Rapport

GoToAssist® CORPORATE

Sikkerhetsrapport for Citrix GoToAssist Corporate

GoToAssist Corporate er et robust sikkerhetssystem som gir fullstendig beskyttelse mot både passive og aktive angrep på konfidensiell informasjon, integritet og tilgjengelighet.

CITRIX® | online

Innholdsfortegnelse

Omfang og målgruppe

Denne rapporten er for Citrix® GoToAssist® Corporate-kunder og andre involverte som må forstå hvordan GoToAssist påvirker informasjonssikkerhetsrisiko og -samsvar i miljøet.

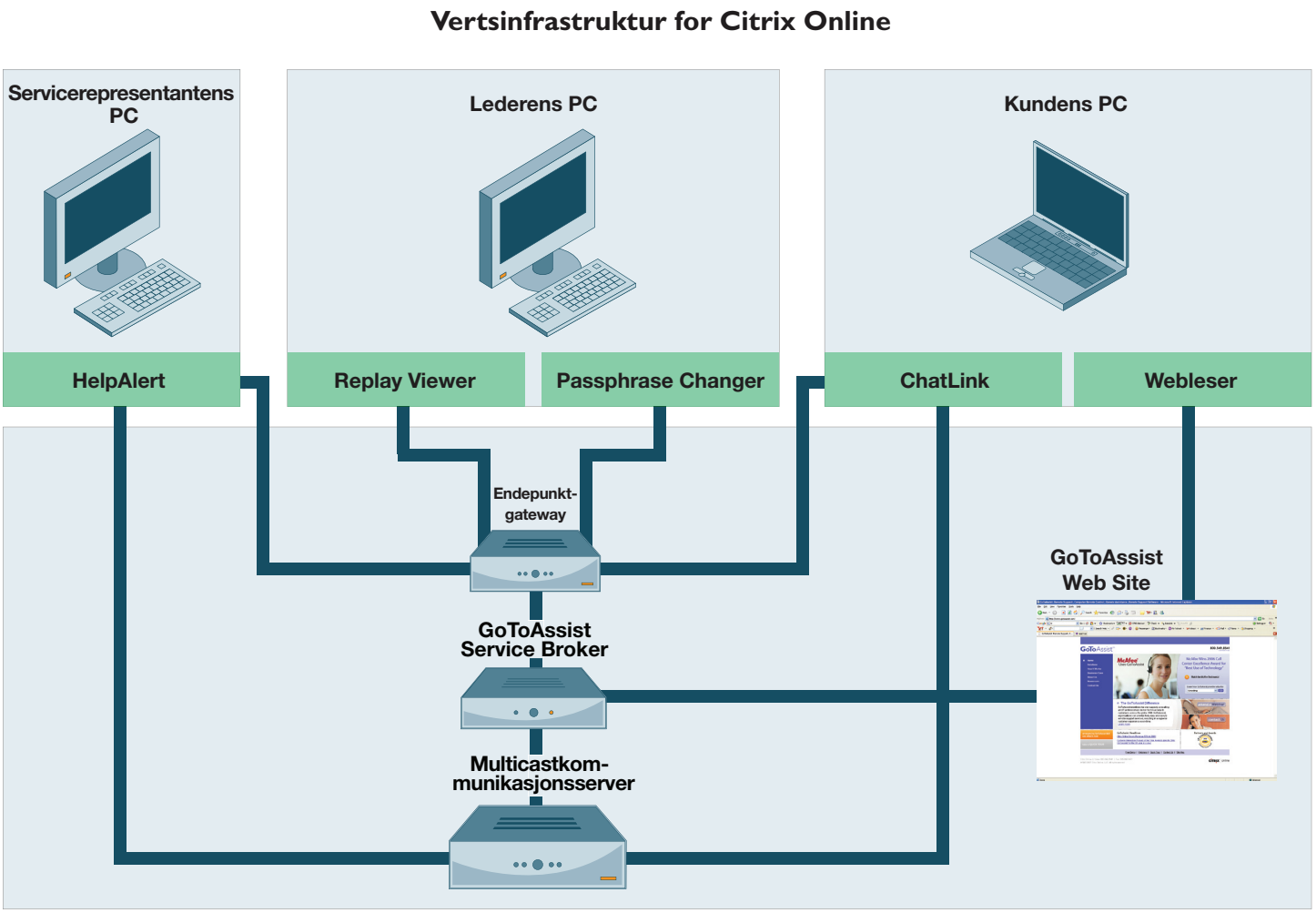
Introduksjon

GoToAssist Corporate er en vertstjeneste hvor man kan gi ekstern støtte til Windows-baserte datamaskiner. Med GoToAssist Corporate kan en bruker be om hjelp fra en kundestøtterepresentant og deretter tildele den representanten rettigheter til å se og eventuelt kontrollere sluttbrukerens PC eksternt.

