Microsoft

Microsoft 365 Business Premium
Security & Services opportunity

Cloud Champion Update

22 maart 2023

Cloud Champion Update

Agenda vandaag:

22 maart 2023

1. Korte **review** Microsoft 365 Business Premium & **Defender for Business**
2. **Zero Trust Principles** als basis voor **Defender portfolio**
3. Nieuwe functionaliteit **Defender**
4. **Strategische keuzes voor MSP's**
5. Impact van de keuzes

Even voorstellen:

Chris de Bruin

c.debruin@flbs.nl

Vanaf 2005: Frontline Business School

FRONTLINE BUSINESS SCHOOL

Microsoft

Vanaf 2016: Partner Platforms

FRONTLINE BUSINESS

MORE.

Microsoft

Doe meer met Microsoft 365 Business Premium

Hoe was het ook alweer?

Microsoft 365 propositie voor small & medium business

Microsoft 365 Business Basic

Cloud Services

Teams Exchange OneDrive SharePoint

€ 5,10 per user/maand

Microsoft 365 Business Standard

Cloud Services

Teams Exchange OneDrive SharePoint

Desktop Apps

Outlook Word Excel PowerPoint Publisher Access

€ 10,50 per user/maand

Microsoft 365 Business Premium

Cloud Services

Teams Exchange OneDrive SharePoint

Desktop Apps

Outlook Word Excel PowerPoint Publisher Access

Comprehensive Security

Intune Azure Information protection Azure AD Premium Windows Virtual Desktop Microsoft Defender

€ 18,60 per user/maand

[1]price is subject to change based on subscription term, currency and region

Note: Not all features/product logos shown.

Microsoft 365 Business Premium: Defender for Business

Defender for Business/for Endpoint

Customer size	< 300 seats	> 300 seats	
Endpoint capabilities\SKU	**Microsoft Defender for Business***	**Microsoft Defender for Endpoint Plan 1**	**Microsoft Defender for Endpoint Plan 2**
Centralized management	✔	✔	✔
Simplified client configuration for Windows	✔		
Threat and Vulnerability Management	✔		✔
Attack Surface Reduction	✔	✔	✔
Next-Gen Protection	✔	✔	✔
Endpoint Detection and Response	✔[1]		✔
Automated Investigation and Response	✔[1]		✔
Threat Hunting and 6-months data retention			✔
Threat Analytics	✔[1]		✔
Cross platform support for Windows, MacOS, iOS, and Android	✔[3]	✔	✔
Microsoft Threat Experts			✔
Partner APIs	✔	✔	✔
Microsoft 365 Lighthouse for viewing security incidents across customers	✔[2]		

[1] Optimized for SMB. [2] Additional capabilities planned [3] iOS, and Android requires Microsoft Intune. Please see Documentation for more detail.
* Microsoft Defender for Business is generally available in Microsoft 365 Business Premium starting March 1. The standalone SKU will be generally available later this calendar year. Read the blog post to learn more.

Vergelijking Microsoft 365 BP, E3 en E5

		Microsoft 365 Business Premium	Microsoft 365 F1/F3/E3	Microsoft 365 E5
Identity and Access Management	**Simplified access management and security:** Centrally manage single sign-on across devices, your datacenter, and the cloud.	●	●	●
	Multi-factor authentication: Strengthen sign-in authentication with verification options, including phone calls, text messages, or mobile app notifications, and use security monitoring to identify inconsistencies	●	●	●
	Conditional access: Define policies that provide contextual controls at the user, location, device, and app levels to allow, block, or challenge user access.	●	●	●
	Risk-based conditional access: Protect apps and critical data in real time using machine learning and the Microsoft Intelligent Security Graph to block access when risk is detected.			●
	Advanced security reporting: Monitor suspicious activity with reporting, auditing, and alerts, and mitigate potential security issues using focused recommendations.		●	●
	Privileged identity management: Provide timely, on-demand administrative access to online services with access-related reporting and alerts.			●
	Windows Server Client Access License (CAL)[1]: Provide each user access to server functions from multiple devices for a single fee.		●	●
Managed Mobile Productivity	**Mobile device management:** Enroll corporate and personal devices to provision settings, enforce compliance, and protect your corporate data.	●	●	●
	Mobile application management: Publish, configure, and update mobile apps on enrolled and unenrolled devices, and secure or remove app-associated corporate data.	●	●	●
	Advanced Microsoft Office 365 data protection: Extend management and security capabilities across users, devices, apps, and data, while preserving a rich, productive end-user experience.	●	●	●
	Integrated PC management: Centralize management of PCs, laptops, and mobile devices from a single administrative console, and produce detailed hardware and software configuration reporting	●	●	●
	Integrated on-premises management: Extend your on-premises management to the cloud from a single console with Microsoft System Center Configuration Manager and Microsoft System Center Endpoint Protection integration for enhanced PC, Mac, Unix/Linux server, and mobile device administration.	●	●	●
Information Protection	**Persistent data protection:** Encrypt sensitive data and define usage rights for persistent protection regardless of where data is stored or shared.	●	●	●
	Document tracking and revocation: Monitor activities on shared data and revoke access in case of unexpected events.	●	●	●
	Intelligent data classification and labeling: Configure policies to automatically classify and label data based on sensitivity and then apply persistent protection			●
	Encryption key management per regulatory needs: Choose default key management options or deploy and manage your own keys to comply with regulations.			●
Identity-driven Security	**Microsoft Advanced Threat Analytics:** Detect abnormal behavior in on-premises systems and identify advanced targeted attacks and insider threats before they cause damage.		●	●
	Microsoft Cloud App Security: Gain visibility, control, and protection for your cloud-based apps, while identifying threats, abnormal usage, and other cloud security issues.	●		●
	Microsoft Defender for Identity[2]: Detect and investigate advanced attacks and suspicious behaviors on-premises and in the cloud.			●

[1]Customers purchasing Windows Server CAL agreements, System Center Configuration Manager, System Center Endpoint Protection, Microsoft Active Directory Rights Management Services CALs via the Microsoft Enterprise Volume Licensing agreements may purchase the Enterprise Mobility + Security Add-on offer

[2]Microsoft Defender for Identity previously known as Azure Advanced Threat Protection

MSP: andere opzet werkplek propositie

Ad-hoc 3rd party solutions

>€ 45
per mnd.

Business Premium

- Single sign on
- Conditional Access + MFA
- Endpoint anti-virus protection
- EDR
- Device management
- Productivity apps and file storage
- Chat based collaboration

Partner

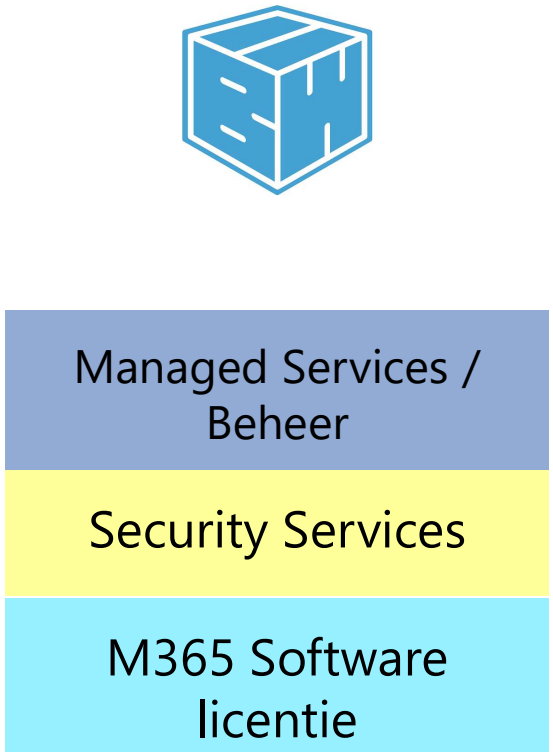
Meer services

Bied meer managed services voor klanten en verbreed het Security portfolio

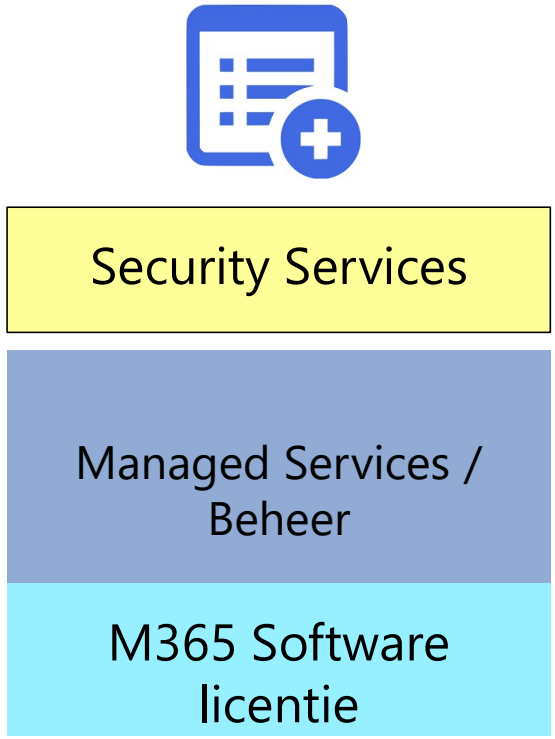
Microsoft 365 Business Premium

€ 20
per mnd.

