Microsoft 365 A5 Security

Bescherm uw school tegen digitale bedreigingen

Hoe hard een school ook werkt om hun medewerkers en studenten te informeren over de constante en versneld evoluerende digitale bedreigingen, ook dan kan de meest attentvolle gebruiker onbewust geïnfecteerde bestanden openen of op kwaadaardige weblinks klikken. Inbreuken op de beveiliging zijn onvermijdelijk. De beste strategie is het maximaal beveiligen van alle aanvalsvectoren via automatisatie, gebruikmakend van artificiële intelligentie. **Microsoft 365 A5 Security** biedt beveiligingsoplossingen die deze aanvalsvectoren aanpakken door bedreigingen te ontdekken, te analyseren en te neutraliseren voordat ze schade veroorzaken.

Identity & Access Management

Identiteit, apps, gegevens en apparaten **beveiligen**

Threat Protection

Stop schadelijke aanvallen met geïntegreerde en **geautomatiseerde** beveiliging

Security Management

Verhoging van weerbaarheid door de juiste **inzichten** en begeleiding

School als veilige werk- en leerplek

In een ideale wereld zou een school zich geen zorgen hoeven te maken over hun digitale veiligheid, helaas is dit niet de realiteit. Het onderwijs staat op de tweede plaats, na de gezondheidszorg, als mogelijk doelwit voor hackers. Scholen worden tevens blootgesteld aan nieuwe informatiebeveiligingsrisico's, de eindgebruikers zijn zich minder bewust van gerichte oplichtingspraktijken zoals phising, ransomeware, datalekken, ... Eénmaal het slachtoffer wordt de dagelijkse werking danig verstoord. Daarnaast legt nieuwe wet- en regelgeving (GDPR | AVG) extra druk en complexiteit op het aantonen van naleving van de bescherming van persoonsgegevens, in het bijzonder voor K-12 scholen door het verwerken van gegevens van minderjarigen.

Het verder negeren van cybersecurity kan nefaste gevolgen hebben. Daarom kunnen scholen geen afwachtende houding aannemen en zijn ze genoodzaakt om beveiliging ter harte te nemen. Als goede huisvader proberen we allemaal onze scholen te beschermen, denk maar aan brandpreventie, inbraakbeveiliging, ... en veel te vaak wordt de digitale infrastructuur vergeten. De school moet de identiteit en de gegevens van alle personeelsleden, de kinderen en hun ouders beschermen zodat die van veilig onderwijs kunnen genieten.

Gebrek aan vaardigheden en middelen

Cybersecurity is een complexe materie die heel wat knowhow en skills vereist om hier op de juiste manier mee om te gaan. Georganiseerde cybercriminaliteit is jammer genoeg een wijdverspreid feit in deze moderne tijden en vraagt daarom ook om een sterk gestructureerde en globale aanpak. Scholen hebben vaak niet de kennis en ervaring om tegen dergelijke criminele organisaties op te boksen of hebben de middelen niet ter beschikking om hier iets aan te doen. Scholen staan in een spagaat, het aantrekken van ervaren cybersecurity personeel is niet evident en ook vaak duur.

