

Microsoft Inspiratie en Innovatie Event K-12 (PO en VO)

Security & Zero Trust

Maurits Knoppert – APS IT-Diensten
Martijn Frank – SLBdiensten



SLBDIENSTEN.NL

APS IT diensten

Voor ICT in het belang van je school

From Wikipedia, the free encyclopedia

For the musician, see *Hint (musician)*.

Jonathan Joseph James (December 12, 1983 – May 18, 2008) was an American **hacker** (a **gray hat ethical hacker**) who was the first juvenile incarcerated for **cybercrime** in the United States.^[1] The **South Florida** native was 15 years old at the time of the first offense

'Leider hackersgroep Lapsus\$ is 16-jarige Brit'
De leider van hackersgroep Lapsus\$, die afgelopen weken onder meer binnendrong bij Nvidia, Samsung en Microsoft, zou een 16-jarige inwoner van Groot-Britannië zijn. Ook een tiener uit Brazilië zou bij de hackersgroep betrokken zijn.

Hacker Erik gaf de hele school vrij en moest voor straf op stage

Remco Andringa
redacteur Politie en Justitie

De hackers die voor het eerst door de politie zijn betrapt, worden op stage geplaatst in plaats van in de gevangenis. Dit is de eerste keer dat de strafmaat is veranderd. De hackers worden nu op stage geplaatst bij IT-bedrijven. Met deze alternatieve straf is het afgelopen jaar al meerdere keren gebruikt. De politie en het Openbaar Ministerie zijn tevreden over de eerste resultaten en gaan ermee door.

Vier jonge hackers hadden privégegevens van mogelijk Nederlanders in handen

MET VIDEO Vier hackers hebben hoogstwaarschijnlijk op enig moment de privégegevens van alle Nederlanders in handen gehad. Ze persten bedrijven ermee af en verkochten de gevoelige informatie door aan criminelen.

Per jaar worden zo'n 100 tot 200 jongeren tussen de 12 en 23 jaar aangehouden voor cybercrime. Vaak overzien zij de gevolgen van hun daden niet; soms beseffen ze niet eens dat ze een strafbaar feit hebben gepleegd. Het gaat bijvoorbeeld om jongeren die onbedoeld ver doordringen in een systeem, alleen maar om te zien of het kan. Dat een bedrijf vervolgens veel geld moet uitgeven, alleen al om bijvoorbeeld alle klanten in te lichten dat er een hack is geweest, realiseren ze zich niet.

Elk jaar worden zo'n zeventig jongeren aangehouden voor cybercrime. Langzaam maar zeker worden ze door hoeveel schade ze aanrichten. Daarom bedachten de politie en het Openbaar Ministerie een nieuwe straf, bedoeld voor hackers tussen de 12 en 23 jaar die onbedoeld de fout zijn gegaan.

De jongeren krijgen les over wat op internet wel en niet mag en gaan in de leer bij beveiligingsexperts van IT-bedrijven. Zo leren ze hoe ze hun talent op een goede manier kunnen benutten.

Elf jongeren kregen dit jaar de alternatieve straf *Hack_Right* aangeboden. Een van hen was 'Erik', die om privacy-redenen niet met zijn echte naam wil worden genoemd. Hij was 17 toen hij zijn school hackte. "Nog voor de eerste schooldag begon, had ik de wachtwoorden van alle docenten al."

Jongeren vaker betrokken bij fraude en cybercrime, politie maakt zich zorgen

Joost Schellevis
redacteur Tech

David van Hulzen
redacteur NOS Stories

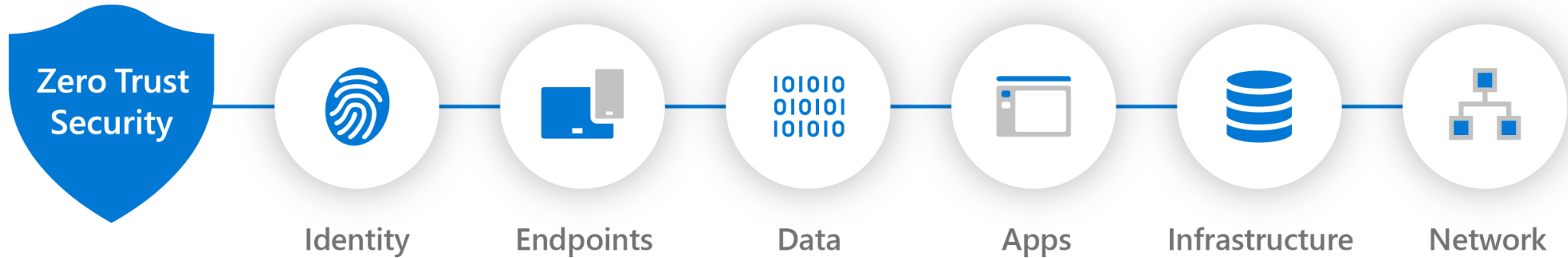
Jongeren zijn de afgelopen jaren bij steeds meer cybercrime-zaken betrokken. Vorig jaar was in 47 procent van de zaken iemand van 21 jaar of jonger betrokken, waar dat in 2018 nog in 33 procent van de cybercrime-zaken het geval was. Dat blijkt uit cijfers die het Openbaar Ministerie op verzoek van de NOS heeft verzameld.