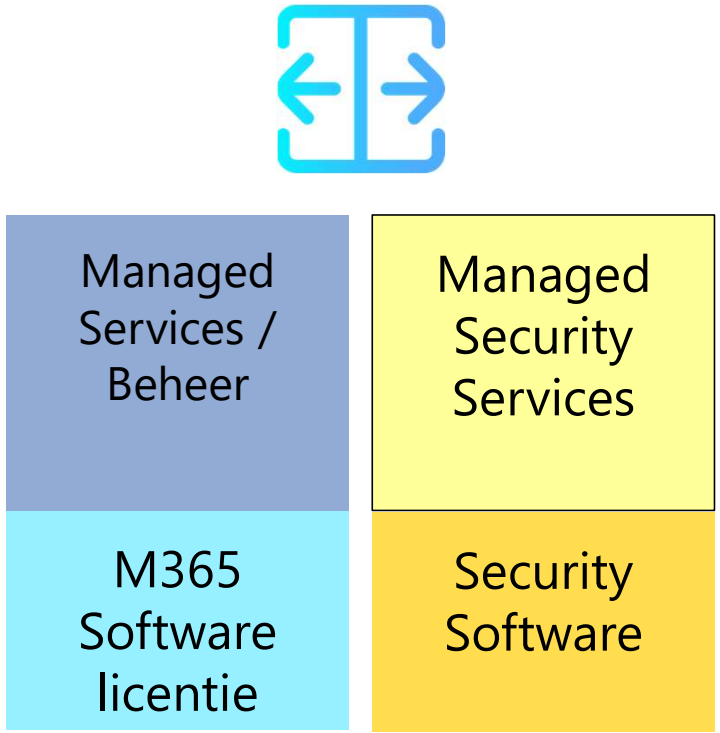
Werkplek propositie MSP: Met gebruik van EDR



1. Als onderdeel van de huidige werkplek propositie



2. Additioneel: Bovenop de Werkplek propositie

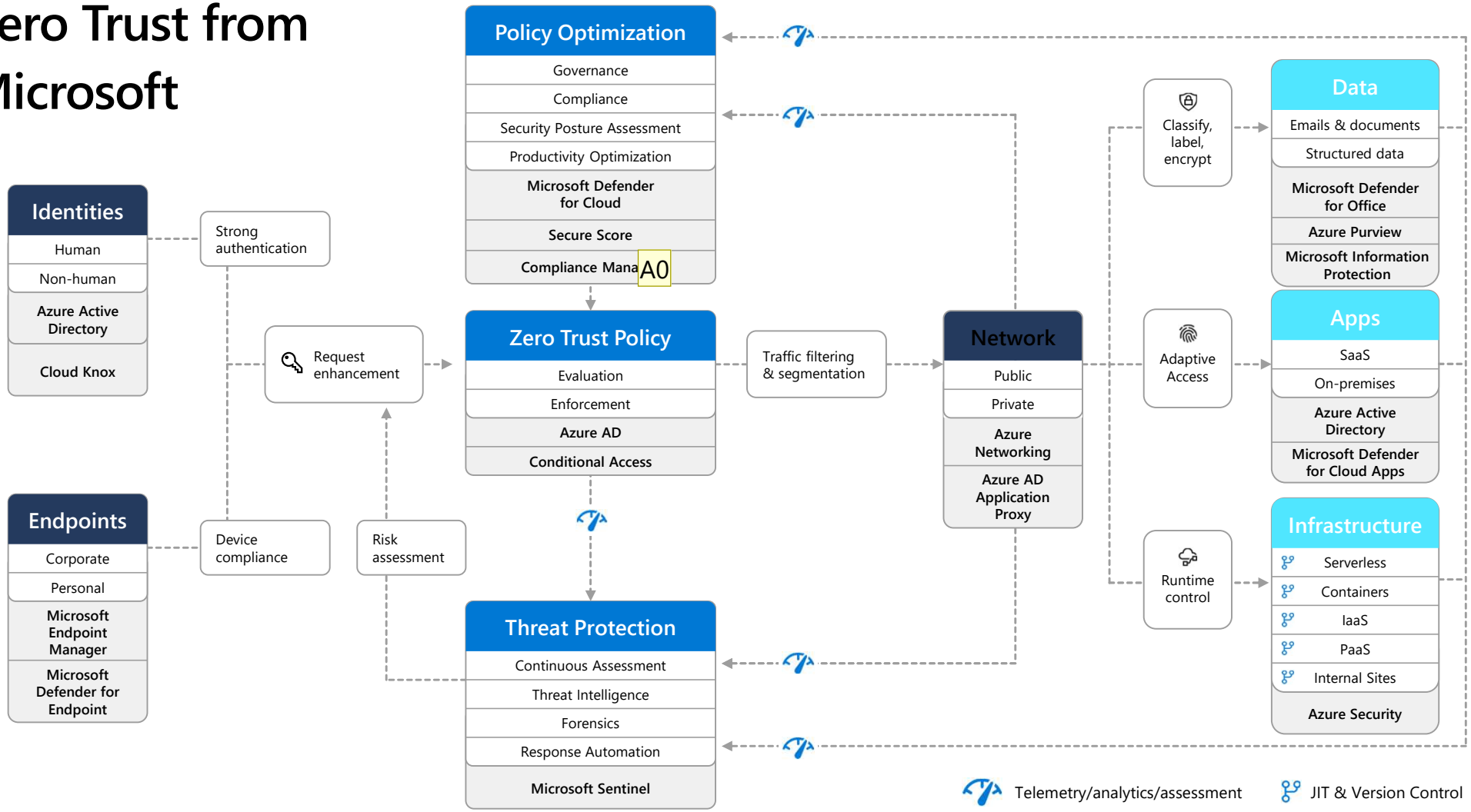


3. Naast elkaar: Onderscheid tussen Managed en Security services

Werkplek propositie MSP: Inpassen Security Services

	Als onderdeel van de huidige werkplek propositie	<u>Voor alle scenario's geldt:</u> ▪ Aanpassen SLA ▪ Uitbreiden Dienstenbeschrijving ▪ Aanpassen Leveringsvoorwaarden ▪ Definitie Managed Security Services ▪ Toepassen van Security Baseline
	Additioneel: Bovenop de Werkplek propositie	
	Naast elkaar: Onderscheid tussen Managed en Security services	

Zero Trust from Microsoft



Dia 12

A0 [Vermelding is verwijderd] please confirm where Cloud Knox should be in the Architecture
Auteur; 2022-01-13T19:14:06.978