Dette dokumentet fokuserer på informasjonssikkerhetsfunksjonene til GoToAssist Corporate. Det antas at leseren har en grunnleggende forståelse av produktet og dets funksjoner. Du finner tilleggsinformasjon om GoToAssist Corporate på webområdet www.citrixonline.com eller ved å kontakte en Citrix Online-representant.

Arkitekturen bak tjenesten GoToAssist Corporate

Diagrammet nedenfor gir deg en skjematisk oversikt over alle større tjenestekomponenter og kommunikasjonsstier i GoToAssist Corporate.



Definisjoner

HelpAlert: Kjørbart Win32-program som ligger på servicerepresentantens datamaskin. Med dette programmet kan representanten motta og svare på innkommende forespørsler fra kunder.

ChatLink: Endepunktprogram som brukes til tekstbasert kommunikasjon mellom en kunde og en servicerepresentant.

Webleser: Vanlig webleser, for eksempel Firefox, Internet Explorer osv.

Replay Viewer: Endepunktprogram som brukes av bedriftsledere, teamledere og ledere for kundestøtterepresentanter til å spille av økter som er tatt opp av GoToAssist Corporate. Replay Viewer kan spille av deling av eksterne og lokale skjermer, chat og ekstern diagnostikk.

Passphrase Changer: Endepunktprogram som brukes til å endre passordet som beskytter den krypterte tilgangen til øktopptak.

GoToAssist Web Site: Webbasert program som gir tilgang til GoToAssist-webområdet og webbaserte interne og eksterne administrasjonsportaler.

GoToAssist Service Broker: Webbasert program som utfører funksjonene for konto- og tjenesteadministrasjon, fast lager og rapportering i GoToAssist Corporate.

Multicastkommunikasjonsserver: Én av en rekke globalt distribuerte servere som brukes til å utføre en rekke høyt tilgjengelige kommunikasjonstjenester for unicast og multicast.

Endepunktgateway: En spesialutviklet gateway som brukes av ulike endepunktprogrammer for å gi sikker tilgang til GoToAssist Service Broker for en rekke formål ved hjelp av eksterne prosedyrekall.

Programsikkerhet

GoToAssist Corporate gir tilgang til en rekke forskjellige ressurser og tjenester. Dette gjøres ved hjelp et rollebasert tilgangskontrollsystem som håndheves av de ulike tjenesteleveringskomponentene. Rollene og de tilhørende uttrykkene defineres i tabellen nedenfor:

Roller

Administrator (eller admin)	En ansatt ved Citrix Online som lager grupper og portaler i styringssenteret for GoToAssist Corporate. Administratorer kan opprette, endre og slette GoToAssist Corporate-kontoer, -portaler, -bedriftsledere og teamledere og endre informasjon om abonnement og prising, i tillegg til å utføre andre administrative oppgaver.
Bedrift	GoToAssist Corporate-kunde som det opprettes portaler for.
Bedriftsleder	En ansatt i kundebedriften som har tilgang til bedriftens styringssenter for GoToAssist Corporate. Har lov til å endre kontoer, portalteam og representanter som er tilknyttet kontoen.
Kunde	Personen som ber om kundestøtte fra kundebedriften via GoToAssist Corporate.
Gruppe/team	En samling representanter som er tilknyttet en bestemt portal. Hver representant tilhører akkurat én gruppe eller ett team, og hver gruppe eller hvert team er tilknyttet akkurat én portal. Grupper/team har noen standardinnstillinger for representanter.
Gruppeleder/teamleder	En ansatt hos kunden som er gitt rettigheter av en bedriftsleder til å endre visse deler av teamet og teamets portal og representanter.
Representant	Kundestøttemedarbeideren som svarer på kundeforespørsler via HelpAlert.

Godkjenning

GoToAssist Corporate-administratorer, -ledere og -representanter godkjennes ved hjelp av et kontonavn og et sterkt passord.