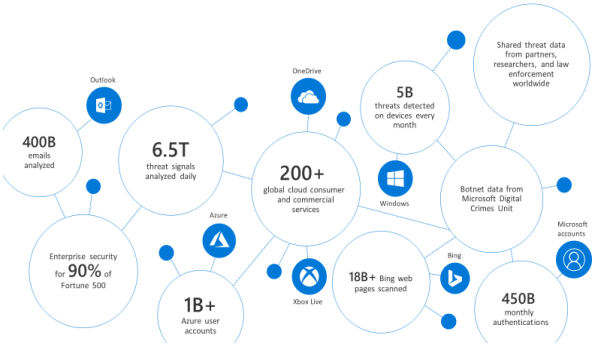
Microsoft 365 A5 Security

Standaardisatie & automatisatie: de ICT-coördinator ontlasten

De ICT-coördinator heeft dan ook zijn of haar handen vol met het beheer van alles wat IT betreft. Vaak heeft deze persoon maar enkele uurtjes ter beschikking per week om dit allemaal te doen, waardoor dit quasi niet haalbaar is om in je eentje te (blijven) dragen. Vaak wordt het IT-beheer ook gedaan door leerkrachten die wat kennis hebben van informatica, maar daarom geen technische profielen zijn. Deze mensen doen hun uiterste best om alles zo goed mogelijk te handhaven in hun beperkte tijd. Om manuele taken of monitoring te vereenvoudigen bevat de **Microsoft 365 A5 security** component geautomatiseerde acties gebaseerd op industriestandaard processen en best practices om de ICT-coördinator maximaal te assisteren. Op die manier wordt de ICT-coördinator ontlast van deze taken waardoor hij zich kan focussen op de kritische bedreigen die zijn aandacht nodig hebben om zo het cyber beveiligingsniveau significant te verhogen.

Microsoft Security als geïntegreerd platform

Microsoft Security is een erkende industrieleider op het gebied van cybersecurity en staat bovenaan in vijf Gartner Magic Quadrants. https://www.microsoft.com/security/blog/2019/12/03/microsoft-security-leader-5-gartner-magic-quadrants/



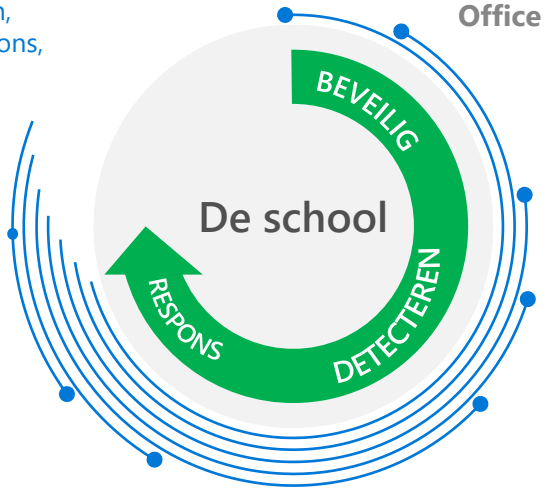
Onze security producten zijn eenvoudig toepasbaar, sterk geïntegreerd en halen hun intelligentie uit de triljoenen gedeelde signalen die dagelijks worden gegenereerd via de Microsoft Intelligent Security Graph. Ze zijn het kloppend hart van al onze security componenten. Op die manier ben je niet meer in silo's aan het werken (bv. endpoint op zich, email op zich, etc.) maar kijk je holistisch naar security over heel de organisatie. Aanvallen worden complexer daarom is zo'n holistisch beeld op uw securitysituatie als maar belangrijker. Microsoft is uniek in de markt met dit innovatieve security platform. Deze security componenten werken ook met niet-Microsoft-oplossingen, zoals applicaties of infrastructuur die on-premises (hybride) of bij andere cloudproviders worden beheerd. Microsoft Defender ATP, de Microsoft Endpoint Security oplossing die deel uitmaakt van de **Microsoft 365 A5 Security** offering, kan je ook cross platform gebruiken, zoals macOS, iOS, Android tot zelfs Linux. Defender is er niet alleen meer voor Windows en Office 365. **Microsoft 365 A5 Security** is een all-in-one geïntegreerd pakket. Het maakt het gebruik van een verzameling aan best-of-breed en/of open source toepassingen overbodig. Deze zijn slechts beperkt integreerbare en bieden geen volledige oplossing.

Cross platform, preventieve beveiliging van endpoints, detectie na inbreuken, geautomatiseerd onderzoek en respons, URL content filtering, ...

