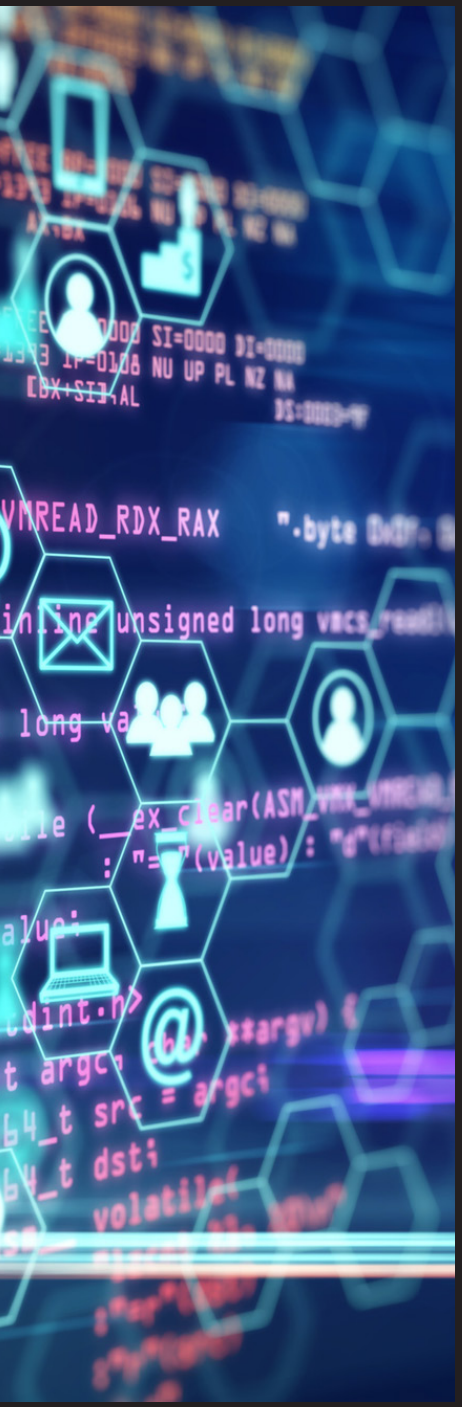

RISKBASERAD AUTENTISERING
Ett kritiskt element i alla
installationer av nollförtroende

INNEHÅLLSFÖRTECKNING

Forrester Research Inc. var först med att mynta termen ”nollförtroende” (zero-trust) år 2010. Nu, ett decennium och en pandemi senare, när företag implementerar hybridmiljöer med kombinationer av flera molnlösningar, kan hanteringen av identiteter och åtkomst inte längre betraktas som ett tillval. Det räcker inte att bara utöka VPN-skyddet.

Riskbaserad autentisering stärker både säkerheten och förbättrar användarupplevelse genom att ni får möjlighet att rangordna vilka resurser ni vill skydda, baserat på risknivå och typ av användare. Det ger er möjlighet att skapa regler som är unika för säkerhetsstrukturen i just er organisation, vilket möjliggör större flexibilitet och starkare skydd endast när det behövs.

I denna e-bok diskuterar vi den kraftfulla kopplingen mellan implementering av nollförtroende och riskpolicyer och hur multifaktorautentisering är central för dessa metoder genom att den tillför synnerligen välbehövlig teknik för att skydda användarnas identiteter och molntillämpningarna.



Varför behövs riskbaserad autentisering?

Användarautentisering

- Något du vet (lösenord, PIN)
- Något du har (hårdvarunyckel, mobiltelefon)
- Något du är (fingeravtryck, ansikte)

Autentisering av användare är ett statiskt sätt att verifiera en användares identitet när hen försöker nå en skyddad resurs. Du kan autentisera med hjälp av enstaka faktor (svag lösning) eller flera faktorer (rekommenderas starkt).

I vår dynamisk värld, där användarnas rörlighet påverkar säkerheten nästan hela tiden, har multifaktorautentisering kommit att bli absolut nödvändigt och en nyckel till att distribution av nätverk med nollförtroende. Varför?

