
# Product omschrijving

# Inhoud

## Wat doet Bastion 365

Standaard emaildiensten zoals Microsoft 365, Google Workspace en bestanden uitwisselingsdiensten zoals WeTransfer voldoen niet aan alle eisen vanuit normeringen zoals NTA7516, NEN7510 en NEN7512. Deze diensten mogen dus niet gebruikt worden voor het versturen en ontvangen van bijzondere persoonsgegevens waaronder ook persoonlijk medische informatie.

Bastion 365 is een uitbreiding op uw emaildienst en biedt extra mogelijkheden om berichten en bestanden veilig te kunnen versturen en ontvangen. Het is een extra bescherming laag op al uw berichtenverkeer.

Bastion 365 is een SaaS oplossing bovenop Microsoft 365 en Microsoft Azure. Het wordt gekoppeld aan uw eigen Microsoft omgeving met mail connectoren, dataopslag en gebruikersbeheer. Alles blijft dus in uw eigen beheer en doordat het volledig integreert, wordt voorkomen dat er dubbel gebruikersbeheer of mailsystemen nodig zijn.
Alles is instelbaar binnen de configuratieportalen van Bastion 365 en van MS Exchange Online.

Door direct te integreren binnen de cloud hoeft er op de lokale werkplekken niks geïnstalleerd te worden, worden alle apparaten automatisch ondersteund (laptop, tablet, smartphone en web access) en hoeven medewerkers zelf niet belast of getraind te worden in gebruik.

Bastion 365 classificeert berichten op inhoud, voert beveiligingsvalidaties uit op ontvangers en verstuurt deze berichten, afhankelijk van hun classificatie, op een zo veilig mogelijke manier zodat altijd voldaan wordt aan de verplichte eisen vanuit uw sector. De berichtenregels zijn volledig en flexibel instelbaar en sluiten zo aan bij het beveiligingsbeleid van uw eigen organisatie.

# Functionaliteiten

## Berichten classificatie

Alle berichten worden geclassificeerd binnen Bastion 365. Afhankelijk van deze classificatie kan de organisatie bepalen op welke wijze berichten verstuurd moeten worden. Binnen Bastion 365 zijn er meerdere mogelijkheden om berichten te classificeren, deze opties zijn allemaal optioneel en naast elkaar te gebruiken.

- Microsoft Information Protection, bestaande labels vanuit Microsoft Purview.
- Exchange Online Routeringsopties en mailheaders.
- Handmatige classificatie middels een knop binnen Outlook of andere mail applicatie.
- Herkenning van termen uit woordenlijsten zoals medische termen, SNOMED, DSM-5 of Psychiatrische termen.
- Herkenning van patronen zoals adressen, postcodes, IBAN, BSN, paspoortnummers en telefoonnummers.
- Herkenning van bijlagen zoals specifiek medische bijlagen als DICOM, HL7, EDIFACT en FHIR.
- Herkenning van algemeen gedeelte domeinen (@gmail, @hotmail, @ziggo, ect)
- Herkenning tegen organisatie specifieke domeinen. (Vertrouwde organisaties of juist zwarte lijsten).
- Organisatie specifieke reguliere expressies. (eigen dossiernummers, zaaknummers of patiëntennummers)

## Kanalen

Er worden verschillende beveiligde kanalen ingesteld. Organisaties kunnen op basis van de classificatie bepalen welke kanalen gebruikt mogen worden.
Afhankelijk van de beveiliging opties welke de ontvangende mailserver ondersteund wordt, worden deze ingedeeld in kanalen. Bastion 365 controleert op de volgende beveiliging opties: NTA7516 records, DNSSEC, DKIM, DMARC, TLS(versies), DANE, SPF, x509 en de geografische locatie de mailserver (binnen of buiten de EU).
Op basis van de aanwezigheid van gecontroleerde beveiligingsmogelijkheden wordt voor ontvangende mailservers het meest veilige email kanaal gekozen.

- NTA 7516, het kanaal wat volledig voldoet aan de NTA7516 eisen. Hierbij ondersteunen wij ook volledige interoperabiliteit met alle andere aanbieders van Veilig Mailen.
- AVG, voor een gegarandeerd aflevering server-to-server met encryptie, geheel volgens de eisen van de AVG.
- mTLS, voor een gegarandeerd aflevering server-to-server met encryptie waarbij organisaties elkaar vertrouwen en verbindingen vastpinnen op basis van vertrouwde mailserver certificaten.

- Microsoft 365, waarbij berichten verstuurd worden via de reguliere exchange server van de organisatie.
- eDelivery, een kanaal waarbij berichten via een beveiligde portal opgehaald kunnen worden met Multi-factor-authenticatie. (het standaard kanaal volgens de NTA7516/AVG om bijzondere persoonsgegevens te delen met patiënten/cliënten/burgers). Berichten zijn hier volledig instelbaar met een geldigheidsduur, antwoord mogelijkheden, het bijvoegen van bestanden en berichten doorstuur mogelijkheden.
- Organisatie specifieke kanalen, voor daar waar specifieke eisen nodig zijn.

