

DIGITAAL VERTROUWEN: DE STAND VAN DIGITAAL VERTROUWEN VOOR DE ECHTE WERELD IN 2024

≡

KOPLOPERS



ACHTERBLIJVERS

PKI

COMPLIANCE

UITVAL

XX
BEVEILIGINGSWAARSCHUWINGEN

IoT

BEST
PRACTICES

digicert®

DIGITAAL VERTROUWEN: DE STAND VAN ZAKEN IN 2024

Het eerste onderzoek naar de stand van zaken op het gebied van digitaal vertrouwen werd in 2022 door DigiCert gepubliceerd. Nu de digitale transformatie zich in vrijwel iedere bedrijfstak voltrekt, is digitaal vertrouwen cruciaal. Dat zorgt ervoor dat we zeker weten dat de mensen en apparaten waarmee we verbinding maken legitiem zijn, en dat onze online interacties zijn beveiligd.

Volgens Jennifer Glenn, Research Director van IDC, is digitaal vertrouwen de basis voor het beveiligen van de online wereld. Het is bovendien onmisbaar voor organisaties die hun klanten, medewerkers en partners het vertrouwen willen bieden dat online bedrijfsprocessen en interacties veilig zijn.

DigiCert is de wereldwijd toonaangevende leverancier van digitaal vertrouwen, die zowel individuen als bedrijven de zekerheid biedt dat hun online aanwezigheid is beveiligd. Om onze klanten optimaal van dienst te kunnen zijn, willen we een goed beeld hebben van hoe bedrijven overal ter wereld digitaal vertrouwen zien, en hoever ze zijn gevorderd met hun inspanningen voor het wekken, beheren en uitbreiden van digitaal vertrouwen.

Bouwen op inzicht in vertrouwen

Uit ons eerste onderzoek bleek dat 100% van de bedrijven digitaal vertrouwen belangrijk vond. En vrijwel allemaal (99%) dachten ze dat als ze het vertrouwen van hun klanten zouden kwijtraken, die klanten mogelijk zouden overstappen naar de concurrent. De meeste consumenten dachten er hetzelfde over: twee derde van hen (68%) zei dat digitaal vertrouwen belangrijk is.

In deze nieuwste uitgave gaan we kijken naar wat er sindsdien is veranderd. In Digitaal vertrouwen: de stand van zaken in 2024 bekijken we specifieke functies en workflows van digitaal vertrouwen om inzicht te krijgen in hoe goed bedrijven het doen en hoe ze hun inspanningen op het gebied van digitaal vertrouwen kunnen blijven optimaliseren.

Werkwijze

Het in Dalles gevestigde Eleven Research heeft het onderzoek Digitaal vertrouwen: de stand van zaken in 2024 in het vierde kwartaal van 2023 uitgevoerd. Dit gebeurde door middel van een telefonische enquête onder 300 senior besluitvormers in kleine tot grote ondernemingen in Noord-Amerika, EMEA en APJ.

Er werd gesproken met deelnemers uit allerlei bedrijfstakken waaronder technologie, productie en financiële dienstverlening. De omvang van de bedrijven liep uiteen van 1.000 tot meer dan 10.000 werknemers.

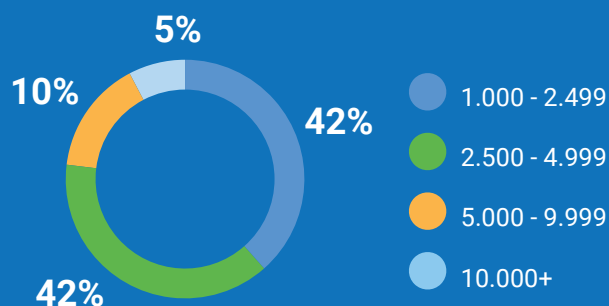
Om een goed beeld te krijgen van specifieke inspanningen op het gebied van digitaal vertrouwen, richtte Eleven Research zich op de verantwoordelijken voor vier afzonderlijke gebieden:

- Bedrijfsvoering: beveiligen van communicatie, gegevens en toegang voor medewerkers, applicaties en cloud.
- IoT en verbonden apparaten: beschermen van smart-apparaten en -services zoals glucosemonitors.
- Software: beschermen van software en apps tegen manipulatie en aanvallen op de supplychain.
- eSignature: waarborgen van de authenticiteit en integriteit van documenten en inhoud.