- Användare ansluter till företagets resurser från en rad oskyddade nätverk
- Arbetstiderna har blivit mer flexibla. Olika anställda kan behöva arbeta från tidig morgon till sen kväll
- Enheter kanske har delats med andra familjemedlemmar
- Allt detta innebär att en angripare kommer att försöka utnyttja denna värld av nya möjligheter

Användarautentisering

Riskfaktorer

- **Till vilket nätverk är du uppkopplad?**
- **Är din dator säker?**
- **Är dina mobila enheter säkra?**
- **Var befinner du dig just nu?**
- **Befinner sig din mobil och din dator på samma plats?**

Riskbaserad autentisering tar hänsyn till olika riskfaktorer när ett beslut om autentisering fattas. Det sträcker sig längre än till en statisk autentisering och gör det möjligt för administratörer att skapa regler som kan anpassa autentiseringsbeteendet och ibland förenkla processen när risken är låg, men ibland kräva extra steg för att säkerställa att det är rätt användare, och att blockera åtkomsten om risken skulle vara för hög, även om användaren tillhandahöll ett korrekt engångslösenord (OTP).

Multifaktorautentisering och riskinformation: Optimal användarhantering

Riskbaserad autentisering stärker både säkerheten och förbättrar användarupplevelse genom att ni får möjlighet att rangordna vilka resurser ni vill skydda, baserat på risknivå och typ av användare.
Det ger er möjlighet att skapa regler som är unika för säkerhetsstrukturen i just er organisation, vilket möjliggör större flexibilitet och starkare skydd endast när det behövs.

Exempelvis kan ni välja att tillåta att användarna autentiserar sig med bara användarnamn och lösenord när de är direkt anslutna till företagets egna lokala nätverk, men använda MFA om de arbetar från något annat nätverk. Och det här är definitionen av avancerad användarhantering.

Vanliga risk-faktorer som eventuellt kan inkluderas i autentiserings-policyer

NÄTVERKSPLATS

Ett företagsnätverk kan innehålla alla säkerhetsåtgärder mot yttervärlden, exempelvis brandvägg, säkrat trådlöst nätverk, detektering av hot m.m. Om någon är fysiskt inkopplad på detta nätverk innebär det därför en mindre risk än om någon ansluter från ett annat kontor som har sämre säkerhet, eller när någon ansluter hemifrån.

RISKER MED MOBILA ENHETER

En användares mobila enhet som har komprometterats utgör en säkerhetsrisk för företaget. Ett sätt som säkerheten i en enhet lätt kan äventyras är om en användare utfört jailbreak av en iOS-enhet eller skaffat sig root-behörighet i Android och därmed kringgår operativsystemets säkerhetsåtgärder. En sårbar enhet ökar den sammanlagda risken och bör för det mesta blockeras.

RISK MED SLUTPUNKT/DATOR

Liksom med risken för en mobil enhet kan risken med en slutpunkt eller dator utvärderas för att bedöma vilka åtgärder som ska vidtas. En användare som använder sin egen bärbara dator och med alla skydd intakta, skulle utgöra en låg risk. Om samma användare senare på dagen försöker att ansluta från en okänd dator, kanske via Tor-webbläsare på en Linux-dator, då vore risken mycket högre.

TIDSBASERADE POLICYER

Datum och tid kan användas på olika sätt. Låt oss säga att en av företagets tillämpningar vanligtvis säkerhets-kopieras och underhålls dagligen mellan 01:00 och 03:00. Då skulle tidsbaserade policyer kunna användas för att blockera åtkomst till tillämpningen under denna tid. Ur riskhänseende, om en användare försöker att nå en tillämpning under veckoslutet, eller kanske mitt i natten, kan detta höja riskbedömningen dramatiskt, eftersom det kan vara en hackare som försöker attackera när IT-teamet har ledigt. Därför kan man då vidta extra åtgärder.

Vanliga risk-faktorer som eventuellt kan inkluderas i autentiserings-policyer

GEOGRAFISKA BEGRÄNSNINGAR (GEOFENCING)

Den fysiska platsen kan användas för att spärra åtkomst från specifika länder eller geografiska platser och på detta sätt minska risken för attacker. Ett företag, vars alla kontor och all verksamhet befinner sig i USA kanske vill blockera åtkomsten från andra länder. Åtkomsten till något specifikt program kanske begränsas till det närmaste området runt ett av företagets kontor.

GEOGRAFISK KORRELATION

Det förväntas att en användare som ansluter sig till någon av företagets tjänster har mobiltelefonen i handen. Om en anslutning initieras från en dator i Sao Paulo, Brasilien, samtidigt som telefonen som bekräftar anslutning-en för närvarande finns i Virginia, USA, kan det vara ett tecken på att en hackare försöker att ansluta till en tjänst och samtidigt använder social manipulation för att övertyga en användare att godkänna MFA-autentiseringen.