Microsoft Defender ATP

Veilige email, bijlagen, weblinks en upload van bestanden

Office 365 Advanced Threat Protection



Actuele dreigingsinformatie & simulatie van aanvallen

Office 365 Threat Intelligence

Detecteren en onderzoeken van geavanceerde identiteitsaanvallen (ook hybride en on-prem)

Azure ATP

Controle en grip op het gebruik van cloud apps

Microsoft Cloud App Security

Veilig gebruik van Microsoft cloud diensten en controle van identiteiten, op basis van Machine Learning. (Azure Identity Protection)

Azure Active Directory Plan 2

Microsoft 365 A5 Security

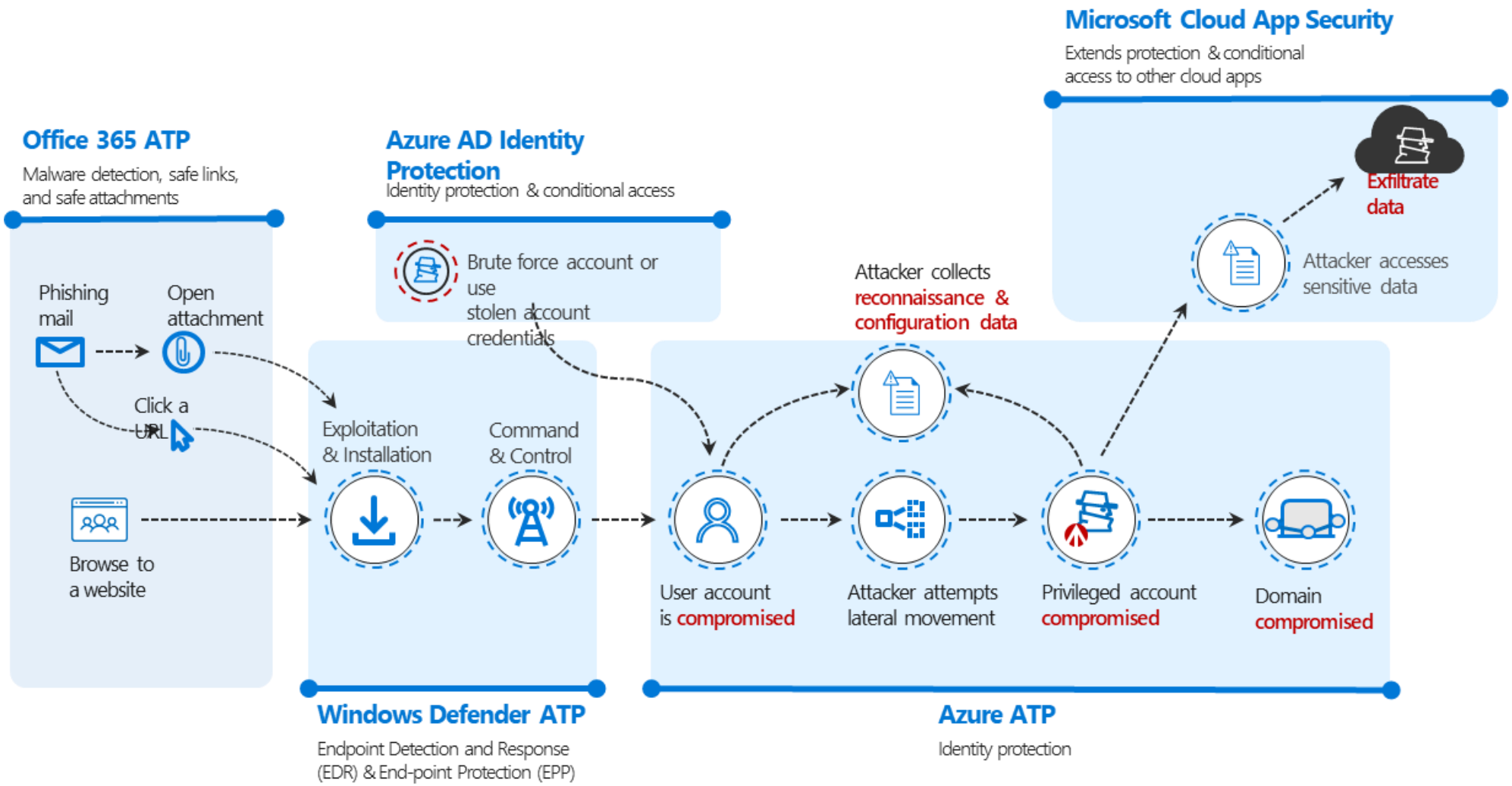
Microsoft 365 A3 / A5

Het Microsoft 365 A3 platform biedt "best-of-suite" (geïntegreerde) technologie voor productiviteit en samenwerken inclusief basiscomponenten voor security. De meerwaarde van M365 A5 security is meer dan alleen automatisatie. Het belangrijkste is dat je met de security features van A5 veel meer visibiliteit krijgt en acties gaat kunnen uitvoeren en je ook veel beter beschermd bent tegen de geavanceerde aanvallen. **Microsoft 365 A5 security** helpt u om uw digitale infrastructuur te beveiligen tegen cybercriminaliteit.

	Item	A1	A3	A5
Platform				
1	Audit logging	✓	✓	✓
2	Geavanceerde Audit Logging (1 jaar)			✓
3	Secure Score voor inzage huidige security niveau	✓	✓	✓
Toegangscontrole				
4	Azure Multi-Factor Authenticatie (MFA)	✓	✓	✓
5	Beveiligingen tegen bedreigingen in Office 365	✓	✓	✓
6	MFA en conditionele access		✓	✓
7	Privileged Identity Management			✓
8	Identity Protection			✓
9	Risico gebaseerde conditionele toegang			✓
10	Selfservice Password Reset	✓	✓	✓
11	Password Protection		✓	✓
12	Uitrollen van MDM en vereisen van compliant devices		✓	✓
Beveiliging tegen bedreigingen				
13	Office 365 Advanced Threat Protection			✓
14	Azure Advanced Threat Protection (ATP)			✓