A0 0 And correct name for Feb
Auteur; 2022-01-13T19:15:03.610

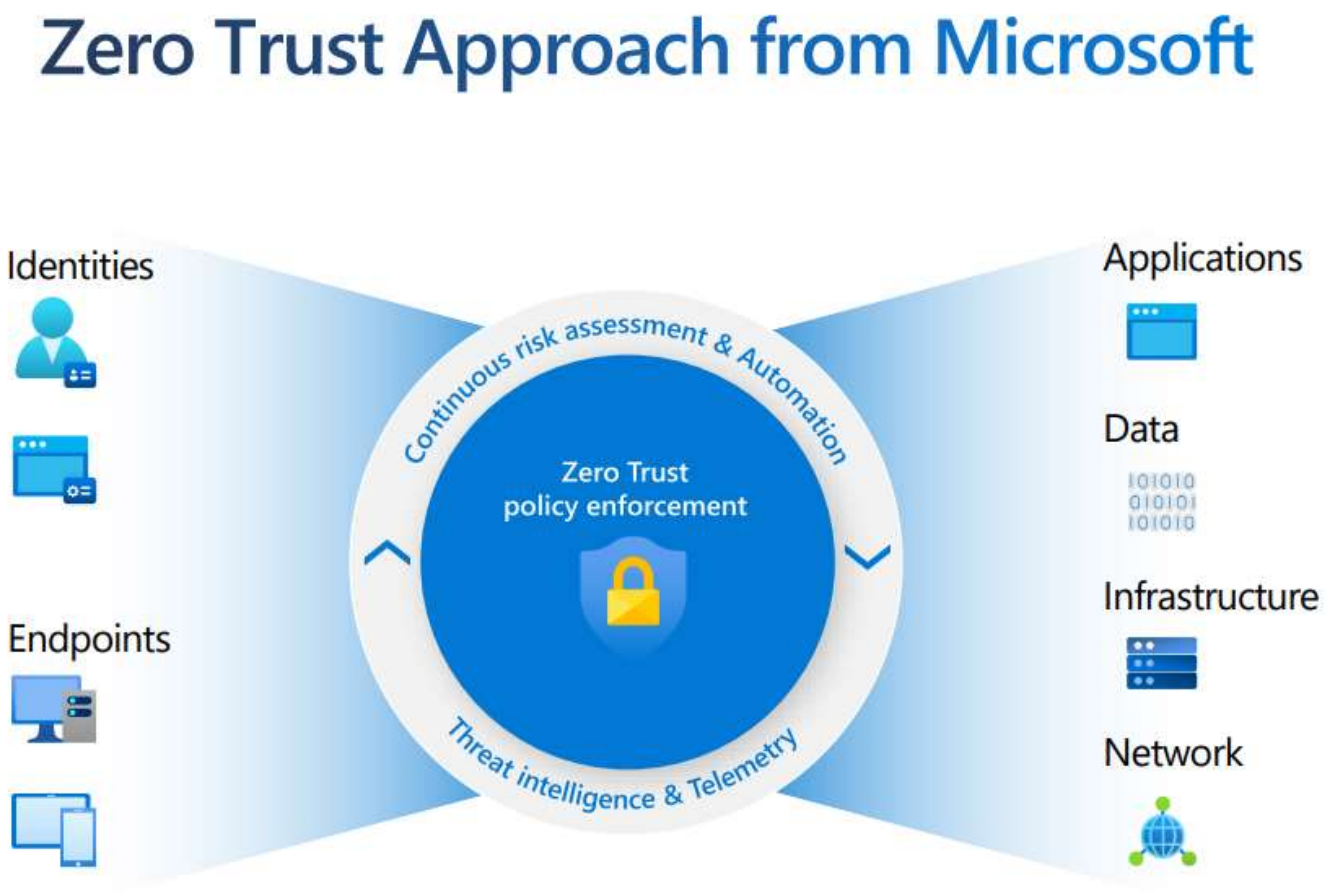
Zero Trust Componenten

Zero Trust components

The Zero Trust model and controls applies *across technologies*

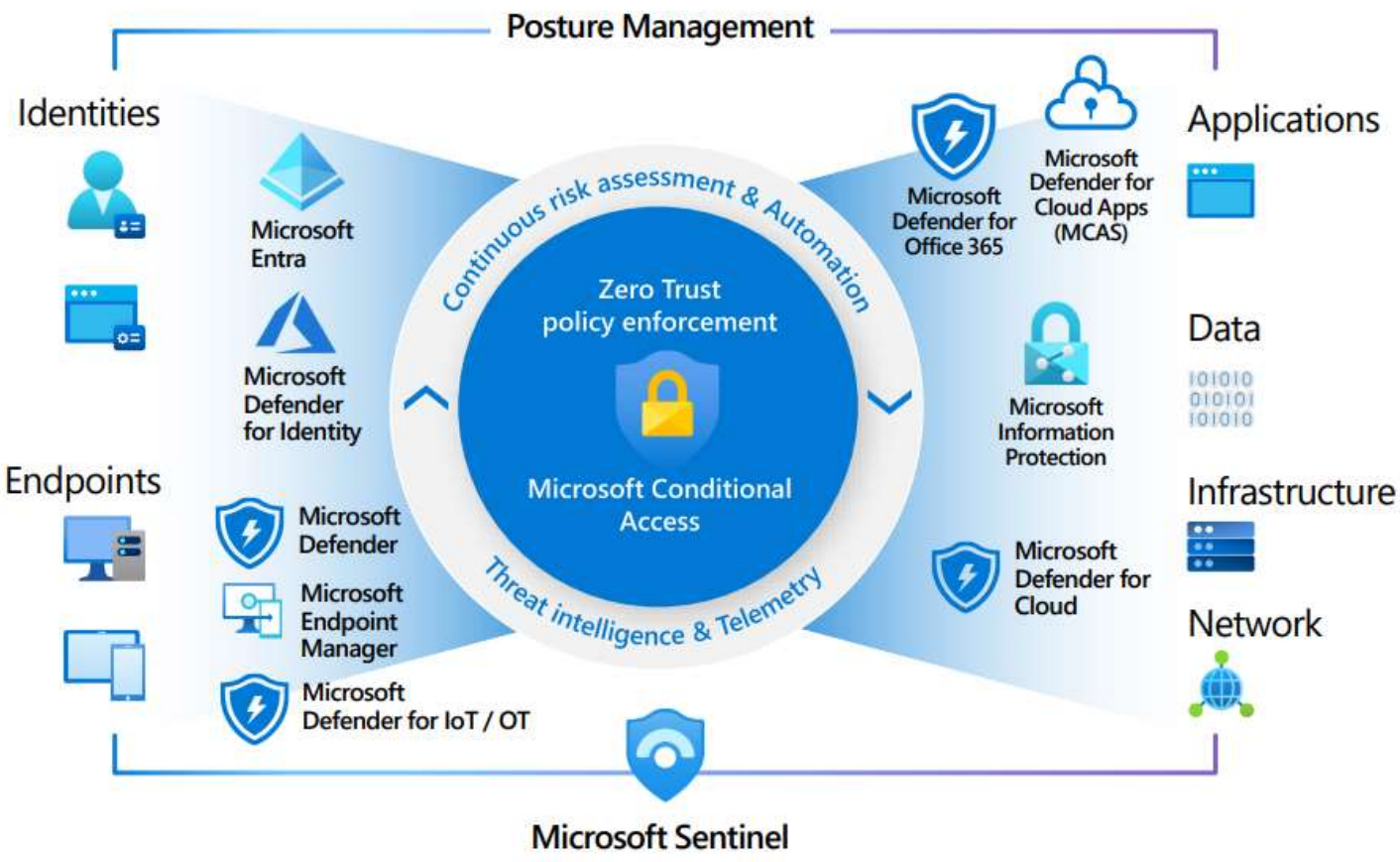
- Identities
- Endpoints
- Applications
- Data
- Infrastructure
- Network

Zero Trust benadering van Microsoft

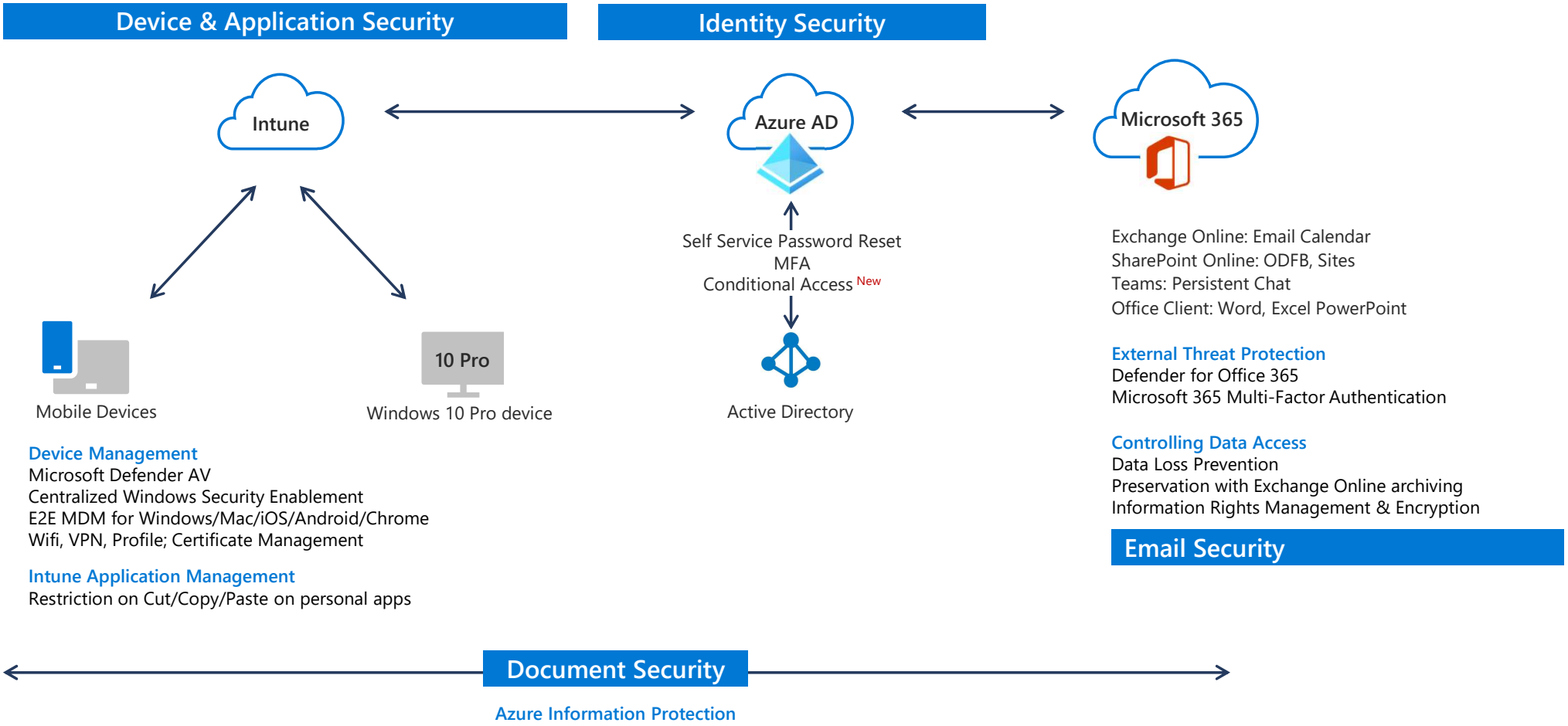


Zero Trust benadering van Microsoft

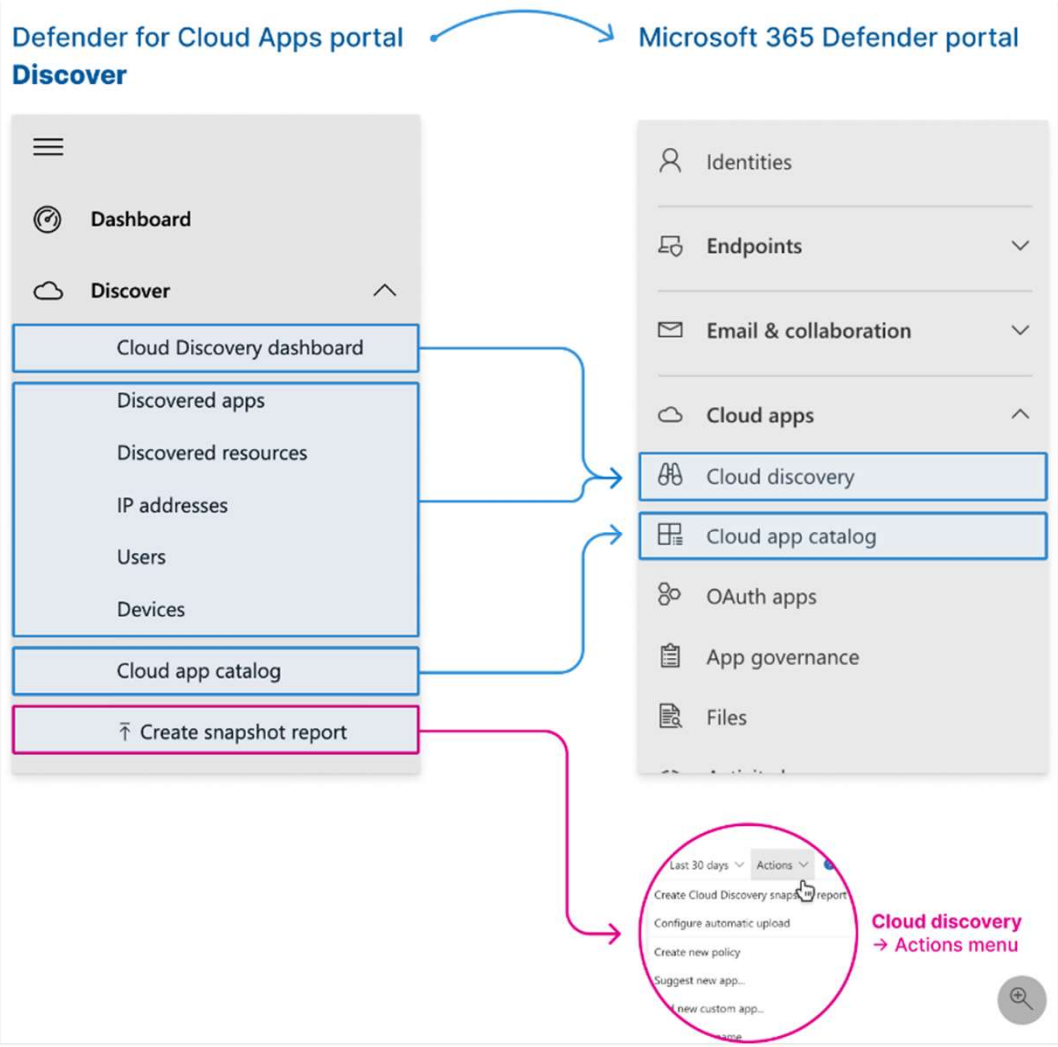
Microsoft Zero Trust Capabilities



Hoe werkt Microsoft 365 Business Premium?



