



Open Universiteit

Just-in-time beheerrechten

Martin Romijn - CISO

Vrijdag 28 juni 2024, 11:15–11:45, Sessiezaal 3





JUST-IN-TIME BEHEERRECHTEN

- 1. Introductie
- 2. De besluitvorming
- 3. De uitrol (Proof of Concept en Productie)
- 4. Het gebruik



1. INTRODUCTIE

- *Just-in-Time* (JIT) toegang is een beveiligingsproces waarbij gebruikers, applicaties of systemen rechten toegekend krijgen voor een beperkte periode of om een taak uit te voeren.
- *Just-in-Time* toegang wordt gezien als een vorm van *Privileged Access Management*.
JIT toegang wordt aangeraden als een wijze om provisioning te verzorgen door permanente *privileged access* tot een minimum te beperken. Ook wordt er gedacht vanuit het *zero trust* model waarbij niets wordt vertrouwd en alles wordt gecontroleerd voordat toegangsrechten worden toegekend.





2. DE BESLUITVORMING

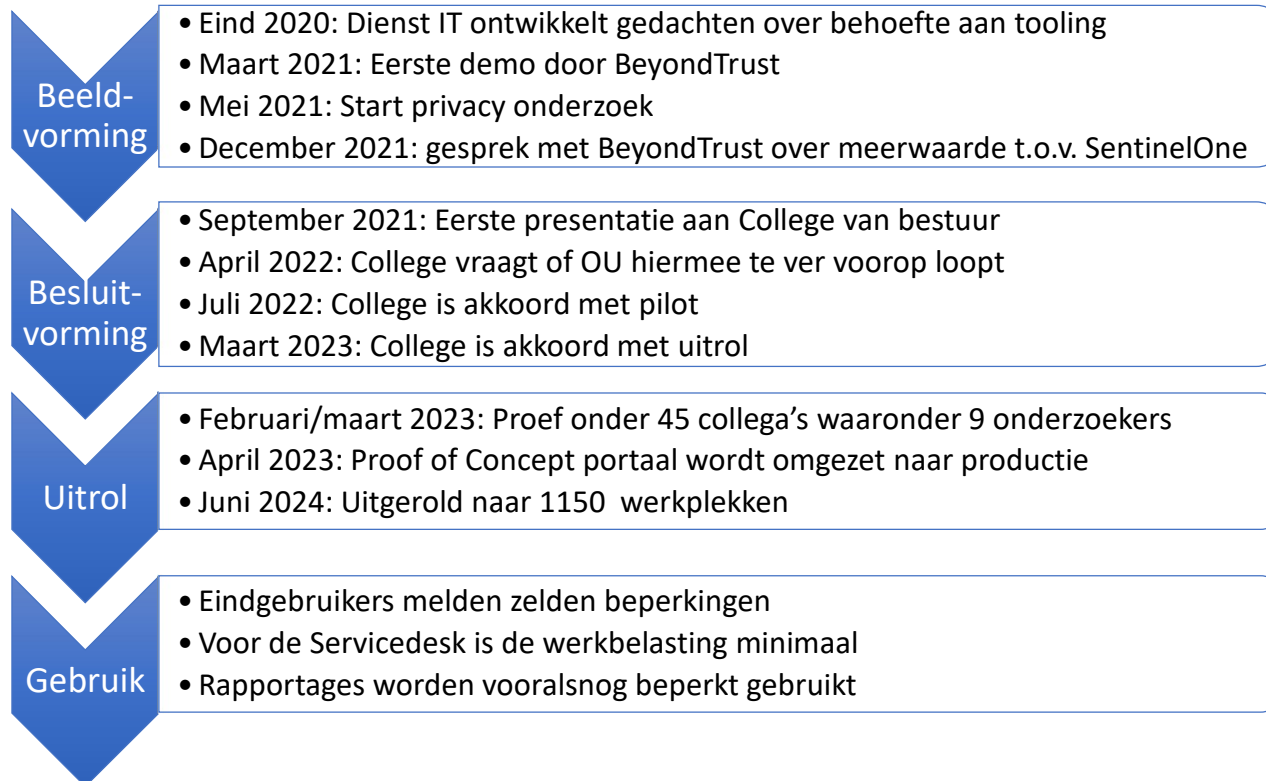


Figure 1: Magic Quadrant for Privileged Access Management

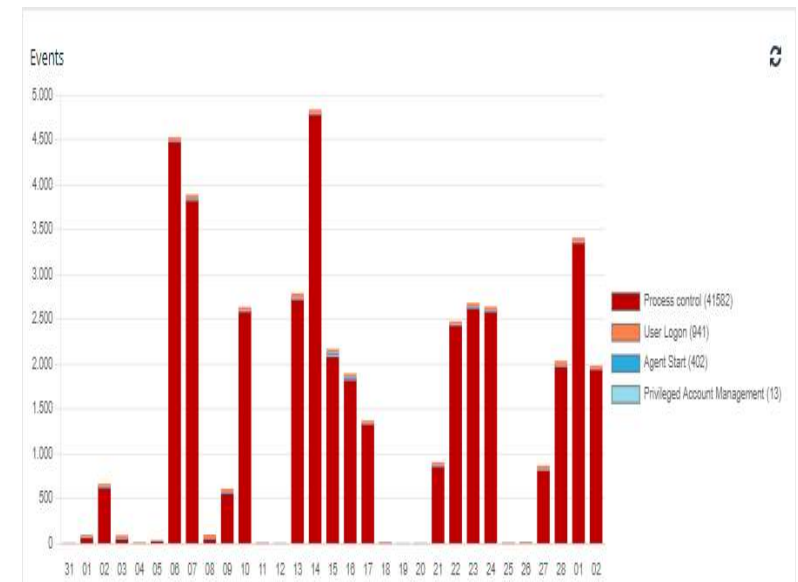


Source: Gartner (July 2022)



3. DE UITROL – PROOF OF CONCEPT

- Van de 43 proefpersonen meldden er 10 dat zij iets van BeyondTrust gemerkt hadden.
- Bij twee medewerkers hielp de Servicdesk met een reguliere oplossing.
- Eén medewerker werd geholpen met een work around.
- Enkele browserproblemen werden vrijwel zeker door geïnstalleerde plug-ins veroorzaakt.
- Enkele problemen met Teams traden ook bij anderen op, na een Teams update.





3. DE UITROL – PRODUCTIE

De uitrol startte op 4 september 2023.

Set-up: *Quick-start High flexibility policy*:

- OU applicaties: geen pop-up
- Goedgekeurde applicaties: alleen Ja/nee
- Onbekende applicaties: reden op te geven
- Malafide geacht: niet mogelijk.

Uitrol naar Apple Mac (omstreeks 35) staat in de startblokken. Linux werkplekken (5x) komen na afronding van de uitrol naar Mac's.

Privilege Management Console | Policies

524 Items

Name	Locked By	Created	Groups Assigned	Size