Passord styres av følgende retningslinjer:

Sterke passord: Et sterkt passord er minst 8-32 tegn langt og må inneholde noe fra minst tre av disse fire kategoriene: store bokstaver [A-Z], små bokstaver [a-z], tall [0-9] og spesialsymboler [~`!@#$%^&*()_-+={}[]|\:;"'<>,.?/]. Sterke passord kan ikke være det samme som påloggingsnavnet eller det faktiske fornavnet eller etternavnet til kontoinnehaveren. Passordstyrken sjekkes når passordet opprettes eller endres.

Utløpsperioden til passord: Du kan konfigurere utløpsperioden til passord (min.: 10 dager, maks.: 120 dager, standard: 90 dager). Hvis kontoinnehaveren logger på etter at passordet er utløpt, må han eller hun endre passordet sitt.

Passordhistorikk: Passordene lagres i en historikk. Et passord kan ikke endres til et passord som allerede eksisterer i passordhistorikken. Du kan konfigurere dybden til passordhistorikken (min.: 1, maks.: 5, standard: 3).

Kontoutestengning: Etter tre mislykkede påloggingsforsøk på rad blir kontoen automatisk satt i en myk utestengningstilstand. Dette betyr at kontoinnehaveren ikke kan logge på før en angitt tidsperiode er forløpt (min.: 5 minutter, maks.: 30 minutter, standard: 5 minutter). Etter at utestengningsperioden er over, kan kontoinnehaveren på nytt forsøke å logge på kontoen sin.

Systemet kan også konfigureres til å bruke hard utestengning. Etter et angitt antall mislykkede påloggingsforsøk blir kontoen satt i en hard utestengningstilstand. Dette betyr at kontoinnehaveren ikke kan logge på kontoen sin før passordet til kontoen er tilbakestilt av en annen kontoinnehaver med tilstrekkelige rettigheter. En hard utestengning aktiveres etter et angitt antall forsøk (min.: 10, maks.: 50, standard: 10).

Beskyttelse av kundens PC og data

En veldig viktig del av GoToAssist Corporates sikkerhet er den tillatelsesbaserte kontrollmodellen. Den beskytter tilgangen til kundens PC og dataene som befinner seg på den.

Først må alle GoToAssist Corporate-økter initieres av den eksterne kunden. GoToAssist Corporate er ikke laget for ubemannede kundestøttesituasjoner.

Deretter blir alltid kunden spurt om tillatelse før det startes skjermdeling, ekstern kontroll eller overføring av diagnostikkdata, filer eller annen informasjon.