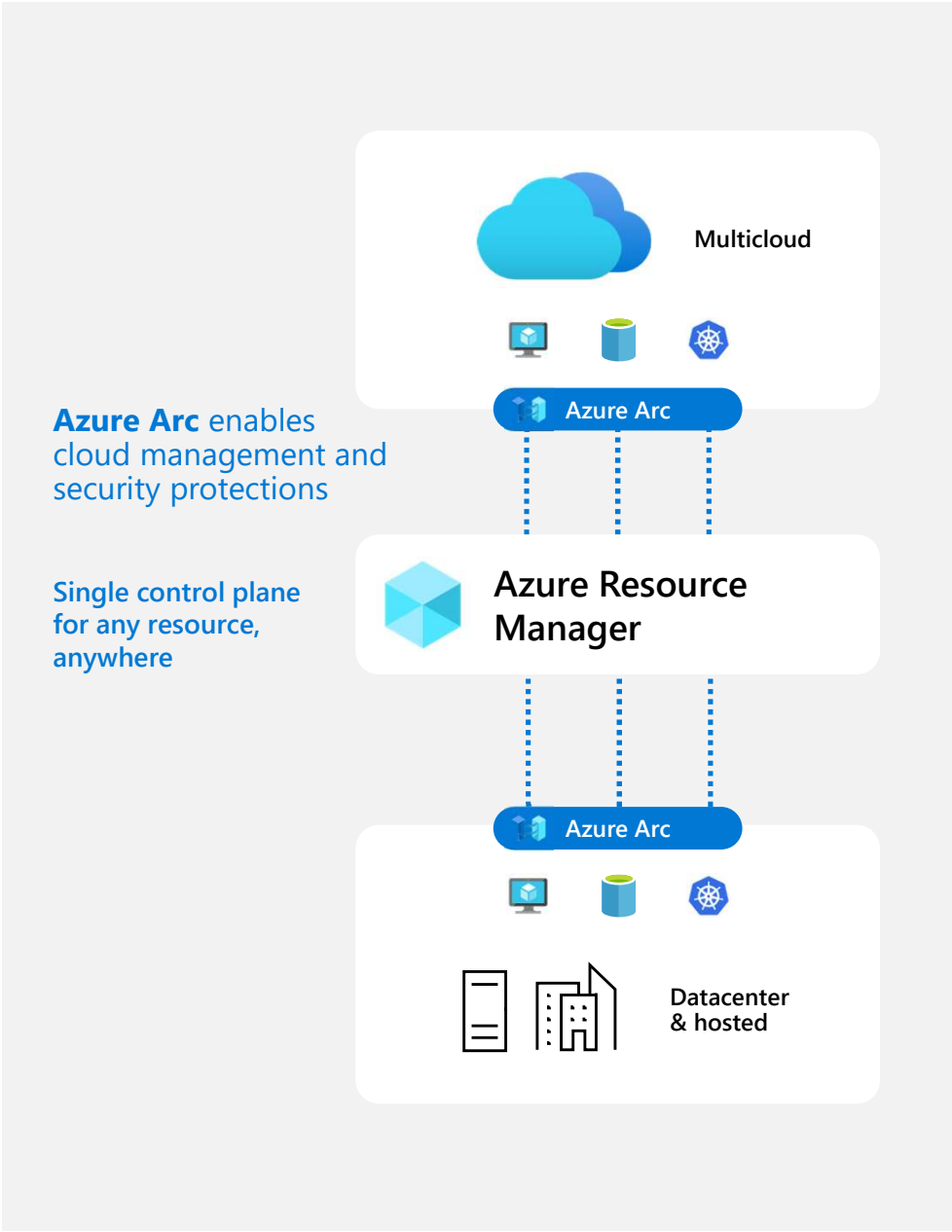
Defender for Business & Defender for Cloud Apps (CASB)



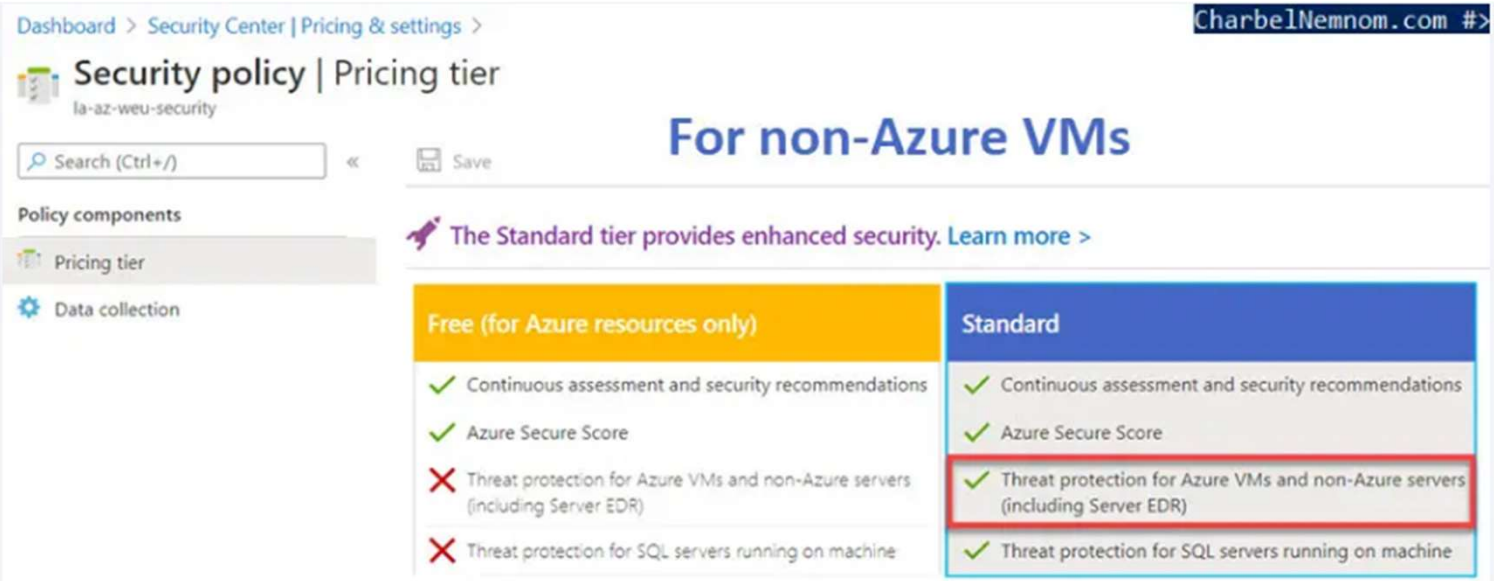
<u>Functie CASB</u>:
Collection of Log information
Usage & Downloads
Policies
Threat alerts
Governance/Compliance

Deploy Microsoft Defender for Cloud threat protection to your workloads anywhere with Azure Arc

- Extension installation, e.g. Log Analytics agent
- Enforce compliance and simplify audit reporting
- Asset organization and inventory with a unified view in the Azure Portal—Azure Tags
- Server owners can view and remediate to meet their compliance—RBAC in Azure



Defender for Cloud Setup with Defender for Endpoint/Business



Geautomatiseerde playbooks en handleiding met ChatGPT

Microsoft

Services rondom Defender portfolio
Opties Managed Security Services voor MSP’s

Compliance: Europese wetgeving op komst NIS 2

NIS covered sectors

- Finance
- Health
- Energy
- Banking
- Transport
- Water
- Digital Infrastructure
- Digital Service Providers

NIS2 expanded scope

- Providers of public electronic communications networks or services
- Digital services such as social networking service platforms and data centre services
- Waste water and waste management
- Space
- Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals)
- Postal and Courier Services
- Foods
- Public administration

NIS 2 verplichtingen (duties) in 2024

Where NIS only covered “Incidents” NIS 2.0 also covers “threats”
You are required to submit to the CSIRT (Computer Security Incident Response Teams) or, where relevant, the competent authority:
• Within 24 hours after becoming aware of the incident/threat you must provide an early warning
• Within 72 hours after becoming aware of the incident/ threat you must provide an Incident notification
• Upon request of a CSIRT (Computer Security Incident Response Teams) or authority an intermediate report
• Submit a final report not later than 1 month after the Incident/threat notification.

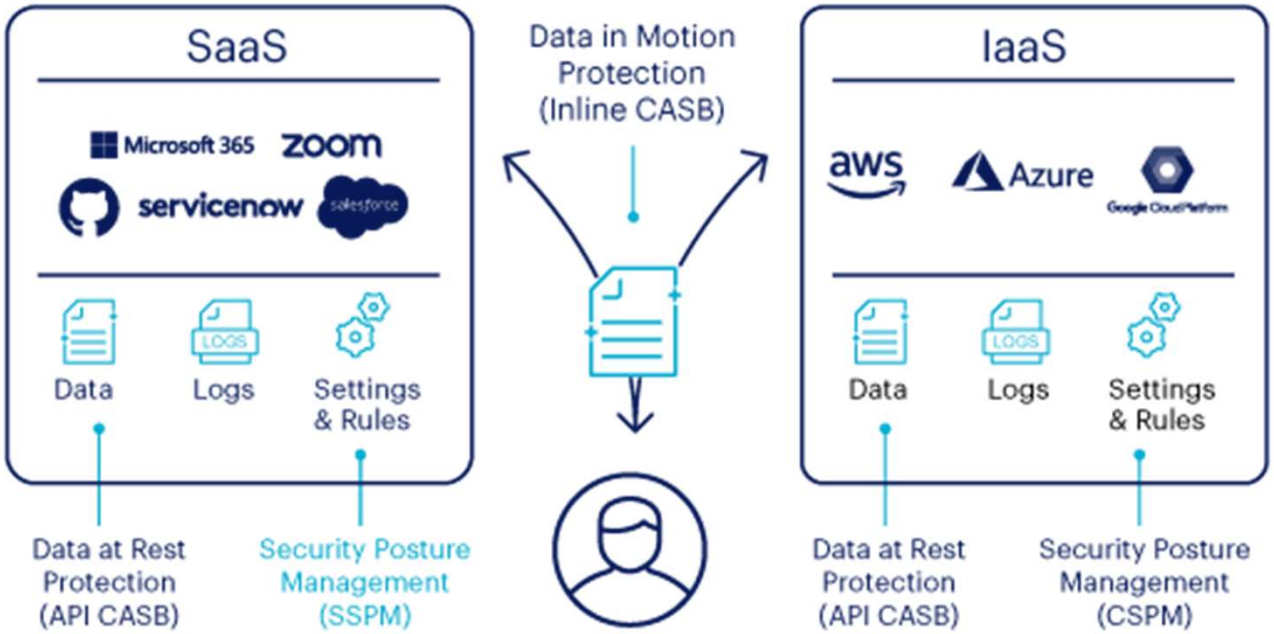
NIS 2 richtlijnen in 2023

Disaster Recovery ?

