Next Level Access Management & Security

topicus KEYHUB

TIJD VOOR ECHTE **VERANDERING** OP HET GEBIED VAN **BEVEILIGING**

CREËER EEN NIEUWE MINDSET

Je wilt het meeste uit je organisatie halen en digitale middelen zijn hierin cruciaal. Of ze nu comfortabel in de cloud staan of in je eigen serverpark. Om efficiënt te blijven werken, is het van belang dat collega's eenvoudig bij deze applicaties, diensten en servers kunnen. Dit creëert een groeiende uitdaging: hoe zorg je ervoor dat iedereen exact de juiste toegang heeft zonder omvangrijke beheerslast en drempels op te werpen?

Iedere organisatie, van MKB tot grote multinational, worstelt met dit probleem: het woud van gebruikte accounts, applicaties, servers en wachtwoorden wordt steeds groter. Dit vormt een groeiende uitdaging. Het borgen van digitale toegang is minstens zo belangrijk als het fysiek beveiligen van een organisatie. Gegevens van klanten en gebruikers zijn veel waard en een datalek kan catastrofale gevolgen hebben. Niet voor niets beseffen steeds meer organisaties dat ze een goede oplossing nodig hebben voor toegangsmanagement.

Cruciaal in een goede oplossing is de adoptie van collega's. Naast uiteraard de hoogst mogelijke veiligheid is eenvoud in gebruik en beheer en het voorkomen van onnodige drempels voor gebruikers van belang. Geen extra hordes, maar een echte oplossing die bewustzijn verhoogt en risico's verkleint.

"Geen extra hordes, maar een echte oplossing die bewustzijn verhoogt en risico's verkleint."

Flexibiliteit zonder drempels

Om digitale veiligheid te borgen is het noodzakelijk om drempels te verlagen. Iedere drempel brengt namelijk een reden om deze te omzeilen. Aan de andere kant mag waardevolle informatie niet zomaar voor iedereen toegankelijk zijn. Idealiter worden exact de juiste drempels gelegd per informatiebron. Flexibiliteit hierin is cruciaal. Zo creëer je gebruiksgemak, bewustzijn en een veiligere organisatie.

Eenvoud in gebruik en beheer

Een systeem dat complex is in gebruik of beheer, frustreert medewerkers en voorkomt adoptie. Dit leidt tot risico's en een gebrek aan overzicht en controle. Er vallen accounts, medewerkers of systemen buiten de boot die gemakkelijk misbruikt kunnen worden. Ook gedeelde accounts, standaardwachtwoorden en privileged accounts zijn grote risico's. Het goed managen hiervan kan alleen met een systeem dat voor eenvoudige toegang, gebruik en integraties zorgt.

"Ook gedeelde accounts, standaardwachtwoorden en privileged accounts zijn grote risico's"

Topicus KeyHub

Met Topicus KeyHub wordt access management binnen uw organisatie eenvoudiger en veiliger met meer bewustzijn bij collega's en minder beheerslast voor systeembeheerder(s). Iedere organisatie die met gedeelde accounts, zelfstandige teams of externe (klant)systemen werkt, wordt productiever en veiliger dankzij de revolutionaire aanpak van Topicus KeyHub: centrale authenticatie en decentrale autorisatie.

Centrale authenticatie

Op één centrale plek wordt gecontroleerd wie de gebruiker is. Oftewel: is de fysieke persoon eigenaar van het account waarmee hij wil inloggen. Door de koppeling aan de Active-Directory of HR-systeem borgt deze centrale authenticatie dat alleen bekende personen gebruik mogen maken van uw systemen en diensten. Onafhankelijk van waar medewerker- of klantgegevens opgeslagen zijn, Topicus KeyHub zorgt ervoor dat de authenticatie eenduidig en centraal beheerd wordt.