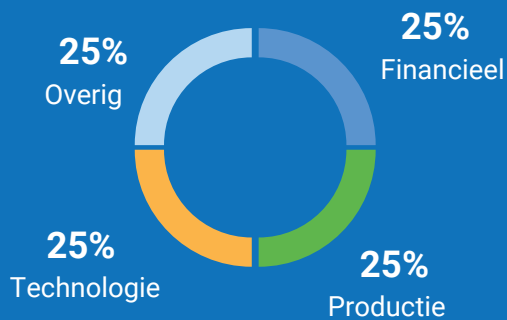
LOCATIE



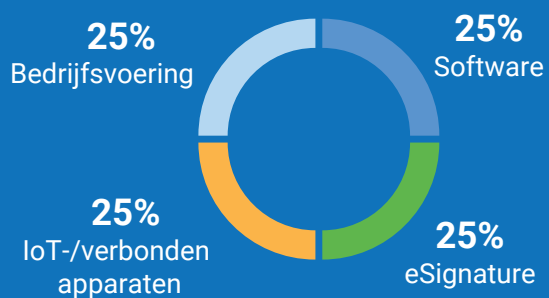
BEDRIJFSOMVANG



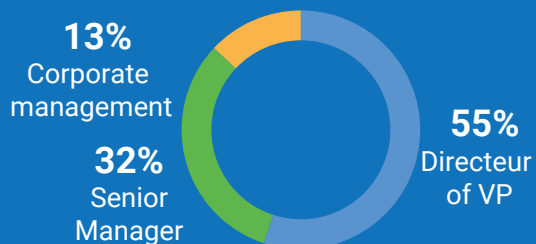
BEDRIJFSTAK



ONDERWERPEN



SENIORITEIT



GROTE ONDERNEMINGEN BLIJVEN GEFOCUST OP DIGITAAL VERTROUWEN

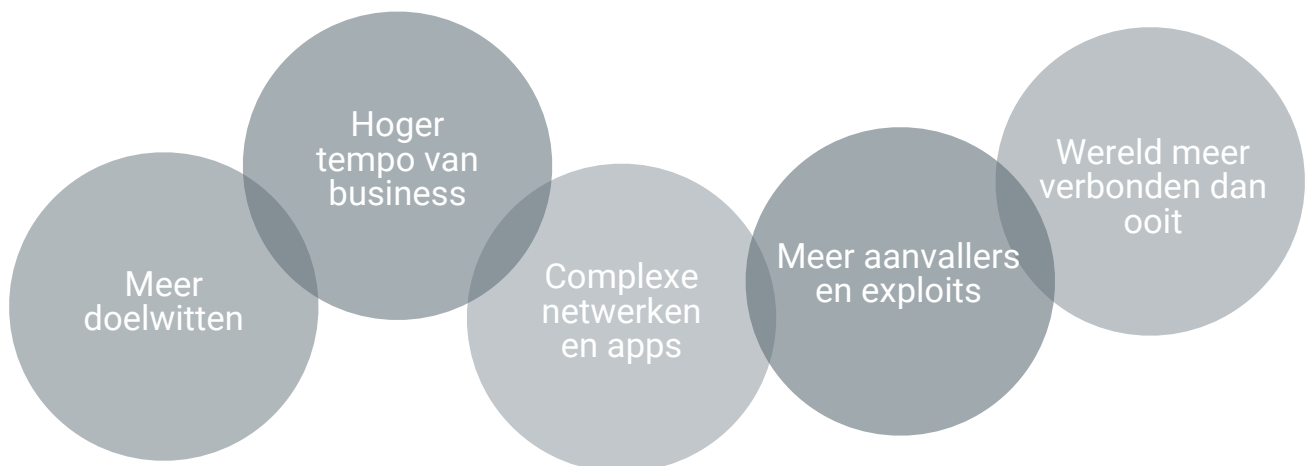
Gezien de overweldigende respons bij het onderzoek van vorig jaar, is het geen verrassing dat de grote ondernemingen zich nog steeds intensief bezighouden met digitaal vertrouwen. De drie belangrijkste drijfveren hiervoor zijn:

- Er zijn nu meer externe medewerkers dan ooit tevoren.
- Ook zijn er meer netwerken (zoals aan de edge en om verbinding te maken met partners en klanten).
- Maar het belangrijkste is dat klanten digitaal vertrouwen verwachten van bedrijven.

DRIE BELANGRIJKSTE REDENEN



OVERIGE REDENEN

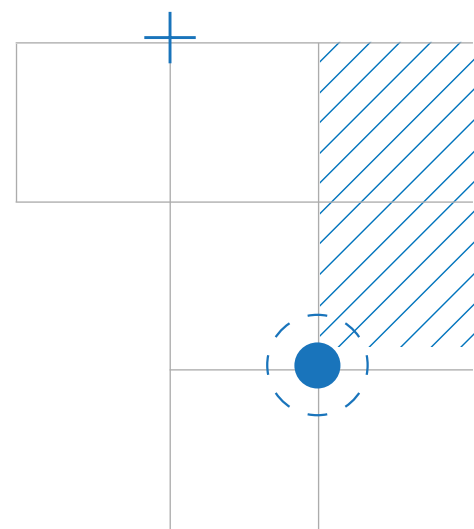


Die bedrijven komen er echter steeds meer achter dat het niet gemakkelijk is digitaal vertrouwen te wekken, monitoren en beheren. Ze worstelen met vijf grote uitdagingen:

- **Gebrek aan expertise bij medewerkers.** Digitaal vertrouwen is een relatief nieuwe discipline en niet iedereen weet hoe het op een gecentraliseerde manier kan worden geïmplementeerd. Daarnaast worden veel interne PKI's, die al tien jaar geleden werden opgezet, nu beschouwd als kwetsbaar en gevoelig voor uitval. Daarmee kunnen medewerkers dus niet de noodzakelijke kennis en ervaring opdoen.
- **De toenemende complexiteit van netwerken en applicaties.** De technologie binnen bedrijven is een stuk ingewikkelder geworden. Op het gebied van netwerken zijn veel ondernemingen afgestapt van de traditionele manier van werken met een datacenter, externe vestigingen en de cloud. De hedendaagse netwerken omvatten edge-netwerken, duizenden externe medewerkers en meerdere clouds.

Daarnaast zijn de omvangrijke en logge applicaties vervangen door in hoge mate gedistribueerde microservice-architecturen, waarbij de onderneming geen rechtstreekse controle heeft over veel van die services. In zo'n complexe omgeving is het extreem moeilijk om digitaal vertrouwen te wekken.

- **De enorme omvang van wat er moet worden beveiligd.** Met het voortschrijden van de digitale transformatie zijn steeds meer digitale middelen missiekritiek geworden. Daarmee is ook de omvang van wat er beveiligd moet worden exponentieel gegroeid.
- **Gebrek aan ondersteuning door het management.** Omdat de economie er minder rooskleurig voorstaat na jaren van pandemie en inflatie, heeft de top van het bedrijfsleven moeilijke beslissingen moeten nemen. Alleen al in 2023 zijn er in de Amerikaanse technologiesector ruim 240.000 mensen ontslagen.¹ Onder die omstandigheden is het niet verrassend dat het management zich wat minder bezighoudt met digitaal vertrouwen.
- Ten slotte is ook de **snelle uitbreiding van cryptografische middelen moeilijk te beheren en bovendien tijdrovend.** Digitale certificaten blijven essentieel voor alle inspanningen op het gebied van vertrouwen, op zowel openbaar als persoonlijk vlak. Maar het beheer van de enorme hoeveelheid certificaten binnen grote ondernemingen is geen eenvoudige kwestie.



¹ Tech Crunch

GEBOEKTE VOORTGANG OP HET GEBIED VAN DIGITAAL VERTROUWEN

Hoe goed presteren bedrijven met betrekking tot het implementeren van digitaal vertrouwen? Het lange antwoord op deze vraag is uitgebreid, ingewikkeld en zit vol met nuances. De korte versie is: 'goed, maar het kan beter'.

Hun welslagen is afhankelijk van het gebied waarop ze zich richten. We hebben vier specifieke gebieden van digitaal vertrouwen onderzocht om te zien hoe de bedrijven presteren:

- Bedrijfsvoering
- IoT-/verbonden apparaten
- Software
- eSignature

Vertrouwen in bedrijven

Digitaal vertrouwen binnen grote ondernemingen wordt meestal beheerd door de IT-afdeling. De meest voorkomende typen digitaal vertrouwen die daar worden beheerd zijn:

- Certificaatbeheer
- Identiteits- en toegangsbeheer
- E-mailbeveiliging
- Eindpuntbeveiliging

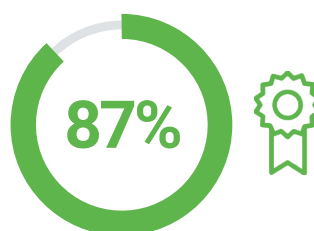
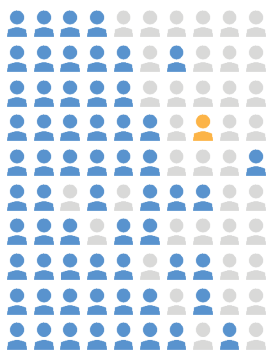
Zelfs digitaal vertrouwen binnen grote ondernemingen – waar we de grootste vooruitgang hadden verwacht – staat nog niet eens in de kinderschoenen. Slechts een enkele leidinggevende (1 op de 100) zegt dat hun inspanningen op het gebied van digitaal vertrouwen 'heel vergevorderd' zijn. Ook geeft 87% aan dat hun inspanningen versnipperd zijn.

Digitale certificaten bieden een mechanisme voor het authenticeren en beveiligen van de communicatie van gebruikers en apparaten binnen een bedrijf, zoals webservern en smartphones. En naarmate de netwerken en gebruiksscenario's groter en complexer worden, hebben ze een snel stijgend aantal certificaten nodig.

In ongeveer de helft (52%) van de ondernemingen worden certificaten beheerd door de IT-afdeling, bij een derde (37%) gebeurt het buiten de IT-afdeling en bij één op de negen bedrijven (11%) worden ze helemaal niet beheerd.