Även om vissa geolokaliseringar inte är särskilt exakta – en del operatörer styr trafiken via någon annan plats och i vissa Android-telefoner kan GPS-koordinaterna ha manipulerats – kan detta vara ytterligare ett sätt att avstyra potentiella attacker.

GEOKINETIK

Ett annat sätt att använda GPS eller geolokaliseringsfaktorer i riskbedömningen kan vara geokinetik eller för-flyttningshastighet. En användare som autentiserar från Seattle klockan 09:05 lär knappast 25 minuter senare autentisera sig från San Diego, som ligger 2000 km bort. Troligast är att autentisering nummer två försöker att återanvända den första autentiseringen.

Riskpolicyer förebygger överträdelser

Om man inte har etablerat några riskpolicyer måste företaget aktivera den säkraste autentiseringsmetoden hela tiden, för alla användare, något som för vissa segment kan upplevas som besvärande för användarna. Riskautentisering är ett sätt att modernisera er strategi genom att använda just så mycket säkerhet med anpassat riskskydd som låter er förbättrar er förmåga att upptäcka och reagera på hot.

Följande scenarier beskriver fall av potentiella IT-brott som kan förhindras man har aktiverat riskpolicyer.

A

ANVÄNDNING AV STULNA INLOGGNINGSUPPGIFTER

Användaren autentiserar sig regelbundet med användarnamn, lösenord och en engångslösenord. En angripare har lyckats komma över inloggningsuppgifterna på dark net eller via en phishing-attack, men har inte lyckats komma över eller klona hårdvarunyckeln.

- **Attack:** Med hjälp av social manipulation ringer angriparen användaren och övertygar denne att uppge ett engångslösenord. Angriparen skriver in inloggningsuppgifterna och det tidsbaserade engångslösenordet och får åtkomst till den skyddade resursen.

- **Förebyggande riskpolicy:**

  Policyer för datorrisk kan visa att det inte är användarens egen dator som används.

  Policyer för geokinetik skulle eventuellt visa att användaren försöker autentisera från en plats som ligger orimligt långt från platsen för föregående autentisering.

B

iOS JAILBREAK

Användaren loggar in med användarnamn, lösenord och push-meddelande. Användaren hade utfört jailbreak på iPhone, vilket ledde till att en angripare installerat ett spionprogram som ger hen full kontroll. Push-meddelandet skyddas inte med någon PIN-kod eller biometrisk avläsning.

- **Attack:** Angriparen befinner sig i ett annat land och använder stulna inloggningsuppgifter för autentisering, samtidigt som hen övervakar användarens telefon. När push-meddelandet kommer till användarens telefon använder angriparen fjärrstyrningen (RAT/Remote Access Tool) för att godkänna push-meddelandet och få åtkomst till resursen.

- **Förebyggande riskpolicy:**

  Policyer för risk med mobiltelefonen skulle upptäcka att användarens mobila enhet inte är tillförlitlig och inte godkänna neka autentiseringar med den.

  Policyer för geokorrelation skulle konstatera att datorn inte finns på samma plats som mobiltelefonen och även här blockera anslutningen.

MFA är hörnstenen för implementeringen av nollförtroende eftersom lösningen tillhandahåller säkerhetsstrukturen för hanteringen av användare och identiteter samt kontinuerlig autentisering för alla användares åtkomst till alla resurser.