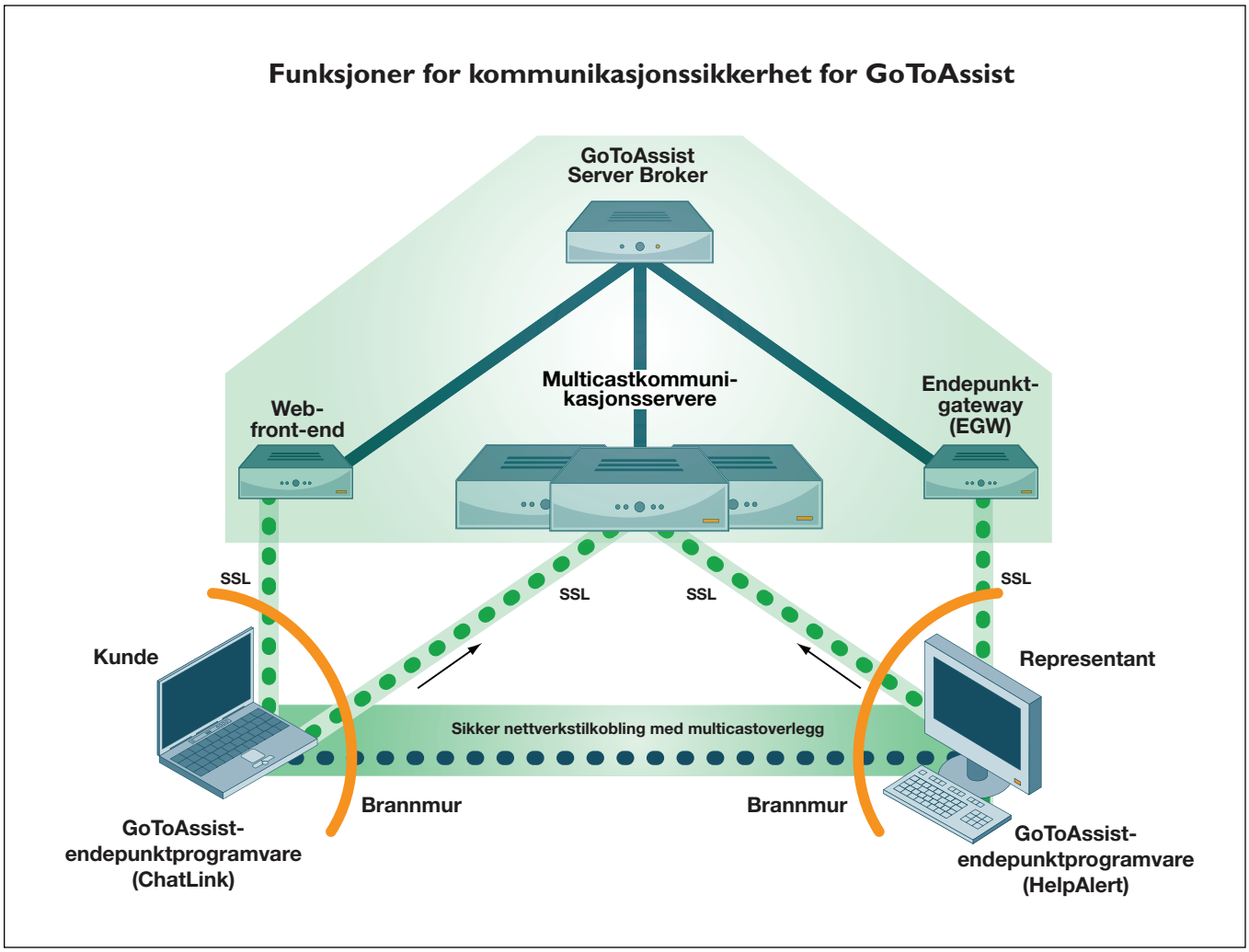
Hvis ekstern kontroll eller skjermdeling tillates, kan kunden til enhver tid se hva representanten gjør. Videre er det enkelt for kunden å ta tilbake kontrollen eller avslutte økten når som helst.

Lokale sikkerhetskontroller på kundens PC blir aldri overstyrt. Kunden eller representanten må fremdeles oppgi godkjenningsopplysninger til Windows eller andre programmer.

Til slutt blir all aktivitet som har skjedd i forbindelse med tilkoblingen, logget. Skjermdelingen og chatøkten kan hvis ønskelig spilles inn og spilles av for gjennomgang på et senere tidspunkt.

Funksjoner for kommunikasjonssikkerhet

Kommunikasjonen som foregår mellom deltakere i en GoToAssist Corporate-økt, skjer via en multicastnettverksstakk som legger seg på toppen av den vanlige TCP/IP-stakken på brukerens PC. Dette nettverket realiseres av en samling Multicast Communication Servers (MCS) som drives av Citrix Online. Denne kommunikasjonsarkitekturen oppsummeres på figuren nedenfor.



Deltakere i en GoToAssist Corporate-økt ("endepunkter") kommuniserer med Citrix Onlines infrastrukturkommunikasjonsservere og gatewayer ved hjelp av utgående TCP/IP-tilkoblinger over portene 8200, 443 og 80. Siden GoToAssist Corporate er en webbasert vertstjeneste, kan deltakere befinne seg hvor som helst på Internett – på et eksternt kontor, hjemme, i et forretningssenter eller koblet til nettverket til en annen bedrift.

Tilgang til GoToAssist Corporate-tjenesten når som helst og hvor som helst gir maksimal fleksibilitet og maksimale tilkoblingsmuligheter. For å sikre at privat forretningskommunikasjon er konfidensiell og sikker, inneholder imidlertid GoToAssist Corporate solide funksjoner for kommunikasjonssikkerhet.

Kommunikasjonens konfidensialitet og integritet

GoToAssist Corporate er et sikkerhetssystem som gir ekte beskyttelse fra ende til ende mot både passive og aktive angrep på konfidensiell informasjon, integritet og tilgjengelighet. Alle tilkoblinger i GoToAssist Corporate er kryptert fra ende til ende og er bare tilgjengelige for autoriserte deltakere i kundestøtteøkten.

Data fra delte skjermer, kontrolldata fra tastatur/mus og tekstinformasjon fra chat blir aldri eksponert i ukryptert form mens det midlertidig befinner seg på kommunikasjonsserverne til Citrix Online, eller under overføring i offentlige eller private nettverk.