Decentrale autorisatie

Authenticatie bepaalt alleen wie de gebruiker is. Wat die persoon vervolgens mag, wordt bepaald door zijn autorisatie. Een organisatie bestaat uit meerdere subgroepen zoals afdelingen, projecten, teams of klantgroepen. Het is niet wenselijk dat iedereen bij alle gegevens van de hele organisatie kan. Iedere medewerker heeft zijn eigen combinatie van applicaties, accounts, servers of toegang nodig om efficiënt te kunnen werken. Met Topicus KeyHub wordt het mogelijk om al die verschillende groepen autorisaties eenvoudig in te richten en te managen. Geen overhead meer van een centrale afdeling, maar de verschillende groepen zijn zelf in control.

Next Level Administrator

De tijd dat een centrale administratie noodzakelijk is voor goed access management is voorbij. Het kan wel, maar het hoeft niet meer. Een administrator kan zich zodoende weer focussen op het beheren van de infrastructuur en applicaties.

Security made easy

Met Topicus KeyHub wordt het veiliger maken van de organisatie erg eenvoudig. Binnen een halve dag is Topicus KeyHub geïnstalleerd en kunt u aan de slag. Afhankelijk van de behoeftes kunnen de verschillende systemen, applicaties en teams aangesloten worden. Hierbij ben je niet veroordeeld tot een ‘big bang’ overstap, maar bepaal je je eigen tempo. Geen gehaast of complexe trainingen van alle medewerkers, maar wel direct resultaat en een veiligere organisatie. Topicus KeyHub maakt het mogelijk!

“Met Topicus KeyHub wordt access management binnen een organisatie eenvoudiger en veiliger met meer bewustzijn bij collega’s en minder beheerslast voor systeembeheerder(s).”

ENKELE VOORDELEN VAN TOPICUS KEYHUB

01 BETERE BEVEILIGING

Centrale authenticatie met 2FA
Authenticatie in Topicus KeyHub is gekoppeld aan de ActiveDirectory of het HR-systeem. Alleen actieve medewerkers kunnen inloggen, waarbij ze gebruik maken van 2-factor authenticatie. Hierbij kan zowel de Topicus KeyHub-app gebruikt worden of een alternatieve 2FA-oplossing.

Real-time provisioning
Systemen die op basis van een LDAP of Active-Directory werken worden real-time en time-based provisioned. Er zijn dus geen accounts aanwezig tenzij expliciet aangezet voor een specifieke periode. Dit biedt bescherming tegen onder andere brute-force attacks: hackers kunnen geen toegang meer krijgen, want de accounts zijn niet aanwezig.

Geen super-administrators meer
Applicatiebeheerders van Topicus KeyHub zijn ook echte applicatiebeheerders. Ze kunnen zichzelf nooit méér rechten toe-eigenen dan ze op dat moment hebben. Voor het toekennen van rechten of het doorvoeren van wijzigingen wordt het 4-ogen-principe toegepast. Hiermee wordt fraude en het risico van grote security-breaches tegengegaan.

Single Sign-On (SSO) met user-consent
Realiseer single sign-on via onder andere SAML2 en OAuth2 (OIDC). Met Topicus KeyHub wordt het mogelijk om deze toegang te beheren per groep: zit een medewerker in een specifieke groep, dan is er SSO-toegang. Verlaat de medewerker de groep, verliest hij direct toegang. Uiteraard voorzien van user consent voor maximale transparantie naar de gebruikers.

02 MEER INZICHT EN CONTROLE

Decentrale autorisatie
Groepen en teams bepalen zelf wie er bij een groep mag en wie niet. De groepsmanagers zien altijd wie er in hun groepen zitten en kunnen groepsleden eenvoudig verwijderen indien nodig. Omdat een groep specifiek toegang geeft tot een set van applicaties, servers, wachtwoorden of systemen, wordt het beheer van de toegang decentraal belegd. Groepsmanagers zijn functioneel of technische verantwoordelijk voor hun eigen groep(en).

Access control en password management
Iedere groep beschikt over een eigen wachtwoordkluis. Fileshares of Excel-sheets met wachtwoorden zijn hierdoor verleden tijd. Via de wachtwoordkluis kunnen sterke wachtwoorden gebruikt en aangepast worden. Het juiste wachtwoord staat immers altijd in de kluis en wordt simpel uitgelezen via de browser-extensie.

