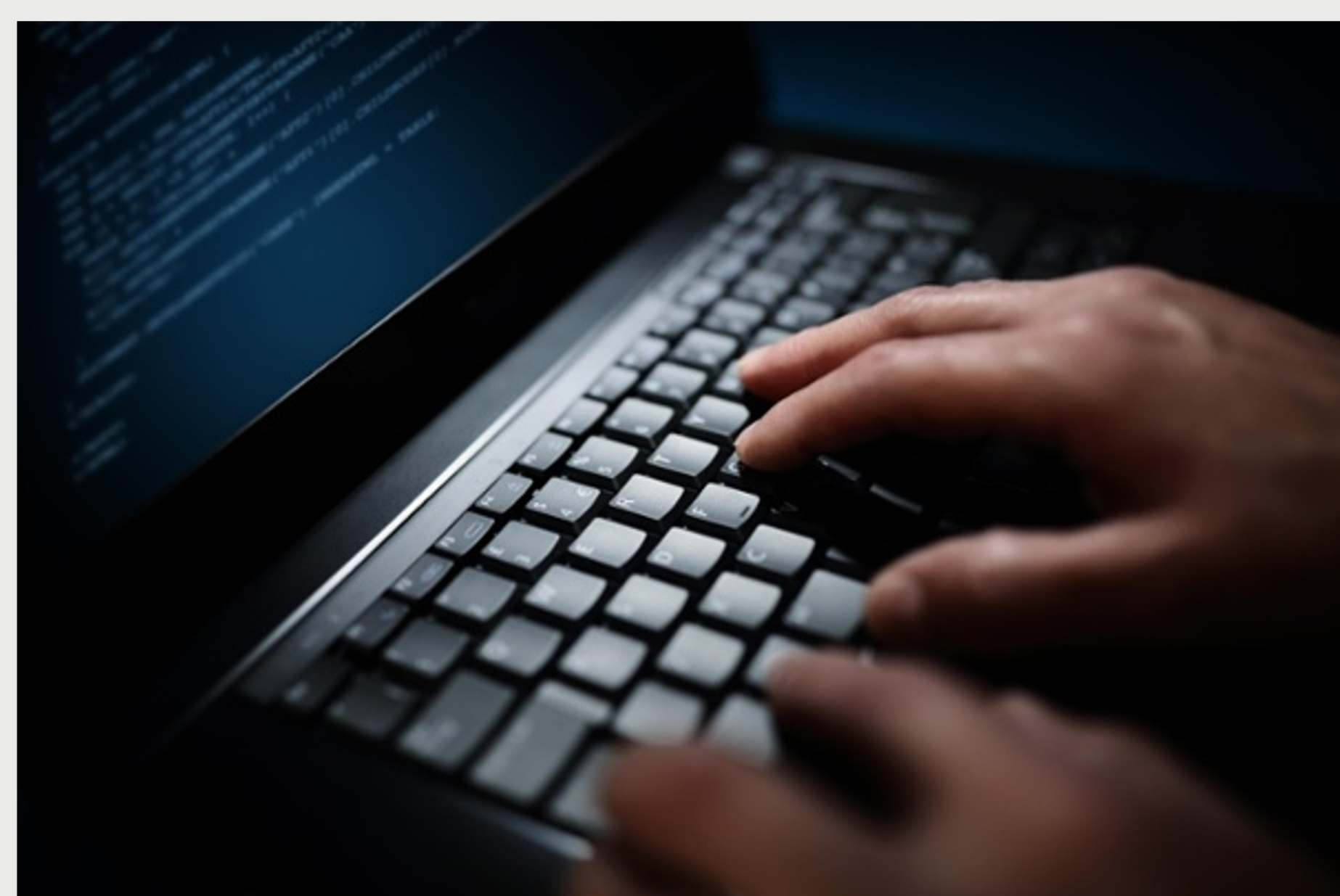
- / Tjenesten leveres 24/7/365 med bemanning av kompetent personell fra Netsecuritys Secure Operations senter.
- / Tjenesten overvåkes, og alle avvik og hendelser detekteres og håndteres i henhold til avtalt SLA.
- / Kunder varsles ved avvik, etter avtalte rutiner og varslingskjeder, innen avtalt SLA.
- / Månedlige standard rapporter utarbeides, oversendes og gjennomgås i status og oppfølgingsmøter. Skreddersydde rapporter kan også leveres ved behov.
- / Tjenesten omfatter alle innrullerte endepunkt. Netsecurity kan bistå med innrulling av endepunkt.

Relaterte tjenester fra Netsecurity



Hendelseshåndtering

De fleste bedrifter og organisasjoner må forholde seg til og forberede seg på sikkerhetshendelser. Dette kan være alt fra hacking, datainnbrudd og distribuert tjenestenekt til løsepengevirus, skadevare og ulike typer virusutbrudd.

[LES MER](#)

Penetrasjonstesting

Vi simulerer hvordan en målrettet angriper vil angripe dine systemer og din organisasjon. Dette gir et godt bilde av hvilken forretningsrisiko som eksisterer i organisasjonen, og tillater deg å rette opp i problemene før de blir utnyttet av andre.

[LES MER](#)

Vil du ha råd om hvordan du kan ta vare på IT-sikkerheten i din bedrift?

**Netsecurity**
Sentralbord:
+47 95 55 15 15

Jostein Angeltvedt
/Sales Director
 +47 901 53 913
 jostein@netsecurity.no

**Netsecurity**
Sentralbord:
+47 95 55 15 15

Frank Kirkeng
/Driftsjef
IT Secure Operations Manager
 +47 489 93 728
 frank.kirkeng@netsecurity.no

/ Netsecurity

Oslo
Strandveien 35
1366 Lysaker

Kristiansand
Dronningensgt. 12
4630 Kristiansand

Bergen
Sandviksbodene 1
5035 Bergen

Grimstad
Bark Silas vei 5
4876 Grimstad

Sandnes
Koppholen 6
4313 Sandnes

 95 55 15 15

 post@netsecurity.no

 www.netsecurity.no