Nollförtroende är omöjligt utan MFA

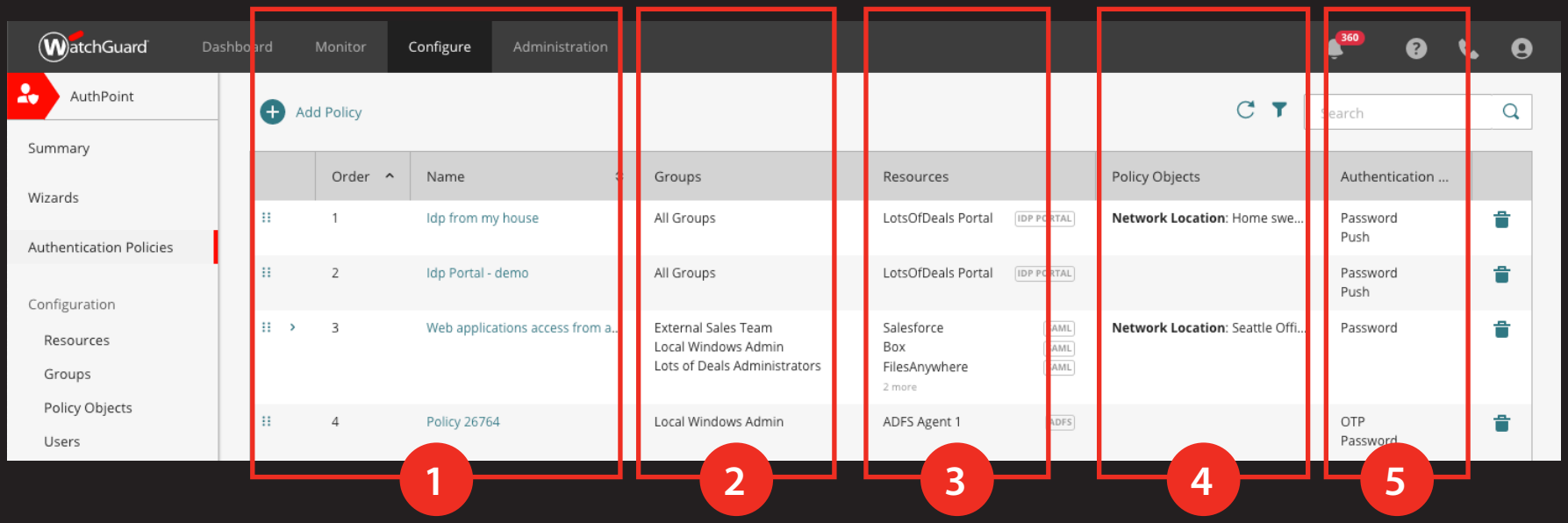
Hantering av identiteter och åtkomsthantering kan inte längre betraktas som ett valfritt tillval. Företagen måste fokusera på starka strategier för användarskydd och -hantering, vilket är de kärnområden som MFA och riskautentisering råder över. Det ger er möjligheten att för företagsnätverket, slutpunkter och molntillämpningar verkligen ta till er tillvägagångssättet att inte lita på någon, utan att användarupplevelsen blir lidande.

Medan traditionella nätverk bygger på en idé om inbyggt förtroende, utgår ett ramverk med nollförtroende från att varje enhet och användare, både i och utanför nätverket, utgör en säkerhetsrisk. Tillvägagångssättet "lita aldrig, verifiera jämt" använder flera skyddsnivåer för att förhindra hot, blockera förflyttningar i sidled och säkerställa detaljerade styrning av användarnas åtkomst.

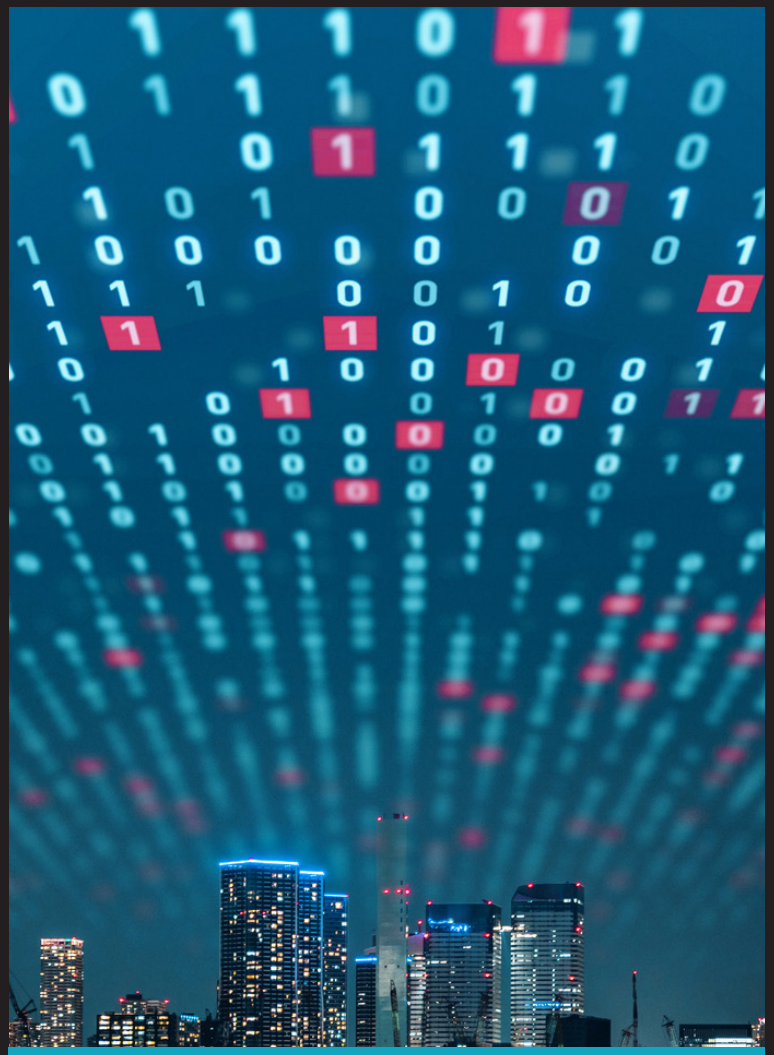
Utifrån grundtanken att man inte kan lita fullt ut på någon eller något, fokuserar lösningen med nollförtroende på tre principer:

Identifiering av användare och enheter	Tillhandahållande av säker åtkomst	Ständig övervakning
Att alltid veta vem och vad som är uppkopplat till företagets nätverk. När företag brottas med att större delen av deras arbetskraft arbetar på distans blir det en stor utmaning att säkra tillgången till de interna verktygen. Molnbaserade tjänster för multifaktorautentisering (MFA/ Multi-Factor Authentication) hjälper till att begränsa effekterna av stulna inloggningsuppgifter, bedrägerier och phishingattacker.	Begränsa åtkomsten till affärskritiska system och program till de enheter som har uttrycklig behörighet att nå dem. I ramverket för nollförtroende är målet med åtkomsthanteringen att tillhandahålla ett sätt att centralt hantera åtkomsten till alla vanliga IT-system, samtidigt som åtkomst ges endast för specifika användare, enheter eller program. SSO-teknik (Single Sign-On) i kombination med multifaktorautentisering kan förbättra åtkomstsäkerheten och minimera besväret med lösenord för användarna.	Övervaka hälsan och säkerheten för nätverket och för alla hanterade slutpunkter. Coronaviruset har bara lett till att hoten från skadlig kod och ransomware har accelererat. Att skydda användarna när de surfar på nätet är svårare när de är uppkopplade utanför företagets nätverk. För att hålla koll på alla hot krävs ständig, avancerad säkerhet som sträcker sig längre än ett antivirusprogram för slutpunkten.

Exempel på användning av riskbaserade autentiseringsprinciper som motsvarar principen om nollförtroende:



1. Policynamnet representerar ett mikrosegment med nollförtroende och kan sorteras efter prioritet och/eller vikt.
2. Grupper av användare som synkroniseras mot Active Directory (eller ej), representerar dem som bör släppas in (och inga andra) till den skyddade resursen.
3. Tillämpning/tillämpningar för mikrosegmentet. Det kan vara ett enstaka program eller flera, om exakt samma policy gäller för alla programmen.
4. Policyobjekt eller riskpolicyer som kan fastställa specifika begränsningar, beroende på nätverk, tid, geolokalisering m.m.
5. Avser vilka autentiseringsmetoder som tillåts, om några alls, eller enbart nekad autentisering, baserat på någon riskfaktor.



Riskpolicyer kan användas för att definiera mer detaljerade regler baserat på dynamiska situationer som bättre stämmer mot de nuvarande trenderna för distansarbete och hybridarbetsmodeller som företag går igenom.

Användning av MFA och riskpolicyer för införande av nollförtroende

Som bekant börjar implementeringen av nollförtroende med antagandet att man inte kan lita på något. Genom att definiera mikrosegment och tillämpa skräddarsydda policyer för organisationens säkerhetsbehov bygger ni upp en betrodd miljö. Det börjar med att man pekar ut användaren som behöver kunna nå dessa program och tjänster.