15	Microsoft Defender (ATP)			✓
16	Microsoft Threat Protection			✓
17	Microsoft Cloud App Security			✓
Databeveiliging				
19	Intune mobile app protection		✓	✓
29	App Bescherming via Intune		✓	✓

Microsoft 365 A5 Security

Protection across the attack kill chain



A5 - Security

Office 365 Advanced Threat Protection (O365 ATP)

Iedere dag zijn er weer nieuwe malware-aanvallen. O365 ATP beveiligt realtime mailboxen, bestanden, online opslag en toepassingen tegen nieuwe, geavanceerde aanvallen. O365 ATP biedt een holistische bescherming in Microsoft Teams, Word, Excel, PowerPoint, Visio, SharePoint Online en OneDrive voor Bedrijven. O365 ATP biedt beveiliging tegen onveilige bijlagen, continue beveiliging tegen schadelijke webkoppelingen en bescherming tegen phishing aanvallen.

Het is daarmee een aanvulling op de beveiligingsfuncties van Exchange Online Protection en beveiligt zo beter tegen zero-day-aanvallen.

O365 ATP:

- Realtime e-mail beveiliging tegen nieuwe, geavanceerde aanvallen.
- Beveiliging van onveilige bijlagen en schadelijke links naar het internet.
- Sandboxing/detonatie analyse scanning van bestanden die geüpload worden
- Bescherming tegen phishing aanvallen.

Office 365 Threat Intelligence (O365 TI)

O365 TI is een verzameling van inzichten en informatie die beschikbaar is in het Office 365 Security & Compliance Center. Met deze inzichten kan het beveiligingsteam de organisatie beschermen tegen aanvallen. O365 TI controleert signalen en verzamelt gegevens uit meerdere bronnen, zoals gebruikersactiviteit, authenticatie, e-mail, besmette pc's en beveiligingsincidenten. Beheerders van Office 365, beveiligingsbeheerders en beveiligingsanalisten kunnen gebruik maken van de informatie om bedreigingen voor gebruikers en intellectueel eigendom te begrijpen en om adequaat te kunnen reageren.