Når opptaksmuligheten er deaktivert, lagres ikke GoToAssist Corporate-øktnøkkelen på Citrix Online-serverne i noen form. Dermed vil ikke innbrudd på en server avsløre nøkkelen for noen kryptert flyt som inntrengeren kan ha funnet.

Når opptaksmuligheten er aktivert, blir data fra chat, skjermdeling og skjermvisning lagret i kryptert form. Øktnøkkelen lagres også, men den er beskyttet av 1024-biters RSA-kryptering med offentlig/privat nøkkel. En offentlig nøkkel som er spesifikk for portalen, brukes til å kryptere øktnøkkelen før den lagres. For å spille av trenger du tre elementer: opptaket av økten, den krypterte øktnøkkelen og portalens private nøkkel.

Kommunikasjonens sikkerhetskontroller er basert på sterk kryptografi og implementeres i to lag: TCP-laget og MPSL-laget (Multicast Packet Security Layer).

Sikkerhet i TCP-laget

SSL- (Secure Sockets Layer) og TLS-protokoller (Transport Layer Security) følger IETF-standarden og brukes til å beskytte all kommunikasjon mellom endepunkter. For å gi maksimal beskyttelse mot avlytting, modifisering eller avspillingsangrep finnes det bare én SSL-sifferserie som støtter TCP-tilkoblinger som ikke går mot webområder. Det er 1024-biters RSA med 128-biters AES-CBC og HMAC-SHA1. For maksimal kompatibilitet med nesten alle weblesere som kan befinne seg på PCene til brukere, støtter imidlertid GoToAssists webområde inngående tilkoblinger ved hjelp av de fleste støttede SSL-sifferseriene. For kundenes egen beskyttelse anbefaler Citrix Online at de konfigurerer webleserne sine til å bruke sterk kryptografi som standard når det er mulig, og at de alltid installerer de nyeste sikkerhetsoppdateringene til operativsystemet og webleseren.

Når SSL-/TLS-tilkoblinger opprettes til GoToAssists webområde og mellom komponentene i GoToAssist Corporate, godkjenner Citrix Online-servere seg selv for klienter ved hjelp av sertifikater med offentlig nøkkel fra VeriSign/Thawte. For ekstra beskyttelse mot angrep på infrastrukturen brukes en gjensidig sertifikatbasert godkjenning på alle tilkoblinger mellom servere (f.eks. MCS-til-MCS, MCS-til-Broker). Disse sterke godkjenningstiltakene hindrer mulige angripere fra å utgi seg som infrastrukturservere eller gå inn i støtteøktkommunikasjon.

Multicast packet-sikkerhetslag

Ekstra funksjoner gir fullstendig sikkerhet fra ende til ende for multicastpakkedata, uavhengig av den sikkerheten som SSL/TLS gir. Mer nøyaktig blir alle data fra multicastøkter beskyttet av krypterings- og integritetsmekanismer fra ende til ende. Disse hindrer at noen med tilgang til kommunikasjonsserverne våre (både venner og fiender) kan lytte til en GoToAssist Corporate-økt eller manipulere data uten at dette oppdages. Dette ekstra nivået med kommunikasjonskonfidensialitet og -integritet er unikt for GoToAssist Corporate. Bedriftens kommunikasjon er aldri synlig for en tredjepart. Dette gjelder både brukere som ikke er invitert til en bestemt kundestøtteøkt, og Citrix Online selv.

MPSL-nøkler blir opprettet ved hjelp av en SRP-6-godkjent nøkkelavtale som er basert på offentlige nøkler, og som bruker en 1024-biters modulus til å etablere en primær krypteringsnøkkel. (Se http://srp.stanford.edu/design.html.) Denne krypteringsnøkkelen brukes deretter til distribusjon av den symmetriske gruppenøkkelen ved hjelp av AES-algoritmen for primærnøkler, IETF RFC 3394. Alt nøkkelmateriale genereres ved hjelp av en pseudotilfeldig nummergenerator som er i samsvar med FIPS. Denne fôres med entropidata som samles inn fra flere kilder på vertsmaskinen under kjøring. Disse sterke metodene for dynamisk opprettelse og utveksling av nøkler gir god beskyttelse mot gjetting og knekking av nøkler.