Audit trail en access governance
Op een leesbare manier terugzien welke medewerker toegang heeft gehad tot welke servers, applicaties en diensten. Transparantie zorgt voor bewustzijn en met Topicus KeyHub zie je alle informatie die voor jou van belang is, zelfs óf en wannéér een medewerker een wachtwoord of 2FA-code uit een kluis heeft gelezen. Een grote stap voor compliance, ISO 27001 en de AVG.

03
FLEXIBILITEIT EN CONNECTIVITEIT

Externe integraties
Op iedere logregel kan een actie worden geplaatst worden om externe systemen realtime op de hoogte te brengen. Stream alle logs naar een SIEM of stel een custom dashboard of Slack-kanaal op de hoogte van specifieke events of toegang tot bijvoorbeeld een productie-database.

Command-line interface
Creëer machine-to-machine integraties via de command-line interface. Geheel geautomatiseerd wachtwoorden uitlezen en wegschrijven, zodat geen enkel script-bestand nog een wachtwoord hoeft te bevatten.

Ex-medewerkers toegang ontzeggen
Met één druk op de knop kunnen medewerkers uitgesloten worden van toegang. Handig als een medewerker naar een ander team gaat of als deze de organisatie geheel verlaat. Zo kan worden voorkomen dat een ex-medewerker nog over gedeelde accounts en wachtwoorden beschikt.

“Iedere medewerker heeft zijn eigen combinatie van applicaties, accounts, servers of toegang nodig om efficiënt te kunnen werken.”

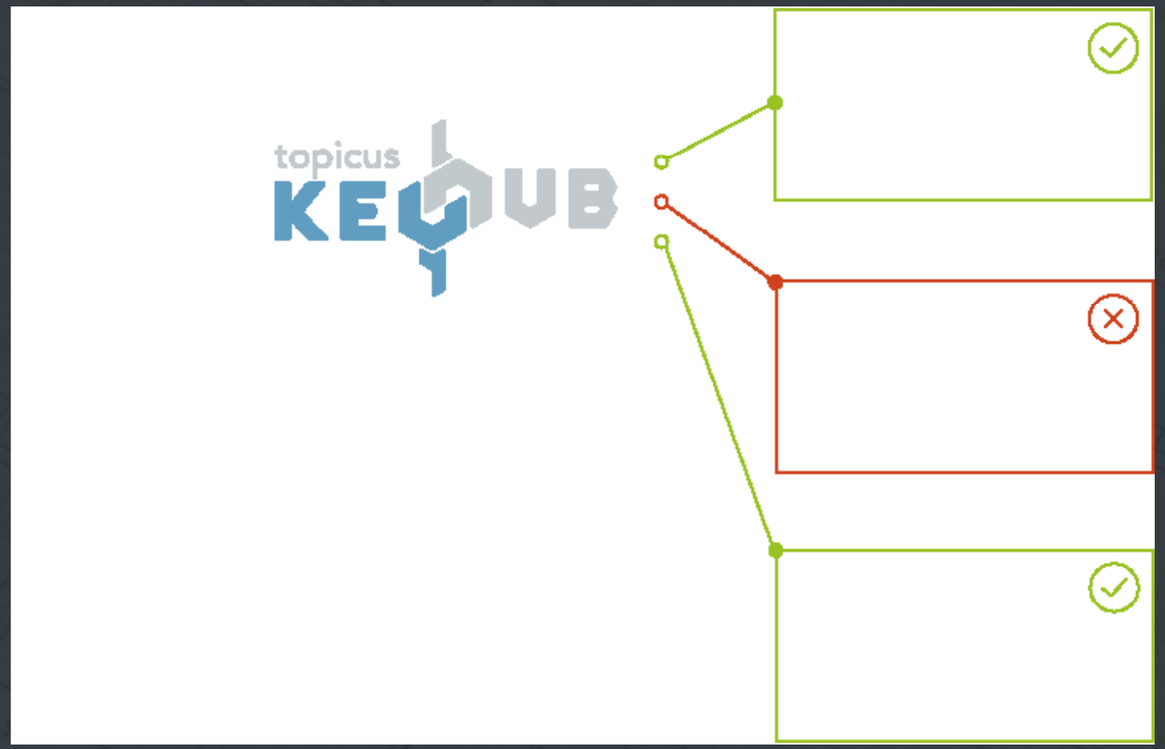
HOE WERKT TOPICUS KEYHUB?