## Authenticatie

Bij het eDelivery kanaal moeten ontvangers zicht authentiseren met een tweede factor. Dit zullen met name patiënten/cliënten/burgers zijn. Hier biedt Bastion 365 de volgende mogelijkheden.

- SMS, een combinatie van een unieke link naar het emailadres samen met een one-time-password (code) via SMS naar de ontvanger.
- Authenticator, een combinatie van een unieke link naar het emailadres samen met een one-time-password (code) via een authenticator app van de ontvanger.
- “Break the Glass” procedure is toe gevoegd voor situaties waarbij het noodzakelijk is om een bericht direct te versturen en men niet in het bezit is van een mobiele telefoon, telefoonnummer of andere vorm van authenticatie.
- Een centraal adresboek kan bijgehouden, geïmporteerd of gekoppeld worden om te voorkomen dat verzenders steeds het mobiele telefoonnummer moeten opgeven.

## Webformulieren

Bastion 365 biedt webformulieren aan welke organisaties op hun eigen publiek website kunnen plaatsen. Deze worden ook wel conversatiestarters genoemd.
Hiermee kunnen externen, bijvoorbeeld patiënten/cliënten/burgers, via Veilig Mailen berichten en/of bestanden sturen naar de organisatie. Organisaties bepalen zelf wat voor bestanden mogen worden meegestuurd. Hier zijn twee type formuleren beschikbaar.

- Standaard webformulieren, iedereen mag een door de organisatie gedefinieerde webformulier insturen en welke via Veilige Mailen wordt geleverd bij de organisatie.
- Webformulieren met authenticatie. Mensen moeten zich eerst authentiseren met email en SMS verificatie voordat ze een webformulier kunnen insturen. Op deze manier beschikt de organisatie direct over een geverifieerd emailadres en SMS-nummer van de indiener. Eventueel kan ook nog een geautomatiseerde workflow aan het webformulier gekoppeld worden.

## Grote bestanden

Naast Veilig Mailen ondersteunt Bastion 365 ook het Veilig Versturen én Veilig Ontvangen van grote bestanden. Dit geheel beveiligd en in overeenstemming met de geldende normen zoals NEN7510, NEN7512 en ISO27001. Ook is het mogelijk om deze oplossing aan uw eigen organisatie MS Azure Storage account te koppelen zodat bestanden altijd binnen uw eigen organisatie blijven.

- Versturen van grote bestanden; medewerkers kunnen op het Bastion 365 gebruikersportaal een bericht opstellen en hieraan middels upload/drag-and-drop grote bestanden toevoegen. De maximale grootte is hierbij onbeperkt. De ontvanger ontvangt het bericht in zijn email en na authenticatie kan deze de bestanden downloaden.

- Ontvangen van grote bestanden; Bastion 365 kan zo ingericht worden zodat externen ook op een veilige wijze grote bestanden naar uw organisatie kunnen sturen. Dit kan middels een reactie op een eDelivery bericht of webformulier (met eventuele authenticatie). Deze berichten en grote bestanden kunnen behalve het portaal ook rechtstreeks in Outlook afgeleverd worden. In de ontvangen berichten staan de fiches/downloadlinks en de daadwerkelijke bestanden staan in uw eigen beveiligde Microsoft Azure Storage account. Organisaties houden zo zelf de volledige controle over ingaande en uitgaande grote bestanden.

## Huisstijl

Bastion 365 is volledig in te richten naar de huisstijl van uw eigen organisatie. Hierdoor komt het berichtenverkeer vertrouwd over zoals verstuurd vanuit uw eigen organisatie. U heeft dus niet de noodzaak om ontvangers vooraf te informeren over het gebruik van een externe berichtendienst.

- Berichten en templates zijn volledig aan te passen met eigen teksten, kleuren, logo's en stijlen.
- Domein / URL's zijn aanpasbaar naar uw eigen domeinen.

## Logging & Inzicht

Bastion 365 logt alle transacties van berichten welke via de dienst verstuurd en ontvangen worden. Hierdoor is het ook mogelijk om een afleverstatus in te zien, een afleverbevestiging te verkrijgen en nog niet afgeleverde berichten in te trekken.

- Transactielog, over verstuurde en ontvangen berichten met inzicht in aflever statussen.
- Dashboards, voor verstrekken van inzichten met welke partijen uw organisatie communiceert, overzichten van het beveiligingsniveau van uw berichtenverkeer en de classificatie van berichten.

- Rapporten, daar voor waar specifieke wensen zijn, kan met rapportages berichtenstromen inzichtelijk gemaakt
- Auditlogs worden bijgehouden van alle wijzigingen door beheerders binnen de dienst.

## Externe koppelingen

Bastion 365 beschikt over meerdere technische koppelvlakken zoals een API en SMTP koppeling voor aansluitmogelijkheden met externe systemen zoals EPD systemen (Epic/Chipsoft/Nedap), CRM systemen (SalesForce/Dynamics), DMS systemen (SharePoint) en PACS systemen (DICOM).
Zo kunnen vanuit deze systemen ook veilig en conform alle normen direct berichten en bestanden verstuurd en ontvangen worden.