MPSL beskytter multicastpakkedata mot avlytting ved hjelp av en 128-biters AES-kryptering i Counter-modus. Data i ren tekst blir komprimert før de krypteres ved hjelp av proprietære teknikker som har høy ytelse og optimaliserer båndbreddebruken. Beskyttelse av dataintegritet iverksettes ved at man legger til en integritetssjekkverdi som genereres med HMAC-SHA-1-algoritmen. Siden GoToAssist Corporate bruker svært sterke kryptografiske metoder som følger bransjestandard, kan kundene være sikre på at data fra kundestøtteøkter som overføres over multicast, beskyttes mot uautorisert avdekking eller endring som ikke oppdages.

Det er heller ingen ekstra kostnader, redusert ytelse eller byrde på brukerne i forbindelse med disse viktige funksjonene for kommunikasjonssikkerhet. Høy ytelse og datasikkerhet basert på standarder er "innebygd" i alle GoToAssist Corporate-økter.

Nøkkelpunkter

- 128-biters AES-kryptering brukes til konfidensialitet under øktene.
- Den første øktnøkkelen blir tilfeldig valgt av Broker og sendes deretter til endepunktene gjennom godkjente og krypterte kanaler.
- Endepunktene forhandler deretter frem en endelig øktnøkkel som brukes mellom dem.
- Broker kjenner ikke til den endelige øktnøkkelen.
- Kommunikasjonsservere sender bare krypterte pakker og har ikke krypteringsnøkkelen for økten.
- Arkitekturen til GoToAssist Corporate minimerer risikoen for at øktdata kan avdekkes, mens den maksimerer evnen til å koble representerer til de som trenger hjelp.

Brannmur- og proxy-kompatibilitet

På samme måte som andre Citrix Online-produkter følger det med innebygd gjenkjenning av proxy-servere og administrasjonslogikk for tilkoblinger i GoToAssist Corporate. Dette gjør det enklere å installere programvare automatisk, man unngår komplisert (re)konfigurasjon av nettverk, og brukernes produktivitet maksimeres. Brannvegger og proxy-servere som allerede befinner seg i nettverket, trenger vanligvis ingen spesiell konfigurering for at GoToAssist Corporate skal fungere.

Når endepunktprogramvaren i GoToAssist Corporate startes, forsøker den å kontakte GoToAssists Service Broker via endepunktgatewayen (EGW) ved at den setter opp én eller flere utgående SSL-beskyttede TCP-tilkoblinger på portene 8200, 443 og/eller 80. Den tilkoblingen som svarer først, blir brukt, og de andre tilkoblingene slippes. Denne tilkoblingen utgjør grunnlaget for alle fremtidige kundestøtteøkter ved at den gjør det mulig med kommunikasjon mellom vertsservere og brukerens skrivebord.

Når brukeren forsøker å koble seg til en kundestøtteøkt, oppretter GoToAssist Corporates endepunktprogramvare én eller flere ekstra tilkoblinger til Citrix Onlines kommunikasjonsservere, igjen ved hjelp av SSL-beskyttede TCP-tilkoblinger på portene 8200, 443 og/eller 80. Disse tilkoblingene frakter data fra kundestøtteøkter mens økten er aktiv.

I tillegg oppretter endepunktprogramvaren, for oppgaver i forbindelse med optimalisering av tilkobling, også én eller flere kortvarige TCP-tilkoblinger på portene 8200, 443 og/eller 80 som ikke er SSL-beskyttet. Disse nettverksprobene inneholder ingen informasjon av sensitiv art eller informasjon som kan utnyttes, og det er ingen risiko for at sensitiv informasjon kan avdekkes.

Du finner en fullstendig liste over seriene med IP-adresser som brukes av Citrix Online, på www.citrixonline.com/iprange.

Ved å automatisk justere forholdene i lokalnettverket med bare utgående tilkoblinger og ved å velge en port som allerede er åpen i de fleste brannmurer og proxy-servere, er GoToAssist Corporate svært kompatibel med sikkerhetstiltak som allerede finnes i nettverket. I motsetning til enkelte andre produkter krever ikke GoToAssist Corporate at bedriftene må deaktivere eksisterende sikkerhetskontroller for nettverksgrenser for å tillate kommunikasjon i webbaserte kundestøtteøkter. Disse funksjonene maksimerer både kompatibiliteten og den generelle nettverkssikkerheten.

