Cisco Cloud Mailbox Defense

cisco Partner
Distribution Partner

Een veiligere mailbox dankzij betere voorspellingen, preventie, detectie en respons

Cloud Mailbox Defense van Cisco biedt alles dat uw klanten nodig hebben om hun security te verbeteren en gebruikers te beschermen in de werkomgeving van nu. De voordelen:

- **Snellere responstijd door de API-ondersteunende architectuur.**
- **Complete zichtbaarheid van e-mails, ook van interne e-mails.**
- **Meer contextuele informatie dankzij een gegroepeerd overzicht.**
- **Tools voor het automatisch of handmatig afhandelen van bedreigingen.**

In 2021 gebruikt 70% van de bedrijven e-maildiensten in de cloud[1]

Organisaties verhogen de productiviteit van hun thuis- en flexwerkers dankzij het migreren van hun e-mailplatformen naar de cloud. Zeker nu thuiswerken de norm is, is dit zeer waardevol. Het biedt ook vele andere voordelen, zoals toegang tot geactualiseerde tools, verminderd onderhoud en snellere gebruikerstoegang tot nieuwe functies.

E-mail in de cloud biedt bedrijven talloze voordelen. Tegelijkertijd maakt het hen kwetsbaar voor aanvallen.

Hackers weten de kleinste openingen in de ICT-infrastructuur te vinden. De belangrijkste dreigingen voor e-mail zijn[1]:

Malware: in 2018 vonden 10,52 miljard malware-aanvallen plaats.

Phishing: in 2020 ging het in 27% van de datalekken om diefstal van inloggegevens.

Ransomware: voor 2021 wordt de totale schade geschat op $20 miljard.

Gehackte mailaccounts: de schade liep tussen 2016 en 2020 op naar $26 miljard.

Gehackte domeinen: 54% van legitieme domeinen worden misbruikt voor phishing-campagnes.

Migratie naar de cloud brengt nieuwe risico's

Bij het migreren van mailboxen naar de cloud moeten securitybeheerders van uw klanten zich bewust zijn van de toegenomen veiligheidsrisico's. Alleen dan kunnen zij voorkomen dat hun organisatie doelwit wordt van:

Onbekende en dynamische dreigingen
In cloudgebaseerde mailboxen verschuilen zich moeilijk detecteerbare dreigingen die makkelijk over het hoofd worden gezien. Om verspreiding van deze bedreigingen via e-mail te beperken, zijn snelle detectie en geautomatiseerde hersteltools cruciaal.

Doelgerichte aanvallen op het platform
Succesvolle phishing van inloggegevens via e-mail in de cloud geeft cybercriminelen toegang tot de volledige omgeving voor kantoorapplicaties. Ze kunnen zich dan voordoen als iemand binnen het bedrijf, of spearphishingaanvallen uitvoeren.

Geavanceerde aanvallen
Geavanceerde technieken, zoals ransomware en gerichte phishing, omzeilen de security die cloudgebaseerde e-mailplatformen standaard bieden.

Geen totaaloverzicht over de netwerkgrenzen
Eén succesvolle phishingpoging kan voldoende zijn om een account te kapen. Criminelen krijgen toegang tot de interne communicatie, waardoor ze de omgeving voor interne en zakelijke mail kunnen aanvallen.

TechData Advanced Solutions

Office 365 domineert in de cloud

cisco Partner
Distribution Partner

Office 365 is door de jaren uitgegroeid tot de meest gebruikte clouddienst voor bedrijven. Maar liefst 1 op de 5 werknemers van grote bedrijven zet Office 365 in[2].

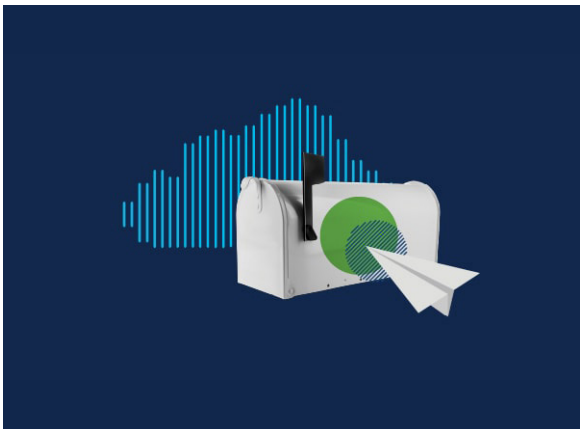
De software van grote leveranciers is altijd al doelwit geweest voor cybercriminelen. Nu medewerkers steeds vaker vanaf afstand werken, is Office 365 een nog aantrekkelijker doelwit. Onderzoek onder 27 miljoen gebruikers binnen 600 grote bedrijven laat zien dat 71% van de zakelijke gebruikers maandelijks te maken heeft met minstens een geslaagde aanval op een account[3].