OM eist vijf jaar cel tegen jonge Drent vanwege grootschalige cybercrime en oplichtingspraktijken

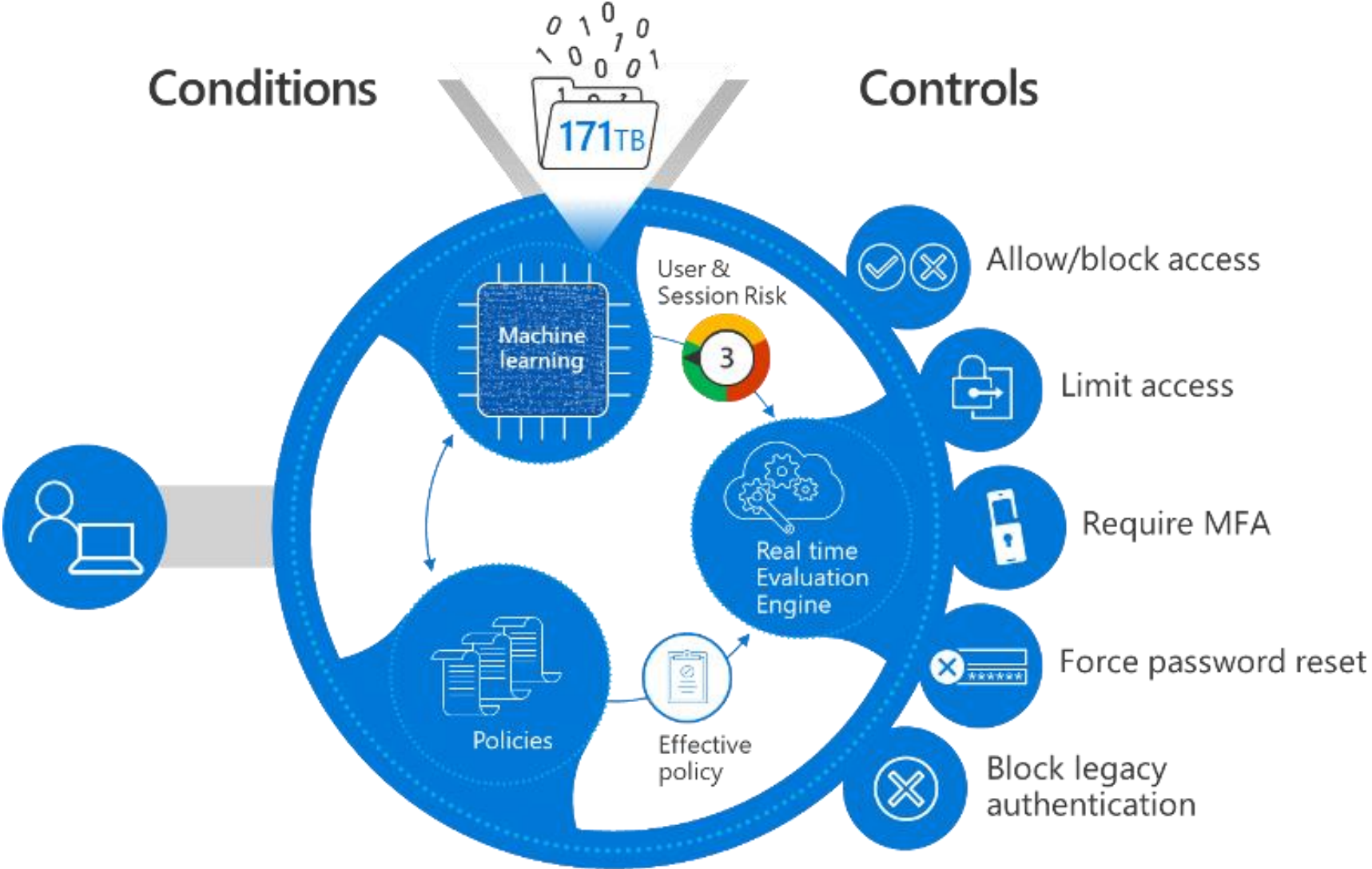
Nieuwsbericht | 10-11-2022 | 18:06

Zero trust

De moderne werkplek heeft een beveiligingsmodel nodig dat zich effectiever aanpast aan de complexe moderne omgeving, de hybride werkplek omarmt, en mensen, apparaten en gegevens beschermt, op elke locatie.