Sikkerhetsfunksjoner i endepunktsystem

Programvare for webbaserte kundestøtteøkter må være kompatibel med en rekke forskjellige skrivebordsmiljøer, men samtidig må den skape et sikkert endepunkt på PCen til hver bruker. GoToAssist Corporate gjør dette ved hjelp av nedlastbare, kjørbare filer som bruker sterke kryptografimetoder.

Signert endepunktprogramvare

Endepunktprogramvaren for GoToAssist Corporate-klienter er en kjørbar Win32-fil som lastes ned til brukernes PC. En digitalt signert Java-applet brukes til å kontrollere nedlastningen og til å sjekke integriteten til endepunktprogramvaren for GoToAssist Corporate fra Citrix Online-serverne. Dette forhindrer at brukeren ved en feiltakelse installerer en trojansk hest eller annen skadelig programvare som utgir seg for å være GoToAssist Corporate-programvare.

Endepunktprogramvaren består av flere kjørbare Win32-filer og dynamisk koblede biblioteker (DLLer). Citrix Online følger en streng kvalitetskontroll og strenge prosedyrer for konfigurasjonsadministrasjon under utvikling og distribusjon for å sørge for sikkerheten til programvaren. Endepunktprogramvaren eksponerer ingen eksternt tilgjengelige nettverksgrensesnitt og kan ikke brukes av skadelig programvare eller virus til å utnytte eller infisere eksterne systemer. Dette beskytter andre PCer som deltar i en kundestøtteøkt, mot infisering av en skadet vert som brukes av en annen deltaker.

Implementering av det kryptografiske undersystemet

Alle kryptografiske funksjoner og sikkerhetsprotokoller som brukes av endepunktprogramvaren for GoToAssist Corporate-klienten, implementeres ved hjelp av de aller nyeste Certicom Security Builder® Crypto™- og Certicom Security Builder® SSL™-bibliotekene. Dette gir god sikkerhet og høy ytelse. (Se www.certicom.com hvis du vil ha mer informasjon.)

De kryptografiske bibliotekene kan bare brukes av endepunktprogrammet for GoToAssist Corporate. Ingen eksterne APIer eksponeres slik at annen programvare som kjører på PCen, kan bruke disse. Alle krypterings- og integritetsalgoritmer, nøkkelstørrelse og andre regelparametre som brukes til kryptografi, blir statisk kodet når programmet kompileres. Siden sluttbrukeren ikke kan konfigurere noen av de kryptografiske innstillingene, er det ikke mulig for brukere å redusere øktsikkerheten for GoToAssist Corporate ved tilfeldig eller overlagt feilkonfigurering. En bedrift som bruker GoToAssist Corporate, kan være sikker på at alle deltakende endepunkter har det samme nivået av sikkerhet i en kundestøtteøkt, uansett hvem som eier eller bruker hver PC.

Sikkerhetsfunksjoner i en vertsinfrastruktur

Citrix Online leverer GoToAssist Corporate ved hjelp av en ASP-modell (Application Service Provider) som er spesialutviklet for robust og sikker drift og sømløs integrering med eksisterende nettverks- og sikkerhetsinfrastruktur i en bedrift.

Skalerbar og pålitelig infrastruktur

Citrix Onlines globale tjenestearkitektur er laget for maksimal ytelse, pålitelighet og skalerbarhet. GoToAssist Corporate-tjenesten drives av høykapasitetsservere som følger bransjestandard, og nettverksutstyr med alle de nyeste sikkerhetsoppdateringene. Redundante svitsjer og rutere er bygget inn i arkitekturen slik at det ikke finnes noen enkeltpunkter som kan få systemet til å bryte sammen. Serverklynger og ekstrasystemer bidrar til å garantere at programprosessene fungerer sømløst – også under tung belastning eller ved systemfeil. For å gi optimal ytelse belastningsbalanserer GoToAssist Broker klient-/serverøktene over kommunikasjonssystemer som er geografisk fordelt.

Fysisk sikkerhet

Alle GoToAssist Corporates web-, program-, kommunikasjons- og databaseservere står i sikre datasentre. Fysisk tilgang til serverne er svært begrenset og overvåkes kontinuerlig. Alle fasilitetene har redundante strømforsyninger og miljøkontroller.

Nettverkssikkerhet

Citrix Online bruker brannmur, ruter og VPN-basert tilgangskontroll til å sikre de private tjenestenettverkene og backend-serverne våre. Sikkerheten til infrastrukturen overvåkes kontinuerlig, og sårbarheten testes jevnlig av internt sikkerhetspersonell og eksterne tredjeparts revisorer.