Ett mikrosegment kan vara ett molnbaserat CRM-system (Customer Relationship Management). Till detta CRM-system kan exempelvis säljteamet och teknisk support behöva åtkomst. Konstruktörsteamet? Antagligen inte, så dem tar vi inte med. Vad gäller supportteamet befinner sig alla medarbetare i samma stad och de arbetar bara under kontorstid, vilket betyder att åtkomsten för denna grupp kanske bör begränsas både geografiskt och tidsmässigt. Och med tanke på hur känsliga uppgifterna i CRM-systemet är ska vi alltid använda MFA.

Om vi lägger in detta i autentiseringskontexten och riskfaktorerna finns det två regler som definierar den riskpolicy som gäller för detta mikrosegment:

REGEL 1 NAMN
CRM FÖR SÄLJTEAMET

Vem har åtkomst: Säljare

Tillämpning: Moln-CRM

Riskbegränsningar: Låg risk mobila enheter, Låg risk geokorrelation

Autentisering: Lösenord + autentisering via push-meddelande

REGEL 2 NAMN
CRM FÖR TEKNISK SUPPORT

Vem har åtkomst: Teknisk support

Tillämpning: Moln-CRM

Riskbegränsningar: Låg risk mobila enheter, Endast kontorstid, Endast USA, låg risk geokorrelation

Autentisering: Lösenord + Autentisering via push-meddelande

Guide för riskbedömning av verksamheten

Genom att bedöma risken i din organisation genom att titta på era potentiella riskscenarier kan ni avsevärt förbättra dessa installationer genom att lägga till dynamiska fakta och analys i beslutet.

UPPRÄTTA ETT RISKFORMULÄR

Vanliga användningsfall för företag, vilka kan hjälpa dig att definiera rätt riskpolicyer:

- ☐ På kontoret: Ansluter era anställda till företagets data och plattformar från kontoret?
- ☐ Fjärranslutet hemmakontor: Har ni många medarbetare som arbetar hemifrån?
- ☐ Fjärransluten från kafé eller kontor som delas med andra företag: Förväntar ni er att era distansarbetare kommer att koppla upp sig till företagets nätverk från kaféer och liknande platser?
- ☐ Resande användare: Har ni några anställda som reser i tjänsten och kan behöva komma åt arbetsplattformarna när du är på språng?
- ☐ Branscher: Är tjänsten som ert företag erbjuder kopplad till några specifika öppettider? Exempelvis sjukvårdsinrättningar
- ☐ Utomstående leverantörer: Ger ni åtkomst till företaget åt entreprenörer eller utomstående leverantörer?
- ☐ Enhet: Förväntar ni er att anställda kommer att hämta jobbinformation på sina egna enheter?

PROVA ATT MIKROSEGMENTERA

En mikrosegmentering ger er bättre förståelse för vilka tillgångar och användare ni har. Nedan ges en enkel tabellmall som kan användas för denna analys – åtminstone den första delen, som handlar om identitet.

Nollförtroendesegment

Molnbaserad CRM

Användargrupp	Scenario	Nätverksplats	Geografisk plats	Tidsbegränsningar	Risk med enheten	Risk med datorn	Autentisering
Säljare	Arbete på kontoret	Kontorets nätverk			Låg risk	Bärbar dator från företaget	Lösenord
Teknisk support för finansavdelningen	Tjänsteresor	Vilken som helst			Låg risk	Bärbar dator från företaget	Push-meddelande för MFA QR-kod för MFA
Utomstående grupp	Arbetar endast på kontoret	Kontorets nätverk		Kontorstider	Låg risk	Företagsdator	Lösenord
	Arbetar via VPN	Företagets VPN		Kontorstider	Låg risk	Företagsdator	Push-meddelande för MFA
IT – CRM	CRM-konsulter	Vilken som helst	Endast USA	Kontorstider			Push-meddelande för MFA
	CRM-stöd	Vilken som helst	Endast USA		Låg risk		Push-meddelande för MFA

Mikrosegment Exempel

Använd denna mall som utgångspunkt för att skapa era egna mikrosegment och utöka tabellen beroende på era egna säkerhetsbehov för att skapa mer specifika åtkomstpolicyer.

Guide för riskbedömning av verksamheten forts.