Daarbij moet worden opgemerkt dat er in de meeste ondernemingen maximaal vijf afdelingen zijn die certificaten uitgeven, maar de meeste zijn van mening dat meer afdelingen dat zouden moeten doen.

Slechts **1 op de 100** zegt dat ze zeer vergevorderd zijn met digitaal vertrouwen.

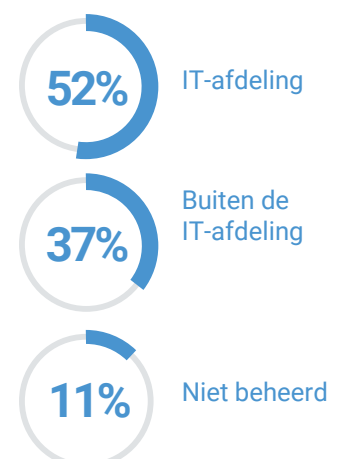


zegt dat hun inspanningen versnipperd zijn

De meeste bedrijven hebben maximaal 5 afdelingen die certificaten uitgeven

De meeste zeggen dat meer afdelingen certificaten zouden moeten uitgeven

Hier worden certificaten beheerd



Vertrouwen in bedrijven

Hoe verlopen de inspanningen op het gebied van digitaal vertrouwen? Niet zo goed als zou moeten, zo blijkt. De deelnemers ondervonden de volgende problemen met betrekking tot digitaal vertrouwen:

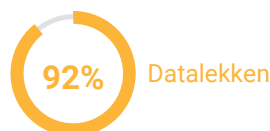
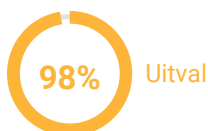
- **Bij bijna iedereen (98%)** zijn er ten minste een paar gevallen van uitval geweest.
- **Bij de meeste (92%)** zijn er datalekken geweest.
- En bij **een behoorlijk aantal (74%)** kregen ze te maken met complianceproblemen.

We hebben nog wat doorgevraagd om hun flexibiliteit op het gebied van digitaal vertrouwen te meten:

- **Geen van de bedrijven** kan zeer snel op uitval reageren.
- **Bijna geen enkel bedrijf (1%)** kan zeer snel reageren op beveiligingsincidenten.
- **Slechts weinig (5%)** kunnen zeer snel reageren op veranderingen in normen voor certificaten.
- **De meeste (61%)** zijn onvoldoende voorbereid op de post-quantumwereld en denken dat ze daarvoor nog drie jaar nodig hebben.

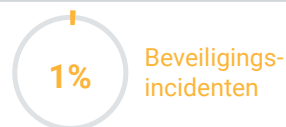
Ondanks deze moeilijkheden zeggen de meeste leidinggevenden op het gebied van digitaal vertrouwen dat hun inspanningen op hoog niveau bijdragen aan het bedrijf, bijvoorbeeld met betrekking tot digitale innovatie, merkvertrouwen en winstgevendheid.

Problemen met betrekking tot digitaal vertrouwen



Slechts weinig bedrijven kunnen zeer snel reageren op

GEEN Uitval

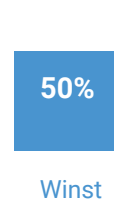
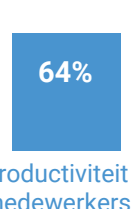
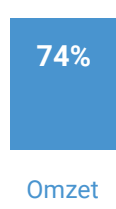
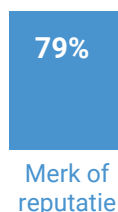


Gebrek aan voorbereiding op quantumcomputers:



De meeste bedrijven schatten 3 jaar nodig te hebben

Maar vertrouwen in bedrijven komt in het algemeen ten goede aan de hele organisatie:



Vertrouwen in IoT- en verbonden apparaten

Hierbij hebben we ons gericht op bedrijven die IoT-apparaten of verbonden apparaten produceren en verkopen aan klanten; dit zijn apparaten zoals fabriekssensoren, sporthorloges en thermostaten voor woonhuizen. We spraken met mensen binnen de organisatie die verantwoordelijk zijn voor bijvoorbeeld:

- Werken aan authenticatiemaatregelen voor IoT-apparaten en verbonden apparaten
- Mogelijk maken van versleuteling op IoT-/verbonden apparaten
- Ondertekenen van software- of firmware-updates voor IoT-/verbonden apparaten
- Gebruiken van cryptografie ter bescherming van IoT-/verbonden apparaten

Ook op dit gebied is de uitkomst die wordt gemeld 'goed, maar het kan beter'. Slechts een op de zeven zegt dat ze zeer vergevorderd zijn. De meeste gaven aan dat ze 'redelijk' vergevorderd waren.

Een verbazingwekkende **87%** verzendt persoonsgegevens van IoT-/verbonden apparaten via niet-versleutelde kanalen.

De meeste bedrijven (88%) hebben een leidinggevende speciaal voor productbeveiliging. Allemaal gebruiken ze digitale certificaten voor het identificeren van geïnstalleerde apparaten en voor sterke authenticatie van gebruikers.