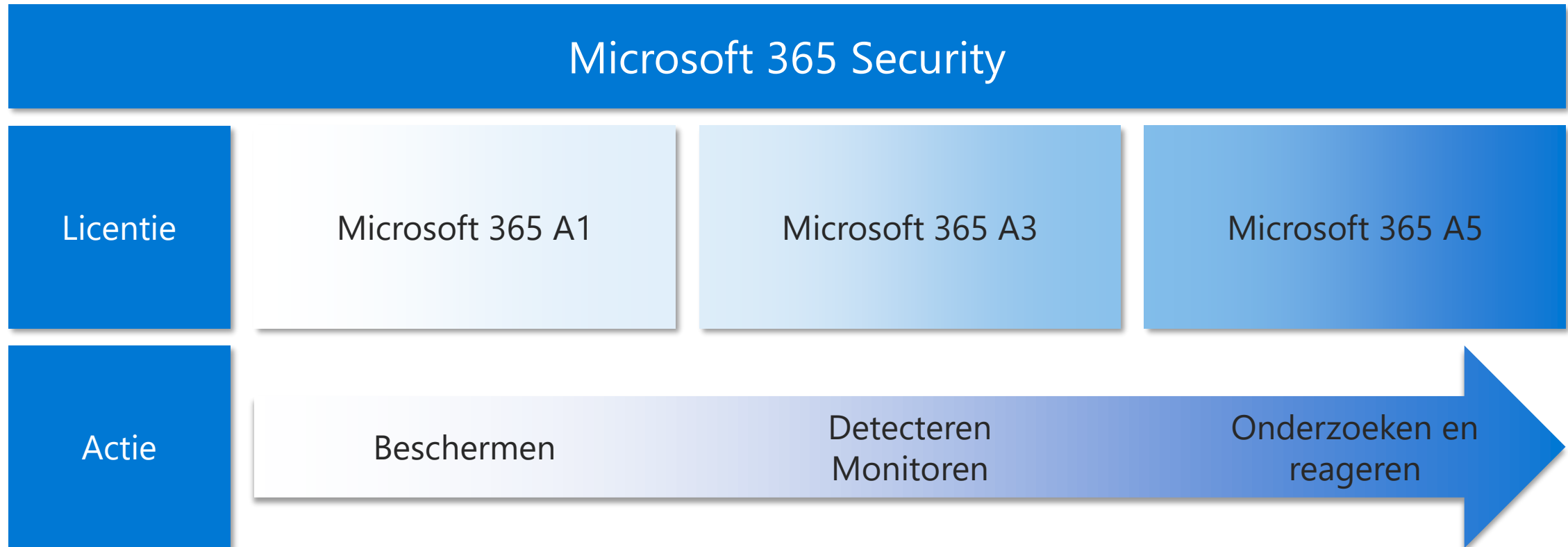


Zero trust



Microsoft A3 – A5 licenties

De verschillen



Microsoft A3 – A5 licenties

De verschillen

A3 licenties

- Azure Active Directory
- Microsoft Defender P1
- Enterprise Mobility Suite
- Azure Information Protection

Do not expire passwords

✔ Completed

 Edit status & action plan  Manage tags

General Implementation

Description

Research has found that when periodic password resets are enforced, passwords become less secure. Users tend to pick a weaker password and vary it slightly for each reset. If a user creates a strong password (long, complex and without any pragmatic words present) it should remain just as strong in the future as it is today. It is Microsoft's official security position to not expire passwords periodically without a specific reason, and recommends that cloud-only tenants set the password policy to never expire.

Implementation status

Your current policy is set to never let passwords expire.

User impact

Your users will no longer need to periodically create new passwords.