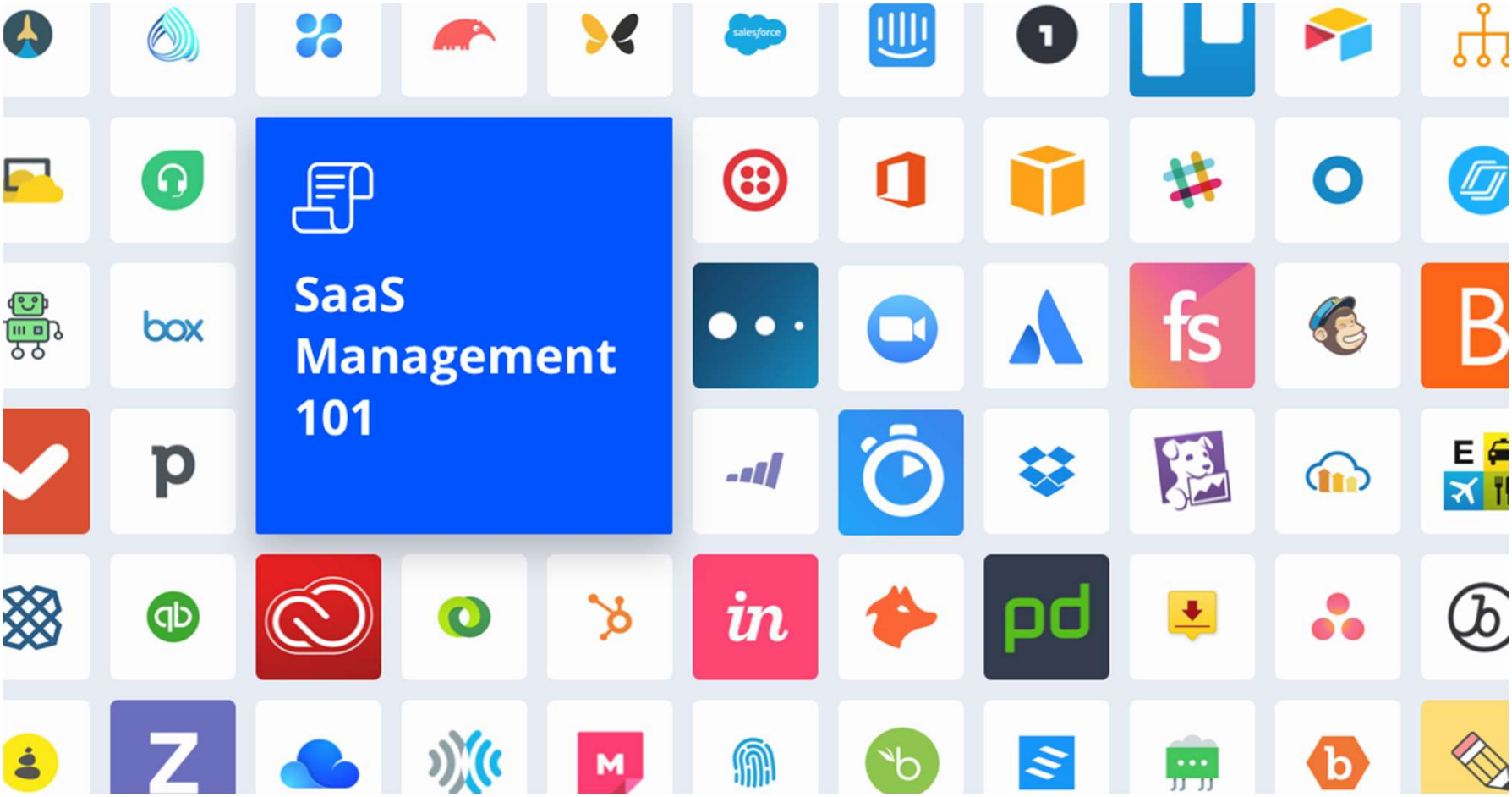
Managen van gebruik van AI tools

OpenAI

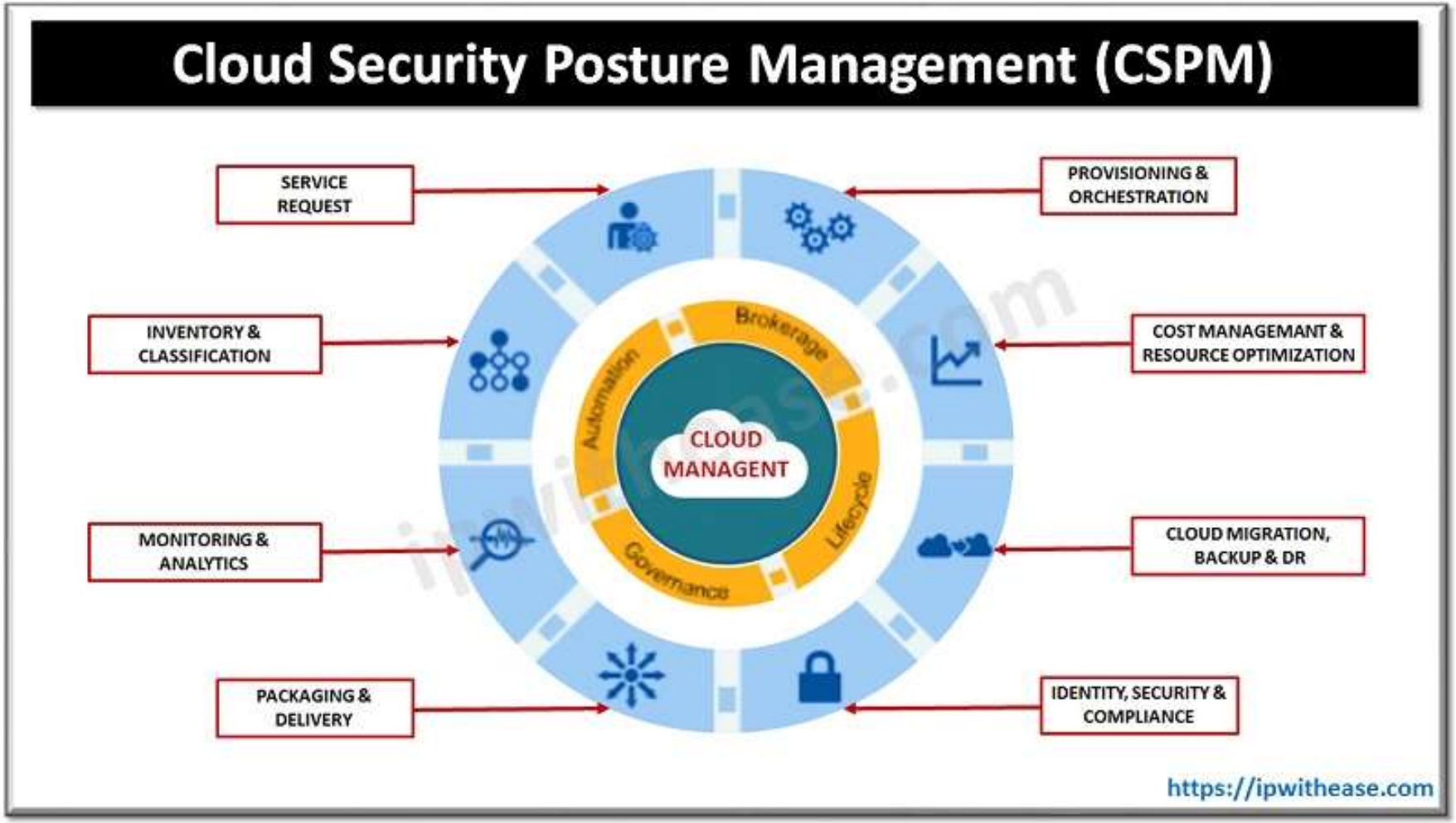
Ontwikkeling Services: Policy Management SaaS applicaties



Ontwikkeling Services: Management SaaS applicaties



Ontwikkeling Services: Policy & Posture Management



Security propositie inpassen MSP

Managed Services / Beheer

Security Services

M365 Software licentie

1. Werkplek propositie blijft de BASIS

MSP+/MSsP

Security Services

Security Software

Managed IT Services

M365 Software licentie

2. Breed Security Portfolio: MDR of SOCless SIEM

MSSP: SOC/SIEM

Managed IT Services / Beheer

Managed Security Services

M365 Software licentie

Security Software

3. Volwaardige MSSP met (eigen) SOC en SIEM

NIST Framework met Defender for Business

Microsoft 365 Business Premium

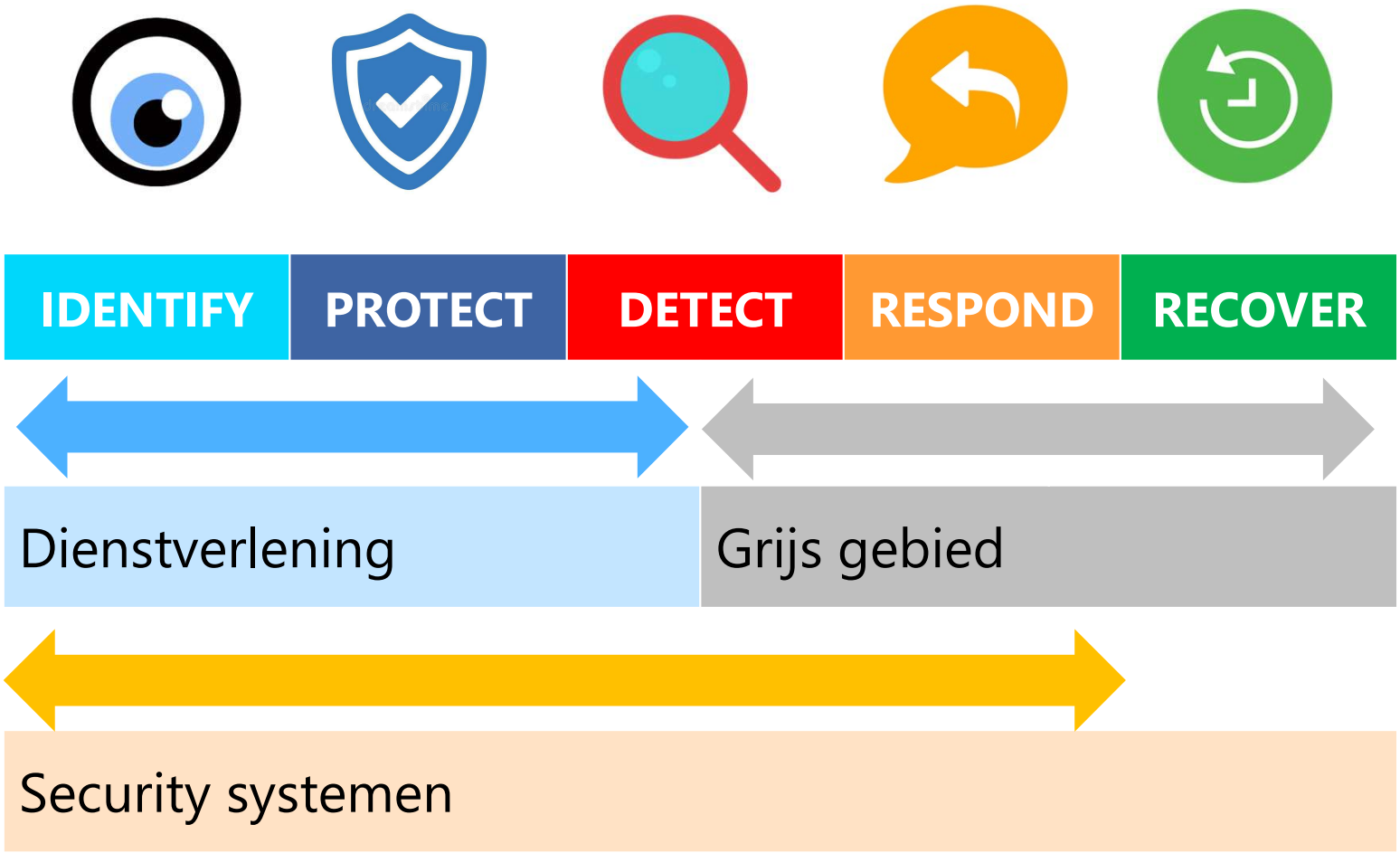




IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Secure Score Next Gen Protection Vulnerability scanning	MFA ASR (Attack Surface) Malware Dmarc API	EDR AIR Threat hunting Log files	EDR AIR (Automated Investigation & Response) Incident & Respons plan	Forensic services Recover Plan