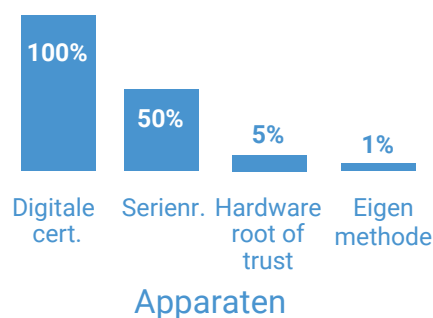
Slechts **1 op de 7** zegt dat ze zeer vergevorderd zijn met digitaal vertrouwen



De meeste zeggen 'redelijk' gevorderd te zijn.



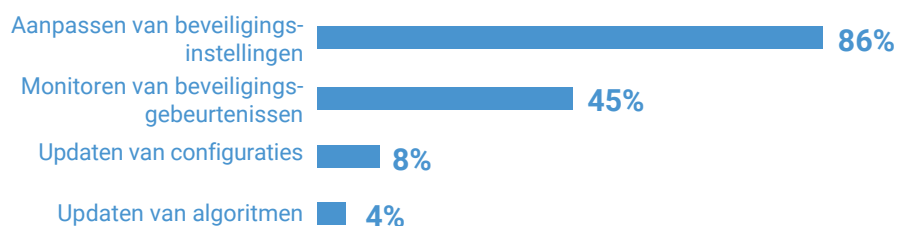
Zo identificeren ze hun geïnstalleerde apparaten en gebruikers ter plaatse:



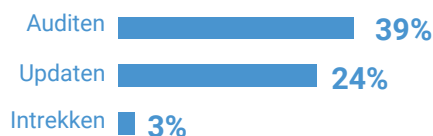
We vroegen de deelnemers om hun capaciteiten op het gebied van IoT-/verbonden apparaten te waarderen. Wat betreft het beheer van geïnstalleerde apparaten liepen de scores uiteen: ze scoren goed op het beheren van beveiligingsinstellingen en voldoende op het monitoren van gebeurtenissen, maar slecht op het updaten van apparaten.

Ook het beheren van apparaatidentiteiten, met name het intrekken daarvan, gaat nog niet al te best. Een lichtpuntje is dat het beveiligen van software goed gaat, maar daar staat tegenover dat het leveren van software-updates te langzaam gaat.

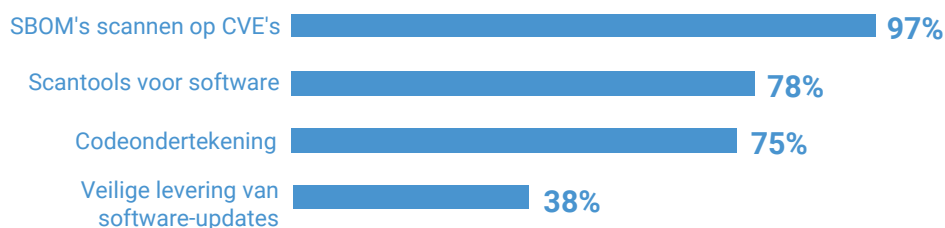
Capaciteiten van geïnstalleerde apparaten: Zeer goed in staat tot...



Beheer van apparaatidentiteiten:



Zo beveiligen bedrijven hun software- en firmware-updates:



Vertrouwen in IoT- en verbonden apparaten: de resultaten

Ondanks deze capaciteiten (of vanwege het gebrek daaraan) ondervonden de producenten van IoT-/verbonden apparaten de volgende problemen:

- **Bij de meeste (93%)** zijn er datalekken geweest. Het merendeel hiervan kon gebeuren vanwege een eenvoudige backdoor in het netwerk.
- **De meeste (93%)** kregen te maken met uitval.
- En samenhangend met ons eerste punt: bij **84%** was er ingebroken door criminelen.

De activiteiten op het gebied van vertrouwen in IoT-/verbonden apparaten boden ook voordelen:

- **86%** zegt dat ze hebben geholpen bij het binnenhalen van klanten
- **82%** zegt dat ze hebben bijgedragen aan digitale innovatie

Desondanks is het duidelijk dat de producenten van IoT- en verbonden apparaten hun inspanningen op het gebied van digitaal vertrouwen moeten opvoeren.