Users affected

All of your Microsoft 365 users

Details

Points achieved

8/8

History

0 events

Category

Identity

Product

Azure Active Directory

Protects against

[Password Cracking](#), [Account Breach](#)

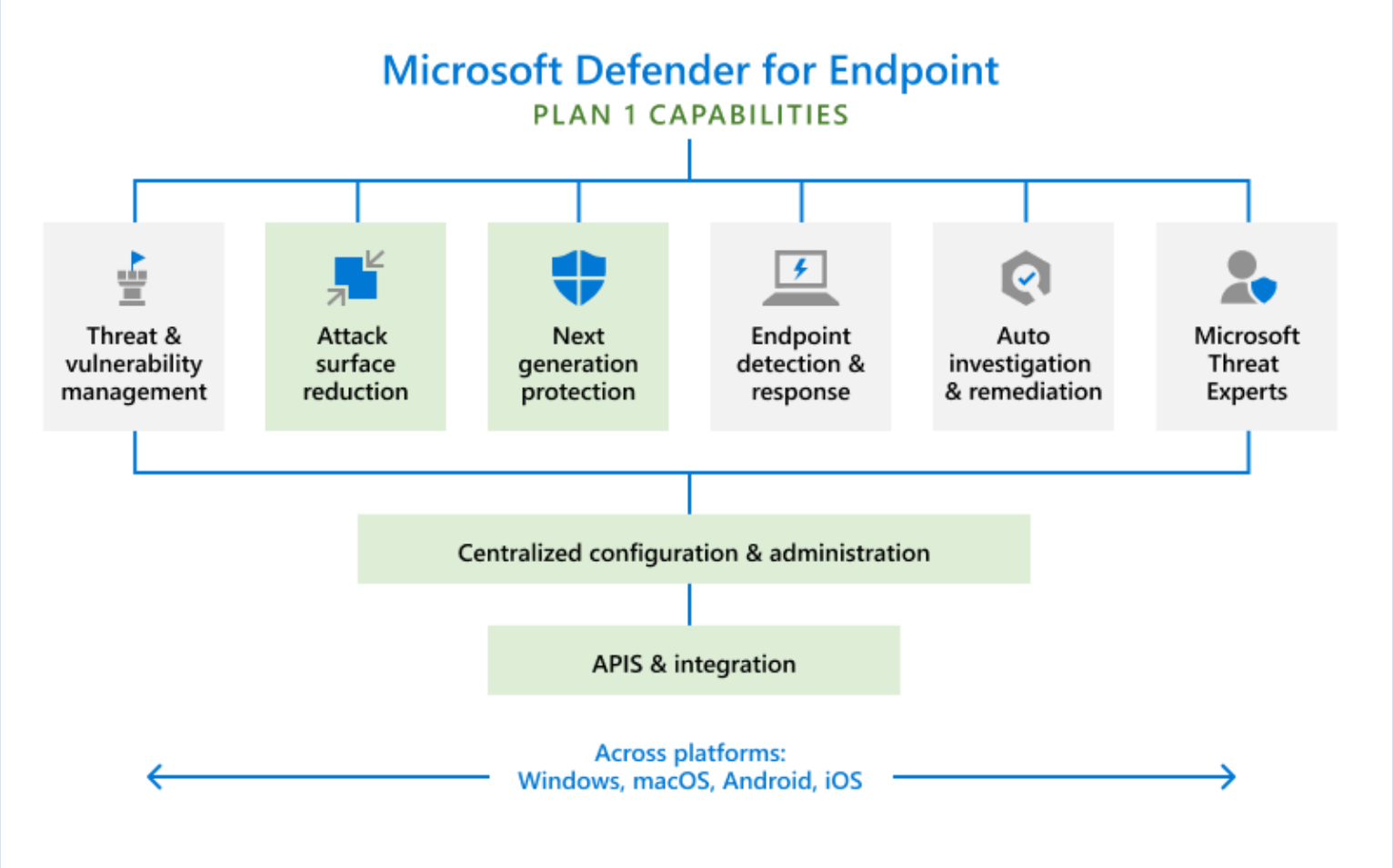
Azure Active Directory

Azure Active Directory	Premium 1	Premium 2
Identiteits- en toegangbeheer	V	V
Geavanceerde toegang	V	V
Voorwaardelijke toegang	V	V
Identiteitsbeveiliging		
Detectie van beveiligingsproblemen en riskante accounts		V
Onderzoek naar risicogebeurtenissen		V
Op risico's gebaseerd beleid voor voorwaardelijke toegang		V
Identiteitsbeheer		
Privileged Identity Management (PIM)		V