NIST Framework met Defender for Business

Status Managed Services



NIST Framework

MSP Services Portfolio

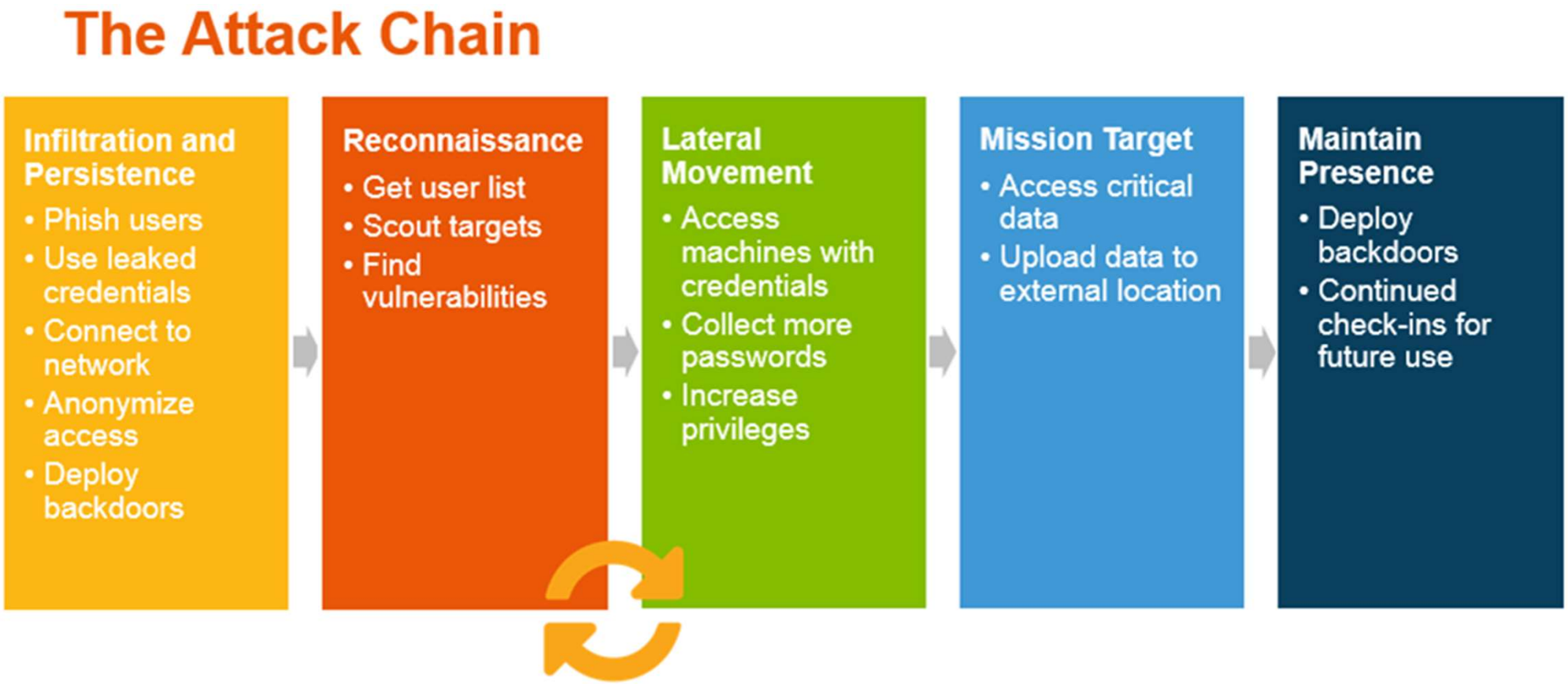
IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Secure Score PEN test CSAT Scan	Antivirus EDR MFA Email	EDR Dashboard	EDR & Incident & Respons plan	Incident & Respons plan
Separate Services	Defensieve Services	Defensieve Services	Defensieve Services	Separate Services

Managed Security Services

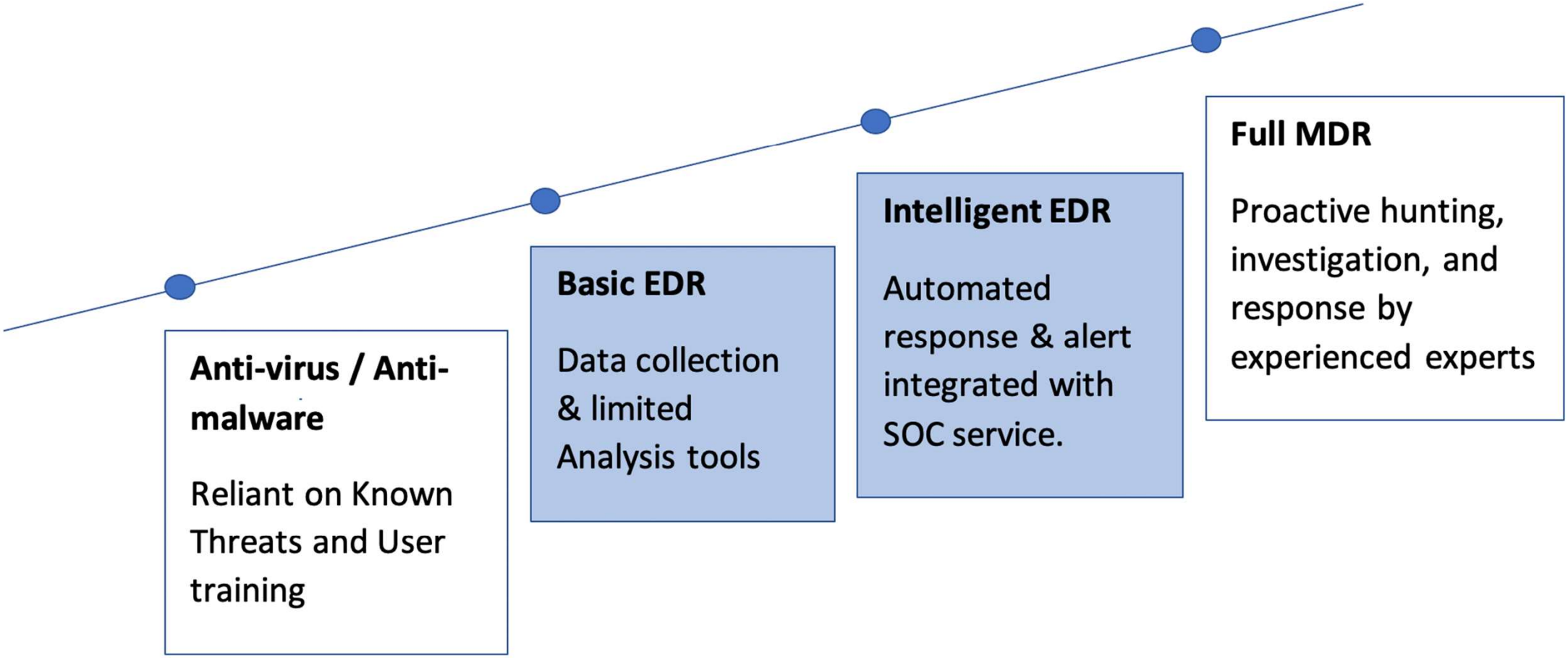
<u>KERNVRAGEN</u>:

Hoe ver gaan we hier in?
Welke functionele mogelijkheden hebben de tools?
Wat is je bereik?
Wat verwachten de klanten?
Welke rol bij een melding?

Cyber aanval proces



Microsoft Defender: van EDR naar MDR?