Aanvallen met kwaadaardige e-mails zijn de grootste bedreiging voor Office 365. Maar liefst 71% van de gebruikers is ooit met malware geconfronteerd.[5] Phishingaanvallen komen op de tweede plaats, met 48% van de gebruikers.[5] 30% is doelwit geweest van een aanval met ransomware.[5] Maar liefst 80% van de organisaties zet extra security in om hun Office-365-omgeving te beschermen.[5]

Een gelaagde security-aanpak is cruciaal

E-mail is kwetsbaar voor geavanceerde aanvallen. Daarom adviseert Gartner bedrijven om hun mailboxen in de cloud extra te beschermen met gelaagde security en veelomvattende threat intelligence.

Om een gelaagde bescherming van het inkomende, uitgaande en interne e-mailverkeer te bieden, is Cisco Cloud Mailbox Defense gericht op de vier belangrijke onderdelen: voorspelling, preventie, detectie en respons.



5 manieren waarop Cisco Cloud Mailbox Defense de security van Office 365 verbetert in minder dan 5 minuten:

1. **Maakt inkomende, uitgaande en interne berichten zichtbaar.**
2. **De geavanceerde threat intelligence van Cisco Talos detecteert en blokkeert dreigingen direct.**
3. **Cisco AMP en Threat Grid bieden bescherming tegen geavanceerde aanvallen.**
4. **Snelle afhandeling van kwaadaardige e-mailcontent op basis van API's**
5. **Geïntegreerd dashboard met zoekfunctie, rapportage en het volgen van mogelijke incidenten.**

TechData
Advanced Solutions

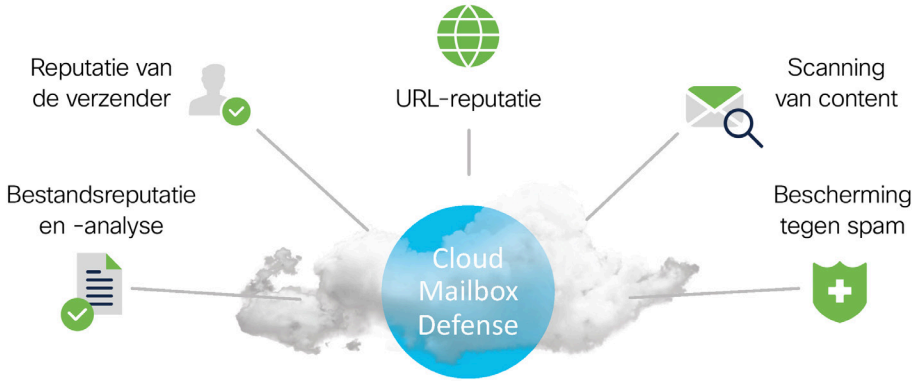
Cloud Mailbox Defense

Cisco Partner
Distribution Partner

Cisco Cloud Mailbox Defense brengt security dichter naar de mailbox dan ooit tevoren. De oplossing voorkomt phishing, spoofing, ransomware, gehackte e-mail en andere cyberdreigingen.

Cisco Cloud Mailbox Defense scant ieder component binnen ieder bericht - ook als deze intern is verstuurd - en detecteert dreigingen van binnenuit, netwerkinbraken en verspreiding van malware.

- **Bestandsreputatie- en analyse:** bijlagen worden gecontroleerd op kwaadaardige bestanden en niet-geregistreerde malware.
- **Reputatie van de verzender:** controle met behulp van cloud intelligence API's.
- **URL-reputatie:** controle van meegestuurde links op categorie en reputatie.
- **Scanning van content:** analyse van berichten om phishing en gekaapte accounts te detecteren.
- **Bescherming tegen spam:** detectie en verwijdering van spam.



Cisco Cloud Mailbox Defense zorgt voor het snel oplossen van bedreigingen - automatisch of handmatig. De oplossing maakt namelijk gebruik van de meest moderne en effectieve tools om strengere securityfuncties in te bedden in Office 365, zonder daarbij de regelmatige levering van berichten te onderbreken.

Cisco Talos: zichtbaarheid, intelligence en response
Een uitgebreide, accurate en proactieve aanpak van threat management voor het tegenhouden van kwaadaardige bijlages en URL's, spam en phishing.