Kundens personvern

Fordi brukernes tillit er svært viktig for oss, har Citrix Online forpliktet seg til å respektere personvernet ditt. Du finner en kobling til en kopi av de gjeldende retningslinjene for personvern til Citrix GoToAssist Corporate på webområdet for tjenesten på www.citrixonline.com.

Samsvar i regulerte miljøer

På grunn av sitt omfattende sett med sikkerhetskontroller for programmer og kommunikasjon, inkludert den kundeautoriserte, tillatelsesbaserte sikkerhetsmodellen, kan du stole på at du kan bruke GoToAssist Corporate til å støtte datamaskiner og programmer i miljøer som er underlagt HIPAA, Gramm-Leach-Bliley-loven eller Sarbanes-Oxley-forskrifter, som sier at det må finnes robuste kontroller for datakonfidensialitet og -integritet.

Citrix Online anbefaler at organisasjoner går nøye gjennom alle standard og konfigurerbare sikkerhetsfunksjoner i GoToAssist Corporate i forhold til sine egne miljøer, brukere og krav fra retningslinjer, slik at det kan avgjøres hvilke funksjoner som bør være aktivert, og hvordan disse bør konfigureres. I noen tilfeller kan det være fornuftig å informere brukere om ytterligere retningslinjer for bruk, slik at man imøtekommer sikkerhetsmålene til alle de involverte partene. Citrix Onlines team for profesjonelle tjenester kan bistå med ekstra materiale om beste fremgangsmåter for distribusjon og bruk av GoToAssist Corporate.

Konklusjon

GoToAssist Corporates intuitive og sikre grensesnitt og utvalg av funksjoner gjør at dette er den mest effektive løsningen for å utføre webbaserte kundestøtteøkter. Med GoToAssist Corporate kan kundestøtte-, konsulent- og IT-medarbeidere raskt og enkelt gi teknisk hjelp til kunder over hele verden.

Bak teppet gir Citrix Onlines vertstjenestearkitektur gjennomsiktig støtte for samarbeid mellom flere punkter i et sikkert og pålitelig miljø. Som denne rapporten viser, er GoToAssist Corporate brukervennlig og fleksibel uten at man må inngå kompromisser i forhold til integriteten, personvernet eller den administrative kontrollen over forretningskommunikasjon eller IT- ressurser.

Vedlegg: Samsvar med sikkerhetsstandarder

GoToAssist Corporate er i samsvar med følgende bransjestandarder og standarder som gjelder for den amerikanske regjeringen, i forhold til kryptografiske algoritmer og sikkerhetsprotokoller:

- TLS-/SSL-protokollen, versjon 1.0 IETF RFC 2246
- Advanced Encryption Standard (AES), FIPS 197
- (FIPS-validert implementering, NIST-sertifikat nr. 175)
- AES-sifferserier for TLS, IETF RFC 3268
- AES-primærnøkkelalgoritme, IETF RFC 3394
- RSA, PKCS nr. 1
- SHA-1, FIPS 180-1 (FIPS-validert implementering, NIST-sertifikat nr. 89)
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Pseudotilfeldig nummergenerering, ANSI X9.62 og FIPS 140-2

Citrix Online

Citrix Online-avdeling

Produktinformasjon:
www.citrixonline.com

Salgsspørsmål:
Nordic@citrixonline.com
Telefon: (+45) 47334123

Mediespørsmål:
pr@citrixonline.com
Telefon: +441 49 454 1715

www.citrixonline.com

Hvis du vil ha mer informasjon om Citrix GoToAssist Corporate, kan du gå til www.citrixonline.com

Om Citrix Online

Citrix Online leverer sikre og brukervennlige elektroniske løsninger som gjør det mulig å arbeide fra hvor som helst med hvem som helst. Enten du bruker GoToMyPC® for å få tilgang til og arbeide på en ekstern PC, GoToAssist® for å gi kundestøtte eller GoToMeeting® for å arrangere elektroniske møter og webseminarer, opplever kundene våre – mer enn 35 000 virksomheter og mange hundre tusen enkeltpersoner – økt produktivitet, reduserte reisekostnader og bedre salg, opplæring og service over hele verden. Selskapet er en avdeling av Citrix Systems, Inc. (Nasdaq: CTXS) og er basert i Santa Barbara, California. Hvis du vil ha mer informasjon, kan du gå til www.citrixonline.com eller ringe 805-690-6400.

18191/11.17.08/PDF