Problemen met betrekking tot digitaal vertrouwen



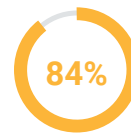
93%

Datalekken



93%

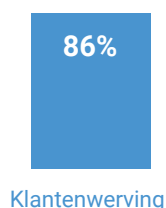
Uitval



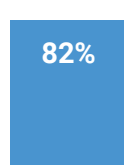
84%

Inbraken door kwaadwillenden

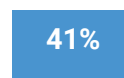
Maar vertrouwen in IoT-/verbonden apparaten komt in het algemeen ten goede aan de hele organisatie:



Klantenwerving



Digitale innovatie



Productiviteit medewerkers



Merk of reputatie

Vertrouwen in software

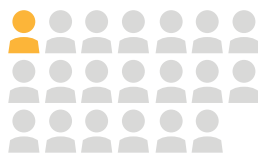
Vertrouwen in software moet ervoor zorgen dat klanten vertrouwen hebben in de software die ze kopen (of krijgen) van bedrijven. Ook hier gaf het onderzoek aan: 'goed, maar kan beter'. Slechts 1 op de 20 (5%) zegt dat ze zeer vergevorderd zijn met hun inspanningen op het gebied van vertrouwen in software. Ook zit er een verschil in welke code bedrijven ondertekenen:

- **Bijna allemaal (99%)** ondertekenen ze softwarebroncode
- **85%** ondertekent binaire softwarebestanden
- **62%** ondertekent buildscripts en infrastructuurconfiguraties

- **33%** maakt gebruik van containers en serverloze omgevingen
- **De meeste (67%)** bewaren persoonlijke sleutels voor codeondertekening in apparaten die voldoen aan FIPS-140-2

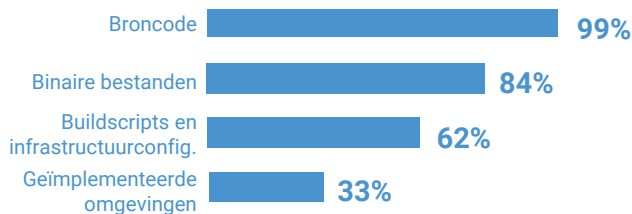
Geen van de ondervraagde ondernemingen zei er zeer snel achter te kunnen komen welke applicaties er allemaal met een specifieke persoonlijke sleutel zijn ondertekend, in het geval dat die sleutel in verkeerde handen zou zijn gevallen.

Slechts **1 op de 20** zegt dat ze zeer vergevorderd zijn met digitaal vertrouwen.

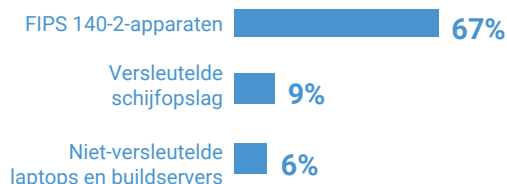


De meeste zeggen 'redelijk' gevorderd te zijn.

Welke code ondertekenen bedrijven:



Waarop bewaren bedrijven hun persoonlijke sleutels voor codeondertekening:



Als een persoonlijke sleutel voor codeondertekening is gecompromitteerd, kan **GEEN VAN DE BEDRIJVEN** snel achterhalen welke applicaties ermee zijn ondertekend.



Bijna alle bedrijven genereren standaard een SBOM (Software Bill of Materials) voor hun software.



Bijna alle bedrijven stellen eisen met betrekking tot risico's, beveiliging en regelgeving aan software van derden.

Vertrouwen in software: de resultaten

Hoe doen bedrijven het op het gebied van softwarecompliance? Slechts 1 op de 8 doet het zeer goed. Er worden ook veel problemen gemeld met betrekking tot vertrouwen in software:

- **86%** had te maken gehad met datalekken
- **80%** had te maken gehad met een inbraak in de build-infrastructuur voor software
- **79%** zei dat software niet meer werkte vanwege verlopen certificaten voor codeondertekening
- **78%** had software geleverd die malware en andere kwetsbaarheden bevatte
- **75%** had release-deadlines gemist vanwege problemen met codeondertekening of gevonden malware

Klanten zijn afhankelijk van de integriteit van de software die bedrijven leveren, maar het beveiligen van alle sleutels die nodig zijn voor codeondertekening is een lastige klus.

Slechts enkele bedrijven zeggen dat ze makkelijk een lijst kunnen genereren van alle softwareonderdelen die ze produceren.

Desondanks zeggen de verantwoordelijke leidinggevendenden dat hun inspanningen op twee manieren ten goede komen aan het bedrijf: digitale innovatie en medewerkersproductiviteit.



doet het zeer goed op het gebied van compliance voor software.



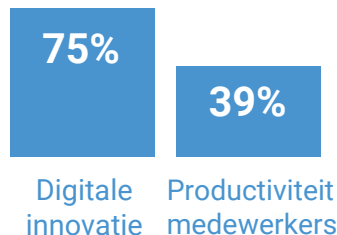
doet het redelijk goed.

Problemen met betrekking tot digitaal vertrouwen



zegt dat het zeer gemakkelijk is een lijst te genereren van software-onderdelen en de configuratie daarvan in hun software

Maar vertrouwen in IoT-/verbonden apparaten komt in het algemeen ten goede aan de hele organisatie:



Vertrouwen in eSignatures

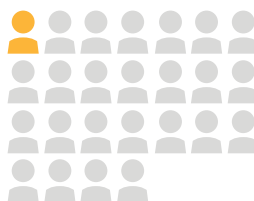
Documentondertekeningscertificaten stellen personen, teams en organisaties in staat een digitale handtekening toe te voegen aan documenten in allerlei bestandsformaten. Daarmee bewijzen ze dat zij de eigenaar ervan zijn en zorgen ze ervoor dat documenten niet worden gewijzigd en vertrouwelijke informatie veilig blijft.

