

Snel naar: Chinese overheid > Maakt het product contact met servers in China? >
Microsoft Teams bewaakt de security > Vragen over netwerk, software en
encryptie >



Yealink & de Chinese overheid

► Hoe weet ik zeker of mijn Yealink hardware veilig is?

Onafhankelijke instituten zoals bijv. NetSPI, Spirent en Miercom hebben als experts op gebied van veiligheid, de producten en oplossingen van Yealink uitgebreid getest en komen tot de conclusie dat er "geen kwetsbaarheden" te vinden zijn.

► Bestaat er een nieuwe regel bij de Chinese overheid die in China opererend techbedrijven verplicht om kwetsbaarheden in hun software binnen 48 uur na ontdekking te melden?

De juridische afdeling van Yealink heeft dit gecontroleerd. Zij geven aan dat deze wetgeving in China niet bekend is, wat betekent dat zij hier natuurlijk niet aan hoeven te voldoen. Yealink hoeft niet aan deze wet te voldoen, omdat zij een beursgenoteerd bedrijf zijn en volledig onafhankelijk zijn hierdoor, dit kan je [hier](https://www.reuters.com/markets/companies/300628.SZ/) (<https://www.reuters.com/markets/companies/300628.SZ/>) terugvinden.

► Hoe veilig is het om de producten van Yealink te gebruiken?

Op basis van positieve rapporten van bijv. experts als NetSPI, Spirent, Miercom zijn de producten veilig bevonden. Als organisatie heeft Yealink onafhankelijke tests ondergaan en is gecertificeerd met ISO 27001 en SOC 1, 2, 3. Dit zijn harde feiten waarmee de conclusie "veilig" getrokken kan worden. Raadpleeg voor de certificeringen: <https://www.yealink.com/en/trust-center/resources>

► Is Yealink verplicht om gegevens af te dragen aan de Chinese overheid?

De Juridische afdeling van Yealink onderzocht of Yealink moet voldoen aan deze Chinese compliance-regels. En hieruit is gekomen dat zij niet op de hoogte van dergelijke wetgeving of regels vanuit de Chinese overheid. Hierbij de reactie van Yealink: "As a Chinese company, Yealink has never been obligated by the government to hand over user data, and there is no law mandating such a requirement."



Maakt het product contact met de servers van Yealink?

► **Maakt mijn VoIP-telefoon contact met servers van de fabrikant?**

Jouw bureautelefoon maakt alleen verbinding met de Yealink RPS-server, wanneer het gaat om een nieuw product wat net uit de verpakking komt en nog de fabrieksinstellingen heeft. Deze server staat niet in China, maar bij AWS in Frankfurt en Azure in Noord-Amerika. De RPS server stuurt het product door (Redirect) naar de bestemming waar het product zijn instelling kan ophalen (de provider).

De instellingen voor bijvoorbeeld, je telefoonnummer, worden opgeslagen op de server van de telefonieprovider. Zodra het product de instellingen heeft ontvangen van het telefonieplatform, wordt de verbinding met de RPS uitgeschakeld. Er is dan geen enkele verbinding meer met de RPS-server.

De RPS-server (welke zich bevindt in Frankfurt en Noord-Amerika) zorgt voor een eenvoudige installatie van de producten. De enige data die wordt overgedragen, is de locatie (URL) waar de instellingen kunnen worden opgehaald. Er worden geen instellingen geladen door de RPS in het product.

► **Checken de VoIP-Telefoons geregeld (en automatisch) of er nieuwe informatie in ‘hun’ provisioningdocument staat?**

Dit is een direct proces tussen het product en het telefonie-platform, zonder tussenkomst van een fabrikant server.

► **Wordt alle informatie zoals het serienummer en je gebruiksgegevens van je VoIP-Telefoons ontsloten via de servers van de fabrikant?**

De genoemde informatie bevinden zich op telefoonproviderplatforms die volledig onafhankelijk zijn van de fabrikant.

► **Zoekt een Yealink meetingbar zijn firmware-updates contact met de servers van Yealink?**

De Yealink meetingbars zijn gecertificeerd door Microsoft Teams en maken gebruik van firmware updates via de Microsoft servers.

Om de installatie te vereenvoudigen, maakt het product (alleen wanneer het nieuw uit de verpakking komt met fabrieksinstelling) verbinding met de Yealink RPS server. Deze server is niet gevestigd in China maar bevindt zich bij AWS in Frankfurt en Azure in Noord-Amerika. De server stuurt het product door (Redirect) naar de juiste bestemming om zijn instellingen op te halen.

De overgedragen data bevat enkel de locatie (URL) waar de instellingen kunnen worden opgehaald. De RPS-server laadt geen instellingen in het product. Zodra het product zijn instellingen heeft, wordt het contact met de RPS-server uitgeschakeld.

Het verdere management van het product qua instellingen en firmware verloopt via het Microsoft Teams-platform en de Microsoft servers. Er is dan dus geen verdere verbinding met de RPS-server.

► **Kan de Yealink RPS server instellingen of firmware in het product laden?**

De Yealink RPS server (welke zich bevindt in Frankfurt en Noord-Amerika) doet alleen een Redirect en kan geen instellingen of firmware in het product laden. De firmware en instellingen worden beheerd door Microsoft.



Microsoft Teams

► Heeft Microsoft Teams strikte specificaties opgesteld voor de certificering van videoconferentie hardware?