DMC-Win-GS	--	14/09/2023 11:48	1	487,29 KB
01 - Soop - Windows-GS	gkumar@beyondtrust.com	04/10/2023 13:07	1	536,82 KB
Excluded	pbello@beyondtrust.com	27/10/2023 13:54	--	487,59 KB
03 - Soop-MAC-GS	gkumar@beyondtrust.com	10/10/2023 06:48	1	161,98 KB
03 - Soop-Server-GS	bchomiak@beyondtrust.com	25/04/2023 13:47	1	784,16 KB
DMC2-the-audit-one	dclifford@beyondtrust.com	13/11/2023 11:23	--	487,60 KB



4. HET GEBRUIK

Door ontbreken van een tool zoals Intune moest de Servicedesk soms contact opnemen met gebruikers om de installatie afgerond te krijgen.

Concrete ervaringen van de afgelopen 90 dagen:

- Voor 77 applicaties moest een 'Ja' gegeven worden.
- Zes gebruikers werd om een reden gevraagd.
- Bij installatie van de Exact client loopt installatie van het .NET framework niet vanzelf door.

Noot: BeyondTrust bewaakt tools. Het bewaakt uitzetten van firewall of virusscanners door eindgebruikers niet.

77 items						
Application Description	Application Name	Versions	Required	Processes	Users	
▼ DiskImager	Win32 Image Writer	1 version	Yes	20	1	
▼ NVIDIA Package Launcher	NVIDIA Package Launcher	2 versions	Yes	11	2	
▼ SynergyUpdater	Exact Holding B.V. SynergyUpdater	1 version	Yes	6	2	
▼ Microsoft .NET Framework 3.5 Setup	Microsoft .NET Framework 3.5	1 version	Yes	6	4	
▼ Setup Installer	Microsoft® .NET Framework	2 versions	Yes	5	3	
ensutils.exe	--	--	Yes	5	1	
▲ .NET Framework 3.5 Setup	.NET Framework 3.5	2 versions	Yes	4	2	
.NET Framework 3.5 Setup	.NET Framework 3.5	3.5.30729.01	Yes	3	1	
.NET Framework 3.5 Setup	.NET Framework 3.5	3.5.21022.08	Yes	1	1	
ImageCapture 8.16	ImageCapture 8.16	--	Yes	2	2	
▼ InstallShield (R) Setup Engine	InstallShield (R)	1 version	Yes	3	3	

Voor meer informatie:
martin.romijn@ou.nl



BEDANKT

Bijlagen

Just in time beheerrechten



INSPIREER

Figure 1: Magic Quadrant for Privileged Access Management

GARTNER MAGIC QUADRANT

@Gartner
Januari 2022



Source: Gartner (July 2022)



POP-UPS BIJ INSTALLATIE DOOR GEBRUIKER