O365 TI:

- Geeft het Security Operations Team relevante en actuele dreigingsinformatie vanuit de Microsoft Cybersecurity Groep.
- Bestaat uit diverse tools om aanvallen te simuleren (bijv. Phishing e-mails) waardoor de bewustwording van medewerkers verhoogt en het risico van een gerichte aanval vermindert.

Microsoft Cloud App Security (MCAS)

Met MCAS houdt de organisatie controle op het gebruik van SaaS-applicaties dankzij inzicht en controlemogelijkheden. MCAS brengt Shadow-IT in kaart en beschikt over de mogelijkheden om risico's te beoordelen, beleid af te dwingen, activiteiten te onderzoeken en bedreigingen te stoppen. Door MCAS kan de organisatie veiliger overstappen naar de cloud terwijl de controle over essentiële gegevens wordt behouden.

MCAS:

- Monitort en beschermt tegen bedreigingen van je SaaS-applicaties.
- Beschermt je kritieke gegevens in SaaS-applicaties. Bijvoorbeeld: het opslaan van sensitieve documenten of PII-data naar opslaglocaties als Dropbox en Google Drive wordt tegengehouden of direct versleuteld.
- Brengt schaduw-IT in kaart waarna op basis van een risicoscore van de SaaS-applicatie het mogelijk is om beleid af te dwingen, activiteiten te onderzoeken en bedreigingen te stoppen.

Azure Active Directory Plan 2 (AAD P2)

Azure Identity Protection maakt deel uit van AAD P2.
AAD P2 biedt risk-based conditional access tot apps en kritieke bedrijfsgegevens op basis van de identiteit van de medewerker. Tevens biedt AAD P2 Privileged Identity Management voor het detecteren, beperken en bewaken van beheerders en hun toegang tot Microsoft diensten door de inzet van 'Just-In-Time-toegang'.

Azure Active Directory Plan 2:

- Voor veilig gebruik van Microsoft cloud diensten en controle van identiteiten.
- Zorgt voor synchronisatie en bescherming tussen on-premise en cloud identiteiten.
- Helpt diefstal van digitale identiteiten te voorkomen door inzicht in gedrag en risico.
- Geeft beheerders beperkt en tijdelijke toegang waarbij activiteiten worden gemonitord.

Azure Advanced Threat Protection (Azure ATP)

Azure ATP bewaakt het gedrag van gebruikers, apparaten en resources en detecteert afwijkingen. Dankzij de ingebouwde intelligentie levert Azure ATP snel inzicht in geavanceerde bedreigingen zowel onpremise als in de cloud.

Azure ATP:

- Detecteert en onderzoekt geavanceerde persistente bedreigingen over lokale, cloud-en hybride omgevingen voordat ze schade veroorzaken.
- Identificeert verdachte activiteiten van gebruikers en apparaten op basis van detectie met bekende technieken en gedragsanalyse.
- Geeft duidelijke geprioriteerde informatie over aanvallen weer op een tijdslijn.

Microsoft Defender Advanced Threat Protection

Microsoft Defender ATP is een cross platform voor intelligente beveiliging, automatische detectie, onderzoek en respons mogelijkheden (oftewel een Endpoint Detection and Response (EDR) oplossing). Microsoft Defender ATP beschermt endpoints (clients en servers) tegen cyberbedreigingen, detecteert geavanceerde aanvallen en gegevenslekken, automatiseert beveiligingsincidenten en verbetert de beveiligingspositie.

Met Microsoft Defender ATP:

- Doe je aan risicobeheersing en mitigatie door de inzet van artificiële intelligentie.
- Gebruik je de kracht van de cloud om use-cases te definiëren waar directe acties aan worden gekoppeld om de ict coördinator te ontlasten.
- Geeft je inzicht in gecompromitteerde devices en/of systemen waarna er een geautomatiseerd onderzoek gestart kan worden voor het bepalen van de impact. Opvolgend kan een geautomatiseerde oplossing de aanval blokkeren.