Cisco AMP en Threat Grid: gedeelde intelligence voor integrale security
Bestandsreputatiescores, sandboxing en bestandsinspectie achteraf voor een continue analyse van mogelijke dreigingen. Zo kunnen gebruikers aanvallen blokkeren, verdachte bestanden volgen, en de omvang van een uitbraak beperken en snel herstellen.

Architectuur met API-ondersteuning: best-of-breed security
Cisco Cloud Mailbox Defense ondersteunt RESTful API's voor eenvoudige en flexibele integratie met andere securitytools. Dit leidt tot snellere detectie en herstel.

Gecentraliseerde gebruiksinterface: een uitgebreid overzicht van wat er gaande is.
De gecentraliseerde interface biedt volledig overzicht over de rapporten, configuratie en de tracking. Met gegroepeerde overzichten van het in- en uitgaande mailboxverkeer, met meer contextuele informatie.

TechData
Advanced Solutions

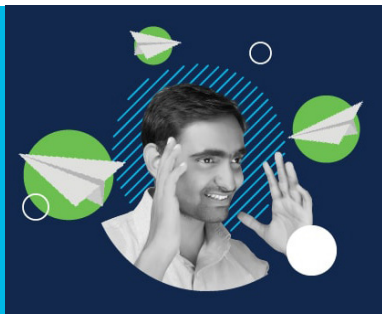
Geavanceerde threat intelligence van Cisco

Cisco Partner
Distribution Partner

Cisco Cloud Mailbox Defense vult de ingebouwde securitymogelijkheden van Office 365 aan met een extra beschermlaag voor e-mail. Deze blokkeert spam en geavanceerde dreigingen als ransomware, gekaapte zakelijke accounts en phishing.

De voordelen van Cisco Cloud Mailbox Defense:

- **Blokkeer meer aanvallen dankzij de geavanceerde threat intelligence van Cisco Talos.**
- **Snellere respons en integratie dankzij architectuur met API-ondersteuning.**
- **Bescherming tegen dreigingen van binnenuit.**
- **De volledige e-mailwisseling kan in een keer geanalyseerd worden met behulp van makkelijk toe te passen forensische tools.**
- **Bescherming tegen geavanceerde dreigingen met Cisco AMP en Threat Grid.**



3 redenen om te kiezen voor Cisco Cloud Mailbox Defense

1. Eenvoud

Cisco Cloud Mailbox Defense ziet iedere mail die wordt verzonden en ontvangen. Ook het verkeer tussen interne mailboxen is volledig zichtbaar. De zoekfunctie geeft alle informatie weer over afzonderlijke berichten en ziet direct welke mailboxen tijdens incidenten zijn besmet. En het verrijkt het onderzoek voor incident-response met analyses van mailwisselingen.

2. Zichtbaarheid

Cisco Cloud Mailbox Defense ziet iedere mail die wordt verzonden en ontvangen. Ook het verkeer tussen interne mailboxen is volledig zichtbaar. De zoekfunctie geeft alle informatie weer over afzonderlijke berichten en ziet direct welke mailboxen tijdens incidenten zijn besmet. En het verrijkt het onderzoek voor incident-response met analyses van mailwisselingen.

3. Controle

Doordat alles binnen Microsoft's cloud-omgeving blijft - ook eventuele bijlagen in e-mails - kunnen beheerders specifieke acties toepassen op berichten die zij via zoekacties hebben gevonden. Denk aan het verplaatsen van berichten of mappen binnen de mailbox van individuele gebruikers, of zelfs het verwijderen daarvan. Voorheen kostte dit erg veel tijd en was het noodzakelijk om hiervoor eerst speciale PowerShell-scripts te schrijven. Nu kan dit plaatsvinden via Microsofts' eigen native cloud API's.

Bescherm uw klanten in de cloud

De sleutel tot het beschermen van een organisatie tegen bedreigingen van binnen én van buiten: scan elke mail die wordt verstuurd of ontvangen en analyseer mailboxen continu.

Bescherm al uw klanten in de cloud. Neem contact op met uw Tech Data-accountmanager om meer te weten te komen over Cloud Mailbox Defense van Cisco.

[1] Bron: "Introducing Cloud Mailbox Defense", Gartner
[2] Bron: https://www.skyhighnetworks.com/cloud-security-blog/7-charts-reveal-the-meteoric-rise-of-office-365/
[3] Bron: https://securityboulevard.com/2019/05/6-security-concerns-with-office-365-2/
[4] Bron: https://www.redscan.com/news/securing-office-365/
[5] Bron: https://www.techrepublic.com/article/40-of-enterprises-experienced-office-365-credential-theft-report-finds/

TechData
Advanced Solutions