We vroegen de deelnemers om aan te geven hoe vergevorderd ze zijn op het gebied van vertrouwen in eSignature. Slechts 1 op de 25 (4%) van hen geeft aan dat ze zeer vergevorderd zijn op dat gebied – dat is de laagste score voor alle vier de onderzoeksgebieden. Een van de kenmerken van dit segment is dat eSignatures, of elektronische

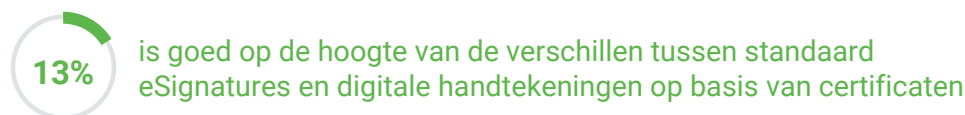
handtekeningen, worden gezet door zakenmensen in plaats van IT-medewerkers (juridische zaken, HR, inkoop enzovoort), en slechts 1 op de 8 weet wat de verschillen zijn tussen eenvoudige elektronische handtekeningen en eSignatures op basis van een certificaat.

- **Ongeveer de helft (48%)** gebruikt elektronische zegels voor documenten (juridisch, verkoop, inkoop enzovoort).
- **De meeste bedrijven (86%)** gebruiken digitale handtekeningen met certificaten die zijn uitgegeven door vertrouwde derde partijen, om ondertekenaars te verifiëren.

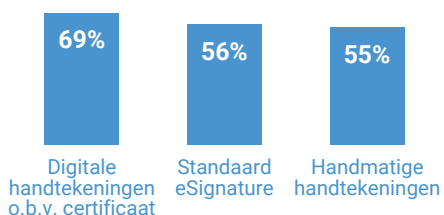
Slechts **1 op de 25** zegt dat ze zeer vergevorderd zijn met digitaal vertrouwen.



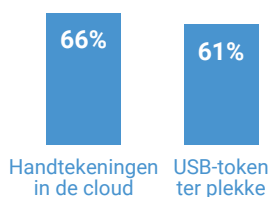
De meeste zeggen 'redelijk gevorderd te zijn'.



Type handtekening dat wordt gebruikt:



Type handtekeningen van gebruikers van eSignatures:



gebruikt digitale handtekeningen met certificaten die zijn uitgegeven door vertrouwde derde partijen, om ondertekenaars te verifiëren.



De helft gebruikt elektronische zegels voor documenten.

Meest voorkomende scenario:



Vertrouwen in eSignatures: de resultaten

Deze groep ondervond het grootste aantal problemen als gevolg van een gebrek aan vertrouwen:

- **100%** zei dat kwaadwillenden hadden doen voorkomen alsof een bepaald document afkomstig was van hun organisatie.
- **100%** had problemen ondervonden met contractuele processen op papier.
- **100%** had problemen ondervonden met diefstal of nabootsing van identiteit.
- Bijna allemaal (**99%**) hadden ze juridische problemen gehad met internationale contracten.

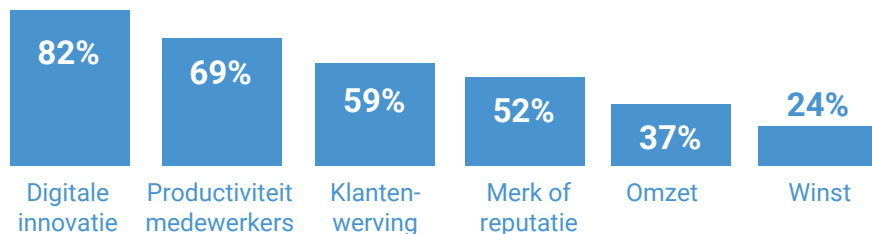
- **96%** ondervond complianceproblemen.
- **87%** vertelde dat organisaties ontkenden dat een overeenkomst was ondertekend.

Ondanks deze problemen zeggen ze dat hun inspanningen ten goede waren gekomen aan de digitale innovatie, productiviteit, klantenbinding en andere zaken binnen het bedrijf.

Problemen met betrekking tot digitaal vertrouwen



Maar vertrouwen in bedrijven komt in het algemeen ten goede aan de hele organisatie:



WAT WE KUNNEN LEREN VAN DE KOPLOPERS

Tot nu toe hebben we alleen de gecombineerde resultaten besproken. Wat ons opviel was dat sommige bedrijven binnen de groep het beter doen dan gemiddeld – en sommige slechter.