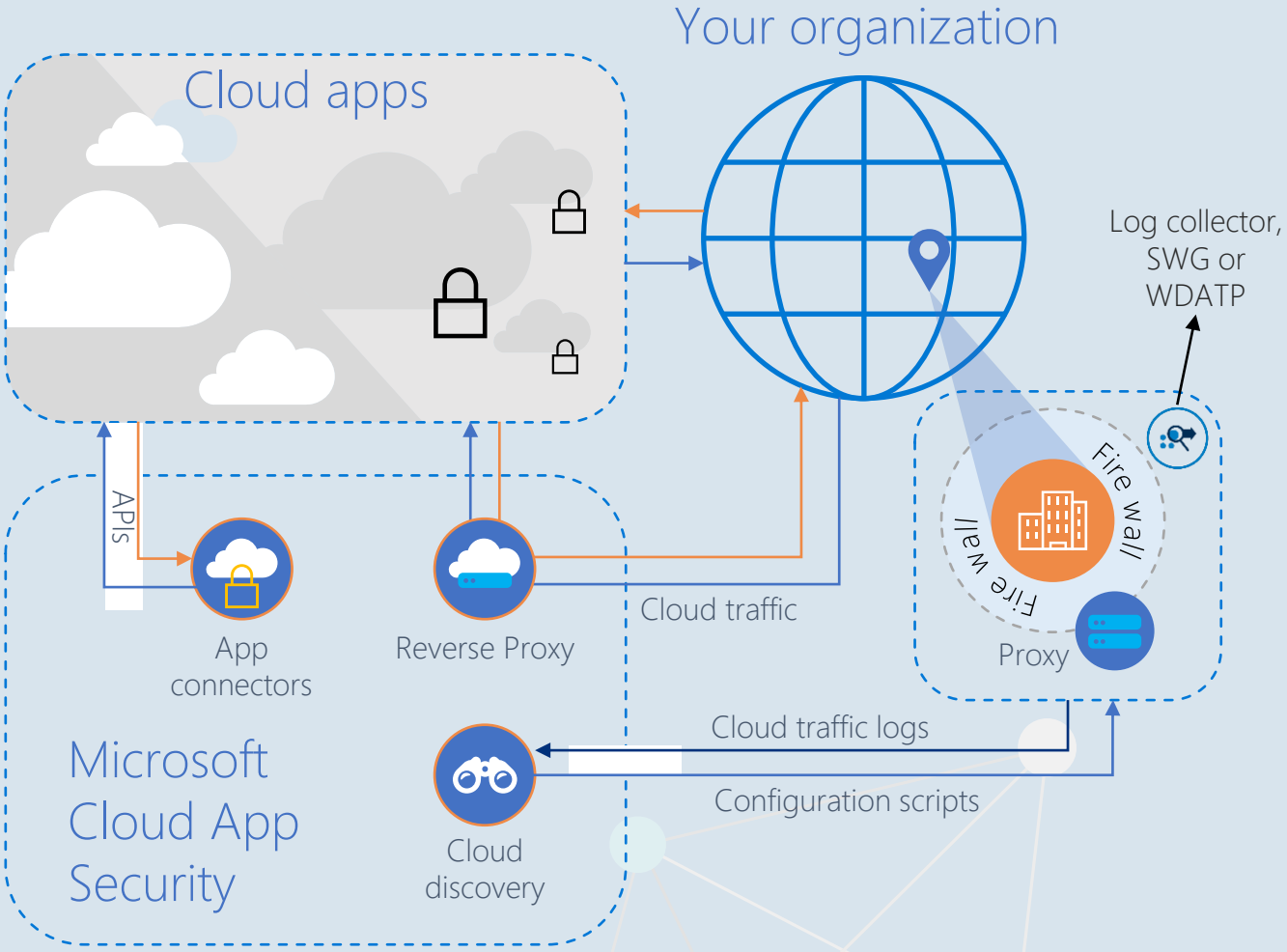
Defender for Office 365

Microsoft Defender voor Office 365	Plan 1	Plan 2
Veilige bijlagen	V	V
Veilige links	V	V
Veilige bijlagen voor SharePoint, OneDrive en Teams	V	V
Bescherming tegen phishing	V	V
Real-time detectie	V	V
Threat Trackers		V
Beveiligingsverkenner		V
Geautomatiseerd onderzoek en respons		V

Defender for EndPoint



Defender for Cloud Apps



Azure Information Protection

Microsoft Information Protection

Protect your sensitive data – wherever it lives or travels



Discover



Classify



Protect



Monitor

Across



Devices



Apps



Cloud services



On-premises