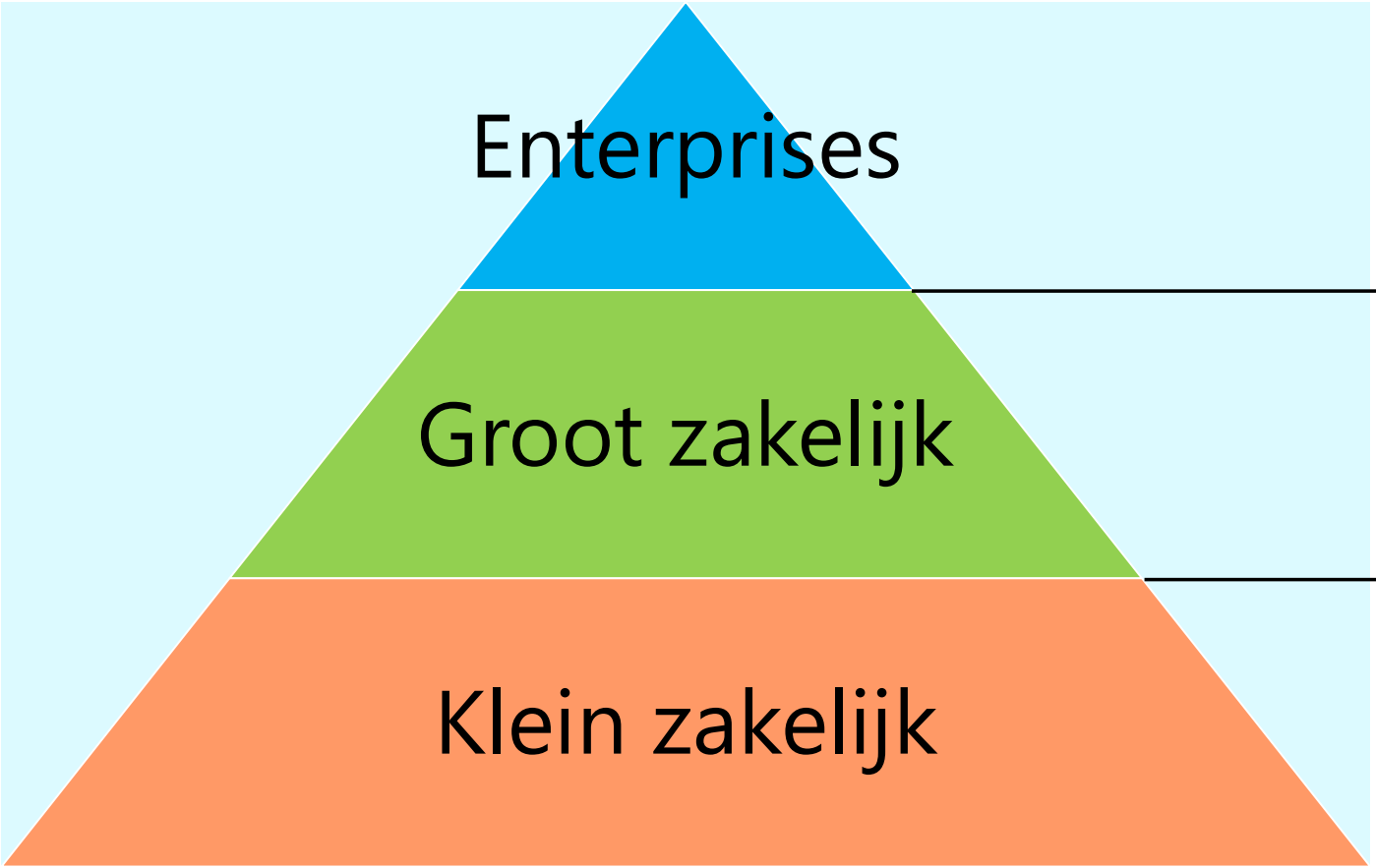


Managed Security Services

MSP	MSSP
Primary focus is IT operations and performance **The MSP+ shares this focus, with a greater emphasis on security*	Primary focus is cybersecurity
Provides administration, IT, and some cybersecurity services	Provides 24/7 cybersecurity services
Often partners with customers' IT and Ops teams	Often partners with in-house security professionals through their SOC

Hoogwaardige Security propositie per segment

FRONTLINE BUSINESS



SOC/SIEM

a) SOC-less SIEM

b) Inhuur SOC

EDR+ oplossing

Security propositie inpassen MSP

Managed Services / Beheer

Security Services

M365 Software licentie

1. Werkplek propositie blijft de BASIS

MSP+/MSsP

Security Services

Security Software

Managed IT Services

M365 Software licentie

2. Breed Security Portfolio: MDR of SOCless SIEM

MSSP: SOC/SIEM

Managed IT Services / Beheer

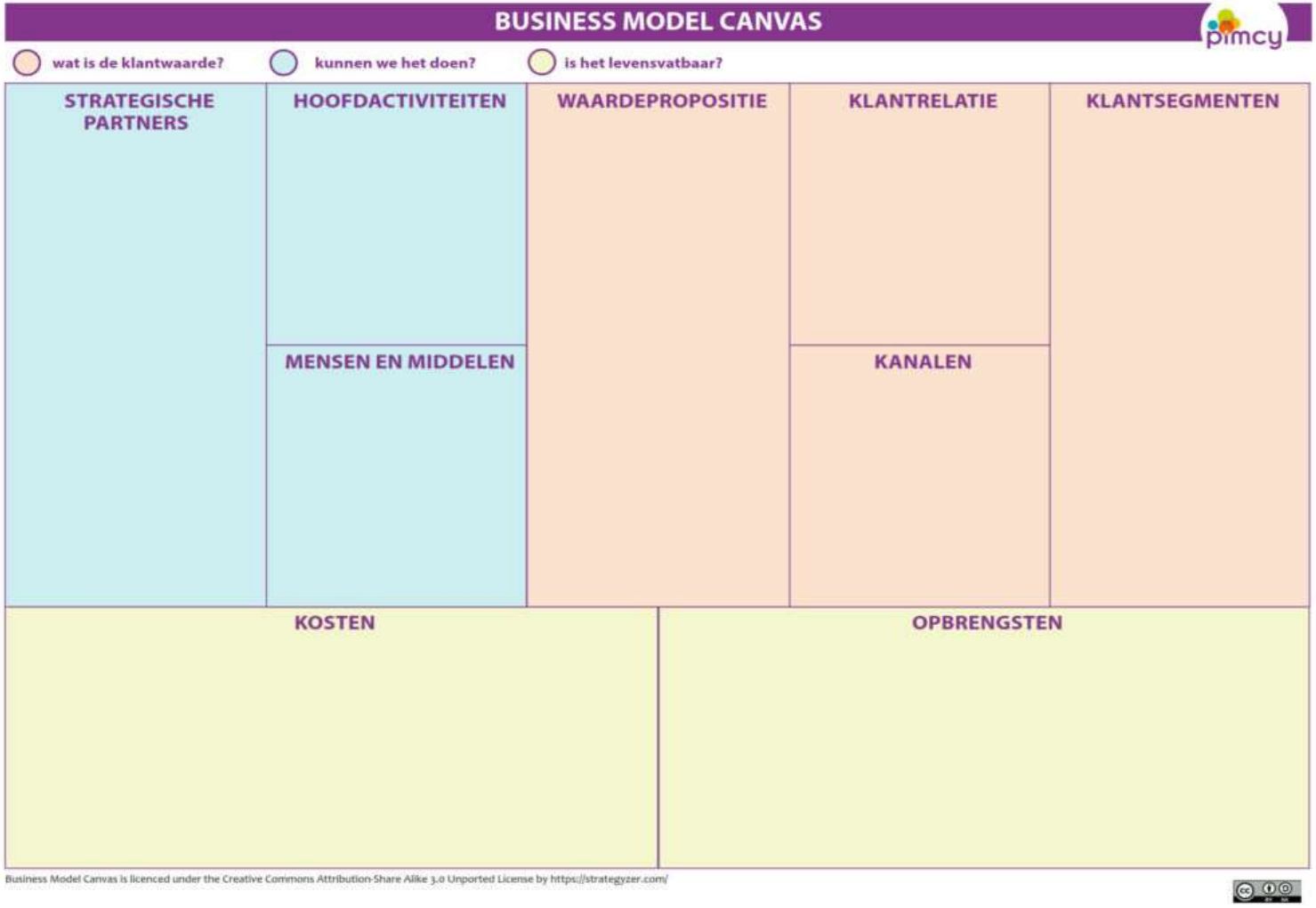
Managed Security Services

M365 Software licentie

Security Software

3. Volwaardige MSSP met (eigen) SOC en SIEM

Business Model Canvas



Scenario 1 MSP: De Werkplek centraal

Key Partners

Keten-partners Met Security proposities

Key Activities

Support INFRA & werkplek

Key Resources

Huidige (NOC) team

Value Propositions

De Veilige Werkplek?

Customer Relationships

Standaard Werkplek + andere MSP's?