GUIDE FÖR RISKBEDÖMNING	Riskfaktor		MFA	Riskegenskaper		
	Användarnamn	Lösenord	engångslösen, QR, push	Nätverksplats	Autentiseringsresultat	Risknivå
SCENARIO 1 Företagets medarbetare ansluter till företagsresurs hemifrån	✓	✓	✓	✗	Tillåt	Godkänn
SCENARIO 2 Företagets medarbetare ansluter från Seattle, kontoret i WA till en företagsresurs	✓	✓	MFA krävs inte	✓	Tillåt	Godkänn
SCENARIO 3 Användaren försöker logga in för åtkomst till företagsdata från okänd plats	✓	✓	✗ MFA ej tillåtet	✗	Avvisa	Avvisa

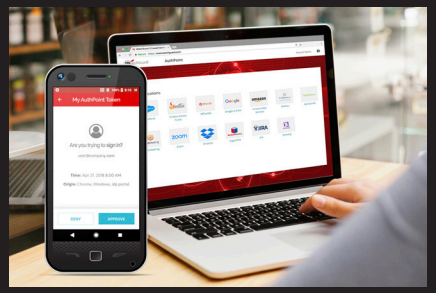
WATCHGUARD UNIFIED SECURITY PLATFORM™

Nätverkssäkerhet

WatchGuards lösningar för nätverkssäkerhet är helt igenom utformade för att vara enkla att distribuera, använda och hantera – förutom att de också ger största möjliga säkerhet. Våra unika lösningar för nätverkssäkerhet fokuserar på att ge förstklassig säkerhet i storföretagsklass till alla organisationer, oavsett deras storlek och tekniska kunnande.

Säkert trådlöst nätverk

WatchGuards lösning för säkring av det trådlösa nätverket innebär en revolution på dagens marknad. Den är konstruerad för att skapa ett säkert, skyddat luftrum för miljöer med trådlösa nätverk, samtidigt som administrativa problem elimineras och kostnaderna sänks avsevärt. Med expansiva engagemangsverktyg och insyn för affärsanalys skapar den sådana konkurrensfördelar som företag behöver för att lyckas.



Multifaktorautentisering

WatchGuard AuthPoint® är rätt lösning för att åtgärda de säkerhetsproblem som uppstår när man behöver använda multifaktorautentisering på en lättanvänd molnplattform. WatchGuards unika metod inkluderar ”mobiltelefonens DNA” som en identifierande faktor för att säkerställa att endast rätt person beviljas åtkomst till känsliga nätverk och molnprogram.

Slutpunktssäkerhet

WatchGuard Endpoint Security är en avancerad molnbaserad portfölj av säkerhetsfunktioner för slutpunkter som skyddar företag av alla typer från dagens och framtida IT-attacker. Dess paradlösning är Panda Adaptive Defense 360, som med hjälp av artificiell intelligens omedelbart stärker en organisations säkerhet. Den kombinerar funktioner för slutpunktsskydd (EPP/endpoint protection) och detektering och reaktion (EDR/endpoint detection and response) med program för nollförtroende- och tjänster för hotjakt.

Om AuthPoint

AuthPoint multifaktorautentisering (MFA) ger säkerheten ni behöver för att skydda användarnas inloggningsuppgifter, tillgångar, konton och information. Hantera AuthPoint var som helst, när som helst via lättanvänd molnbaserad hanteringsplattform som erbjuder ett gränssnitt för riskbaserad policyhantering, utformat för att ge bästa möjliga efterlevnad av principerna om nollförtroende.
Låt ert företag fungera tryggt och bekymmersfritt med kraftfullt skydd från AuthPoint MFA. Läs mer

Om WatchGuard

WatchGuard® Technologies, Inc. är® en global ledare inom nätverkssäkerhet, slutpunktssäkerhet, säkra trådlösa nätverk, multifaktorautentisering och nätverksintelligens. Över 18 000 säkerhetsåterförsäljare och tjänsteleverantörer litar på företagets prisbelönta produkter för skyddet av fler än 250 000 kunder. WatchGuards uppdrag är att göra säkerhet i storföretagsklassen tillgänglig för företag av alla typer och storlekar genom enkelhet, vilket gör WatchGuard till den idealiska lösningen för medelstora företag och geografiskt spridda företag. Företaget har huvudkontoret i Seattle, Washington, med kontor i hela Nordamerika, Europa, Asien, stillahavsområdet och Latinamerika.

Läs mer genom att besöka WatchGuard.com.

FÖRSÄLJNING NORDAMERIKA +1-800-7349905 INTERNATIONELL FÖRSÄLJNING +1-206-6130895 WEBB www.watchguard.com