Topicus KeyHub is de poortwachter die de toegang tot het server- en applicatielandschap regelt. Dit gebeurt op basis van centrale authenticatie en decentrale autorisatie zoals weergegeven in de afbeelding.

Iedereen die toegang nodig heeft tot de organisatie dient zich op dezelfde plek te authenticeren. Na authenticatie is bekend wie de gebruiker is, maar mag deze nog niets. Daar komt de echte revolutie om de hoek.

“Iedere medewerker heeft een eigen, unieke combinatie van toegangsrechten”

Met Topicus KeyHub worden alle verschillende onderdelen van de organisatie verdeeld in ‘groepen’. Iedere groep geeft toegang tot een willekeurige set van servers, applicaties en gedeelde wachtwoorden. Een groep wordt beheerd door groepsmanagers die verantwoordelijk zijn voor wie er toegang heeft tot de groep.



Afhankelijk van de organisatie kunnen verschillende onderdelen decentraal worden beheerd. Er is geen centrale admin meer nodig om dit in goede banen te leiden.

Voor toegang wordt onderscheid gemaakt in drie niveaus van beveiliging. Het hoogste niveau is single sign-on. Indien dat niet mogelijk is, kan een LDAP of ActiveDirectory realtime geprovisioned worden. Accounts zijn dan alleen (tijdelijk) beschikbaar als een groep in Topicus Keyhub wordt geactiveerd. Het derde niveau van toegang zijn de gedeelde accounts. Hiervoor wordt een gedeeld wachtwoord uit een kluis opgehaald. Deze actie wordt door Topicus Keyhub vastgelegd, waardoor er te allen tijde is na te gaan wie deze actie heeft uitgevoerd.

Topicus KeyHub is eenvoudig te implementeren binnen de bestaande IT-architectuur van de organisatie en kan naast huidige oplossingen draaien. Binnen een dag zijn de voordelen al merkbaar.

TOPICUS KEYHUB IN ÉÉN OVERZICHT

Authenticatie

Centrale authenticatie

Integratie met meerdere LDAPs of ActiveDirectories

2-factor authenticatie

Autorisatie

Geen super-admins of god-modes

4-ogen principe

Time-based activatie van LDAP/AD-systemen

Real-time provisioning van LDAP/AD-systemen

Custom groepen met applicaties, servers en/of wachtwoorden

Verantwoordelijkheid per groep decentraal belegd

Single sign-on met SAML2/OAuth2

Wachtwoordbeheer

Wachtwoordkluizen per groep

2FA op gedeelde accounts

Persoonlijke wachtwoordkluis

Browser-plugin voor wachtwoorden

Awareness

Leesbare audit trail

Iedere actie van eigen groepen inzichtelijk

Transparantie van alle events

Connectiviteit

Webhooks op audit records

Command-line interface

Installatie in een halve dag

Eenvoudige en intuïtive user interface

TOPICUS KEYHUB

Vermindert beheerskosten

Versnelt productiviteit nieuwe medewerkers

Verkleint risico's van ex-medewerkers

Vereenvoudigt ISO27001, ISAE-3402 en SOC-II

Verhoogt direct bewustzijn van alle medewerkers

Vergroot veiligheid

MEER INFORMATIE?

Bezoek onze website op www.topicus-keyhub.com, mail naar keyhub@topicus.nl of bel: +31 (0)85 065 3011. Wij komen graag langs om meer te vertellen en om de mogelijkheden van Topicus KeyHub voor jouw organisatie te verkennen.

Powered by topicus