Channels

Customer Segments

Voornamelijk SMB

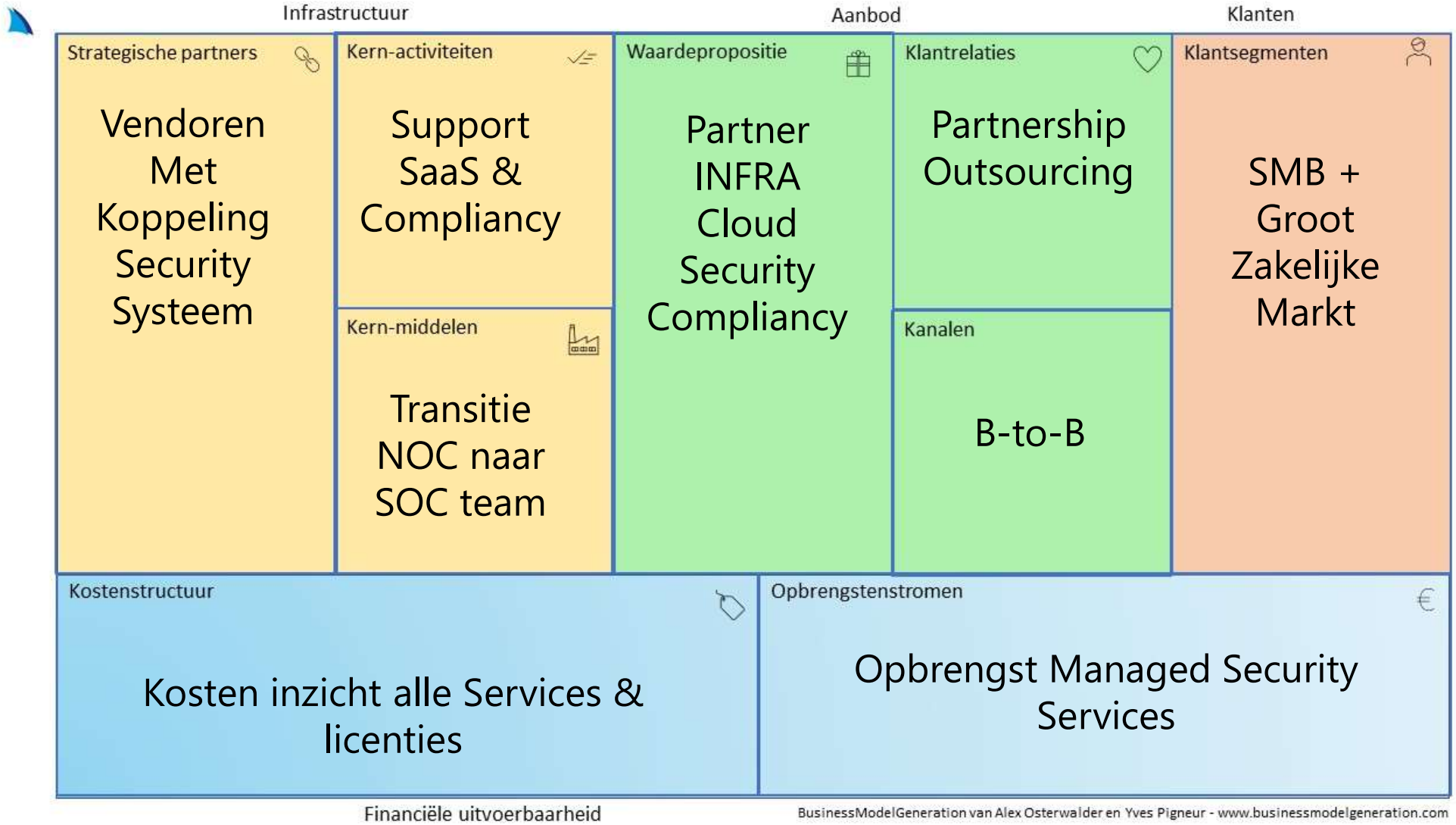
Cost Structure

Kosten per Werkplek en gerelateerde services & licenties

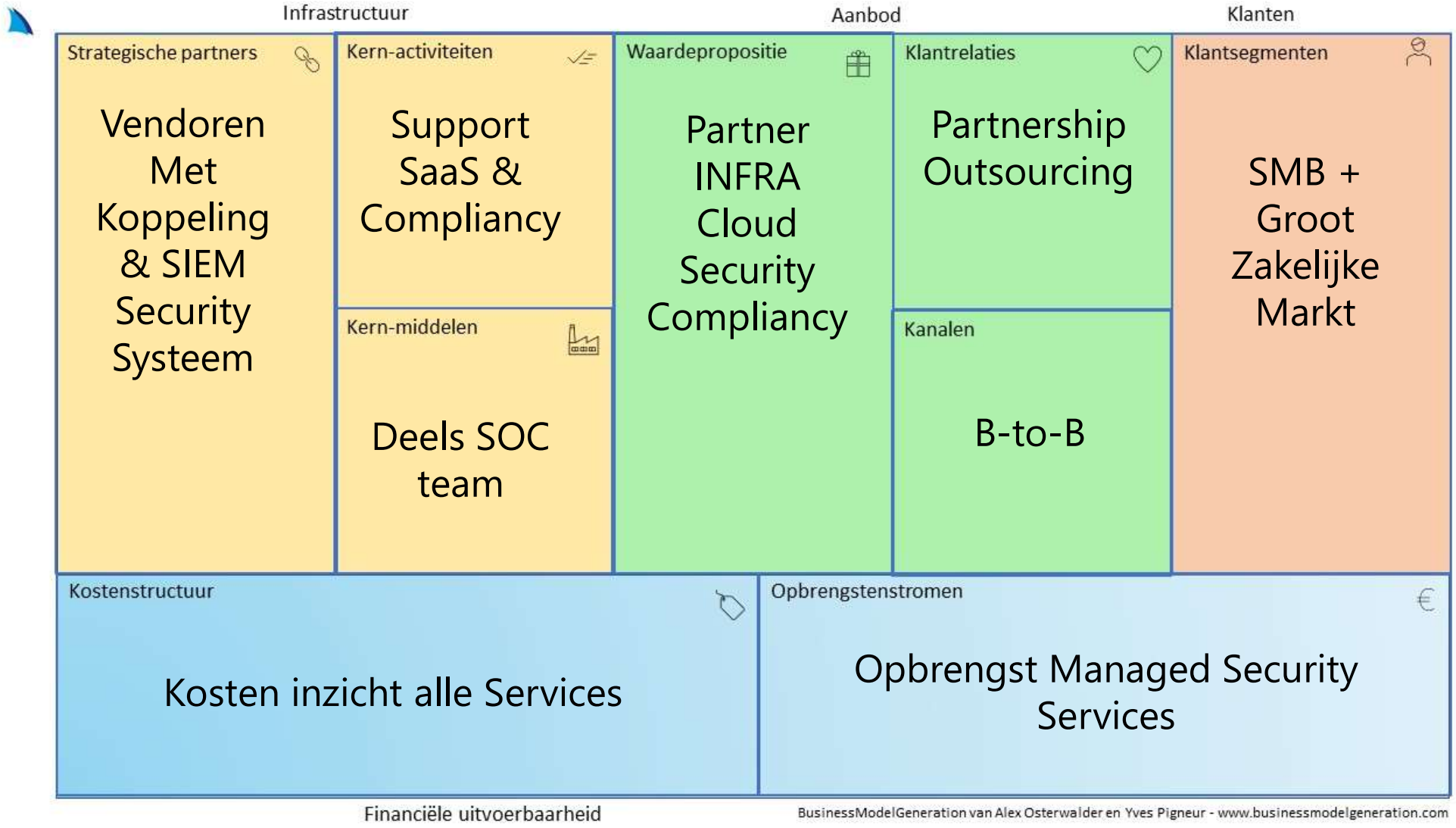
Revenue Streams

Opbrengst per Werkplek

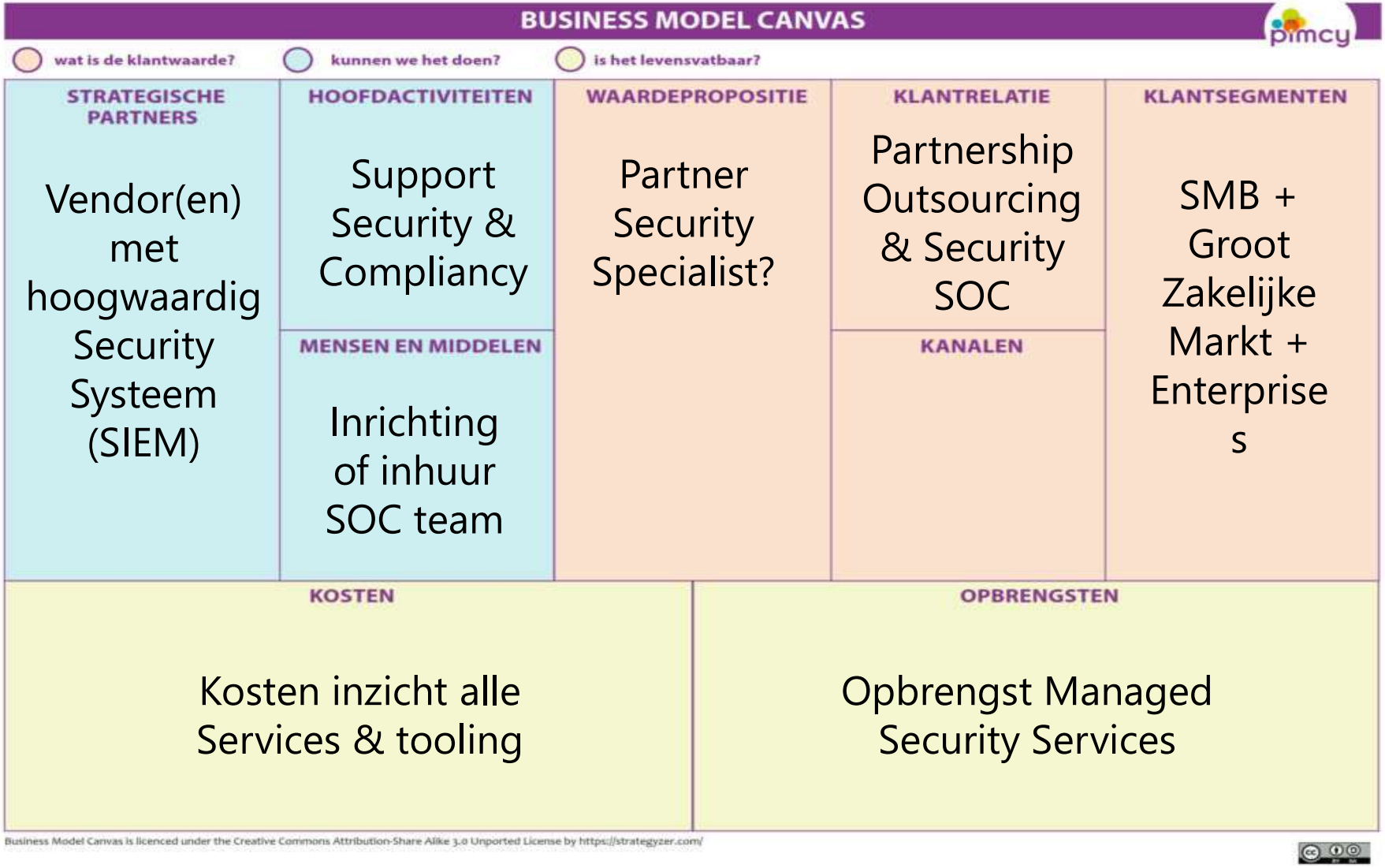
Scenario 2A MSP: De Next Gen MSP / MSsP



Scenario 2B MSP: De Next Gen MSP & inhuur SOC/SIEM



Scenario 3 MSSP: met SOC/SIEM



Dienstenbeschrijvingen Managed (Security) services

Reactieve diensten
Meldingen van Gebruikers (incidenten & tickets)
Meldingen van Security Systemen (Triage)
Meldingen van Systemen
Wijzigingen Gebruikers

Pro actieve diensten
Monitoring van meerdere dashboards
Patches van diverse software
Updates van diverse software
Changes uitvoeren

Preventieve diensten
Back-up controleren (dagelijks)
Aanbevelingen (Recommandations) opvolgen
Nieuwe functies en Applicaties

Hoeveel UUR per dag/week/maand is hiervoor nodig?
Hoeveel MELDINGEN per dag/week/maand komen binnen?

Managed (Security) Services 2023: Calculatie

FRONTLINE BUSINESS

Reactieve diensten	Alerts	Uren
Meldingen van Gebruikers (incidenten & tickets)		
Meldingen van Security Systemen (Triage)		
Meldingen van Systemen		
Wijzigingen Gebruikers		

Preventieve diensten	Alerts	Uren
Back-up controleren (dagelijks)		
Aanbevelingen (Recommandations) opvolgen		
Nieuwe functies en Applicaties		

Pro actieve diensten	Alerts	Uren
Monitoring van meerdere dashboards		
Patches van diverse software		
Updates van diverse software		
Changes uitvoeren		

Totaal Overzicht	Alerts	Uren
Reactieve diensten		
Pro actieve diensten		
Preventieve diensten		

Opties MSP's op een rij: Samenvatting

	Kansen	Bedreigingen
De Werkplek Centraal	- Afbakening Security oplossingen - Eenvoud voor de klein zakelijke markt	- Hoeveel tools maken de werkplek veilig genoeg? - Andere MSP's nemen het Security domein over
Next Gen MSP of MSsP	- Verbreding Security portfolio - Afstemmen op NIS 2.0 of security baseline - Uitbesteden SOC/SIEM als aanvulling	- Leerproces om Security Services in te vullen (dashboards) - Waar ligt de grens van de dienstverlening? - Uitbesteden SOC/SIEM; marge & controle?
MSSP	- Duidelijkheid: zo volwaardig mogelijk - Onderscheid IT vs Security dienstverlening	- SOC inrichten: bemanning zoeken - Concurrentie met bestaande SOC/SIEM spelers

Protect multicloud environments from development to runtime

Resources

- ESG Technical Validation
- Microsoft Defender for Cloud Interactive Guide
- Defender for Cloud Blog
- Defender for Cloud Tech Community
- Defender for Cloud in the field video series
- Documentation and quick starts

Start a free trial

Key Zero Trust Resources

to help you on your Zero Trust journey

Zero Trust Resources

aka.ms/zerotrust

Maturity Model

aka.ms/ztmodel

Business Plan

aka.ms/ZTbizplan

Deployment Guidance

aka.ms/ztguide

- Zero Trust: Security Through a Clearer Lens session (Recording | Slides)
- CISO Workshop Slides/Videos
- Microsoft's IT Learnings from (ongoing) Zero Trust journey