Tjänstebeskrivning: Secure Endpoint

Av denna Tjänstebeskrivning framgår vad som gäller för tjänsten Secure Endpoint .

Tjänsten

Secure Endpoint är ett molnbaserat klientskydd som förebygger, upptäcker och skyddar mot skadlig kod i filer och i RAM-minne genom analys och sandboxning.

Skadliga programvaror upptäcks i realtid genom att en lokal mjukvara installeras på varje klientenhet. Denna mjukvara uppdateras därefter automatiskt.

Secure Endpoint granskar kontinuerligt alla filer som hanteras i de enheter i kundens nätverk som har mjukvaran installerad. Genom en kombination av historisk information och avancerad logik i analysarbetet och att alla aktiviteter i nätverket registreras, följs alla aktiviteter (även retroaktivt) vilket möjliggör isolering och borttagande av malware som redan finns i kundens miljö.

I tjänsten ingår ett molnbaserat webbgränssnitt som ger en översikt över alla upptäckta hot och där ges möjlighet att övervaka enheternas nätverkstrafik och isolera infekterade enheter.

Automatisk scanning sker av de mjukvaror som finns i kundens infrastruktur och som har installerat klientskyddet, och med information om att de mjukvaror som klassas som sårbara för attacker bör uppdateras.

Policy

I webbgränssnittet har kundens administratör möjlighet att sätta kundunika policys och även gruppera enheterna beroende på funktion, plats eller andra kriterier. Möjlighet att generera en uteslutningslista som godkänner specifika filer som inte ska spärras.

Rapporter

Kunden kan ta fram rapporter över antal enheter som är anslutna till AMP. I webb-gränssnittet är det även möjligt att få en summering av antal skannade filer, misstänkta aktiviteter och filer satta i karantän fördelat på önskade perioder. Rapporten kan anpassas efter önskat innehåll och skickas ut automatiskt till rapportägaren i ett förutbestämd intervall. Webbgränssnittet synliggör även de program som klassas som sårbara för attacker och bör uppdateras.

Tekniska förutsättningar

Tjänsten är molnbaserad och kräver ingen dedikerad utrustning, Klientskyddet som ingår installeras på kundens egna enheter och kräver ett av följande operativsystem:

Microsoft

- Windows 7
- Windows 8, 8.1
- Windows 10, 11
- Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019, 2022

Apple

- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur
- macOS 12 Monterey

Servicenivå

Kundens avtalade servicenivå (SLA) för FC/FB gäller för tjänsten.

Leveransvillkor/ansvarsfördelning

Bredband2 ansvarar för att:

- tillhandahålla en kontaktperson som ansvarar för leveransen av tjänsten.
- tillgång till en snabbguide på svenska för installationen på enheterna.
- tillgång till webbgränssnitt för administration av tjänsten.
- tillgång till support vid behov rörande installation av klientskyddet på godkända enheter.
- säkerställa att det finns en generell säkerhetspolicy för klientskyddet tillgänglig som är lämplig för majoriteten av företag inom segmentet 10-250 användare.
- tjänstens webbgränssnitt är tillgänglig samt uppfyller alla certifieringskrav från Cisco.
- debitera tjänsten månadsvis baserat på den volym av klientskydd som installerats.

Kund ansvarar för att:

- utse en kontaktperson inom den egna organisationen som finns tillgänglig under hela implementeringsfasen.
- i tjänstens webbgränssnitt följa och besluta om åtgärder rörande eventuella larm om skadlig kod som inte hanteras automatiskt.
- besluta och genomföra eventuella uppgraderingar eller avslutande av de mjukvaror som flaggas upp som sårbara för attacker.
- säkerställa internetåtkomst via HTTPS för enheter med tjänsten installerad.
- installera/avinstallera klientskyddet på berörda enheter.