Ja, voor de Teams Rooms-oplossingen heeft Microsoft strikte specificaties opgesteld voor certificering. Deze oplossingen worden gebruikt om Teams-vergaderingen in vergaderruimtes te faciliteren.

Yealink voldoet met al haar Microsoft Teams producten aan deze certificering van Microsoft omdat je alleen dan door Microsoft het stempel "certified" kan krijgen en mag voeren.

De vereisten voor certificering omvatten:

- Hardware beveiliging
- Softwarebeveiliging
- Accountbeveiliging
- Netwerkbeveiliging.

Klik hier (<https://learn.microsoft.com/en-us/microsoftteams/rooms/security?tabs=Windows>) voor de volledige Microsoft security specificaties.



Software, netwerkpoorten en encryptie

► Staat de Yealink sleutel (encryptie) op en bloot gepubliceerd in de software die voor provisioning wordt gebruikt?

Het is aan de provider om te beslissen hoe het telefonieplatform is ingericht en of de instellingen (in het artikel proviosingsdocument genoemd) versleuteld worden, of dat er andere maatregelen worden genomen om de inhoud niet leesbaar te maken.

Uit ervaring blijkt dat de encryptietool van Yealink helemaal niet gebruikt wordt door professionals, zoals Carriers, in de telecommarkt.

In de VoIP-industrie werken professionals die de platforms en beveiliging beheren. Ze weten dat standaard pin- of defaults codes niet gebruikt moeten worden, net zoals bij het wijzigen van de pincode van een smartphone. De professionele providers (meer dan 99% van de hosted voip providers) gebruikt deze methode niet gebruiken.

► Waarom staat bij VoIP-telefoons (bureautelefoons) standaard de netwerkpoort open?

De open poort, 5060, is essentieel voor de werking van de telefoon en wordt gebruikt als standaardpoort voor VoIP-communicatie.

Het gebruik van deze poort is niet uniek voor Yealink-producten, maar wordt door alle fabrikanten in de VoIP-industrie gebruikt. Het gedrag van andere fabrikanten is

hetzelfde als dat van Yealink.

Als de provider ervoor kiest om de communicatie naar de telefoon via een andere poort te leiden, kan deze standaardpoort worden gesloten met de juiste instellingen.

► **Waarom bevat de Yealink software open source software?**

Yealink heeft haar eigen software heeft geschreven voor de open source modules. Deze software zorgt ervoor dat de veiligheid van het complete product gegarandeerd is.

► **Waar kan ik zien welke kwetsbaarheden er gevonden zijn in de beveiliging van Yealink producten?**

Elke softwarefabrikant, heeft te maken met mogelijke verbeteringen in de software.

Wij nodigen je uit om op <https://cvedetails.com> te kijken en zelf een oordeel te vormen over Yealink in vergelijking met andere fabrikanten.

Yealink scoort positief op cvedetails en blijft voortdurend investeren in het verbeteren van hun producten en het vermijden van beveiligingsproblemen. Ze werken samen met experts van Netspi, Spirent en Miercom voor gedetailleerde onafhankelijke controles.

► **Waarom gebruiken veel professionals pentesten om hardware en software op security te testen?**

Dit is de enige juiste manier om producten en fabrikanten onafhankelijk en grondig te beoordelen middels uitgebreide (pen)testen.

Zoals meerdere grote telefonieproviders over de hele wereld aangeven wordt de veiligheid beoordeelt door onafhankelijk en feitelijk te testen, in de telecommarkt worden hiervoor pen testen gebruikt.

Yealink & Lydis staat

Heeft u meer vragen omtrent de security?

Vul dan het onderstaande contactformulier in en onze experts nemen zo spoedig mogelijk contact met je op

Bedrijf (optioneel)

Naam

tussenv.

Achternaam

E-mailadres

Telefoonnummer (optioneel)

Opmerking

VERSTUUR

LYDIS

Lydis B.V.

Jool-Hulstraat 16

1327 HA Almere

+31 (0)36 20 20 120 (tel:+31 36 20 20 120)

info@lydis.com (mailto:info@lydis.com)

LINKS

Contact (/contact)

Klantenservice (<https://www.lydis.nl/klantenservice>)

Vacatures (/over-ons/vacatures)

Algemene voorwaarden (/algemene-voorwaarden)

Privacy & Cookie verklaring (/privacy-en-cookie-verklaring)

Routebeschrijving (/contact)

RESELLERS

Registreren (/registreren)

Inloggen (/login)

Reseller worden? (/reseller-wordsen)

Zoek een Reseller (/contact/zoek-reseller)

Lydis Update (<https://www.lydis.nl/over-ons/lydis-update>)

Webinars (<https://www.lydis.nl/webinars-lydis>)

Acties (<https://www.lydis.nl/over-ons/actie>)

NIEUWSBRIEF

e-mailadres

AANMELDEN

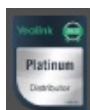
VOLG ONS

(<https://www.linkedin.com>

 /company

/lydis- (<https://www.youtube.com>


b-v-)  /user/lydisvideo)



(/merken/yealink)



(<https://www.stibat.nl/>)

spectra.link  (/merken/spectralink)
partne elite



([https://itunes.apple.com/nl/app/lydis-ip-communicatie-specialist
/id1007547625?mt=8](https://itunes.apple.com/nl/app/lydis-ip-communicatie-specialist/id1007547625?mt=8))



(<https://play.google.com/store/apps/details?id=com.Pangaea.lydis>)

© Lydis 2024. All rights reserved.

(<https://pangaea.nl>)