Dit wekte onze nieuwsgierigheid, dus hebben we de resultaten naast elkaar gehouden en vergeleken. Daarvoor hebben we een score toegekend aan elke vraag waarmee een resultaat wordt gemeten, zoals 'hebt u een datalek gehad' en 'hoe snel kunt u reageren op incidenten?' We kenden een positieve score toe aan goede resultaten en een negatieve score aan slechte resultaten. Door deze vervolgens bij elkaar op te tellen, werd een totaalscore voor elke deelnemer verkregen.

De bedrijven die scoorden in de hoogste 33% in alle categorieën werden benoemd tot 'Koplopers in digitaal vertrouwen'. De bedrijven met een score in de laagste 33% zijn de 'Achterblijvers in digitaal vertrouwen'.

Daarna keken we voor elk van de vier vormen van digitaal vertrouwen naar de verschillen tussen uitkomsten en inspanningen voor deze twee groepen.

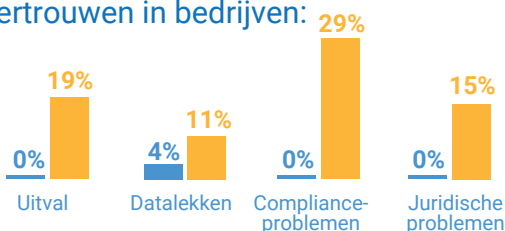
Vertrouwen in bedrijven

In het onderdeel Vertrouwen in bedrijven doen de koplopers het veel beter. Ze ondervinden veel minder problemen op het gebied van vertrouwen in bedrijven: geen uitval, nauwelijks datalekken en geen problemen met compliance of juridische zaken.

Ongeveer driekwart van de koplopers (74%) zegt dat ze zeer snel kunnen reageren op uitval, ten opzichte van slechts 59% van de achterblijvers.

Koplopers zeggen bijna zes keer zo vaak dat ze zijn voorbereid op post-quantumcomputers (**59% ten opzichte van 11% van de achterblijvers**).

Ondervond minder problemen op het gebied van vertrouwen in bedrijven:



Snellere voorbereiding op PQC

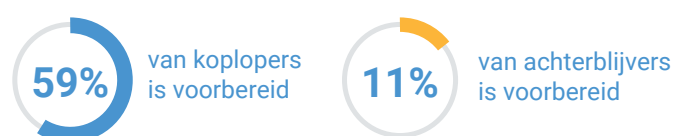


Koplopers hebben twee jaar nodig t.o.v. drie jaar bij achterblijvers

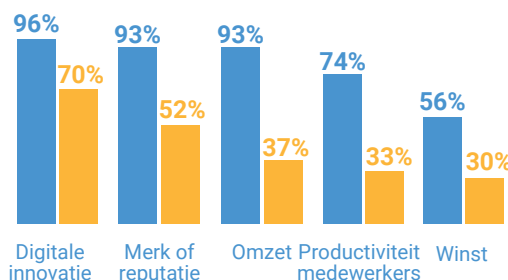
Sneller reageren op uitval



Snellere voorbereiding op PQC

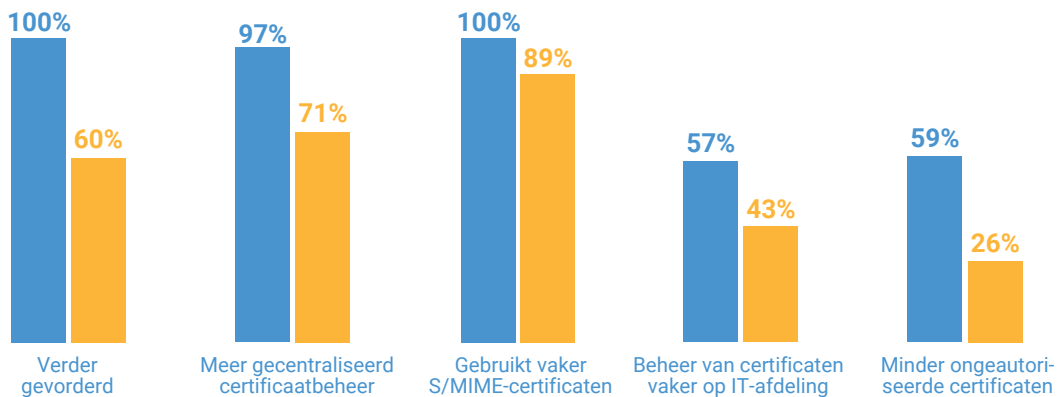


Vertrouwen in bedrijven heeft aanzienlijk bijgedragen aan de organisatie:



Wat doen de koplopers anders?

Ten eerste zegt 100% van de koplopers op het gebied van Vertrouwen in bedrijven dat ze daarmee zeer vergevorderd zijn. Ze werken meer gecentraliseerd, gebruiken S/MIME-certificaten om e-mailcommunicatie te beveiligen en beheren certificaten op de IT-afdeling. Ze zeggen ook dat er minder ongeautoriseerde certificaten worden gebruikt – hoe tegenstrijdig dat ook lijkt.

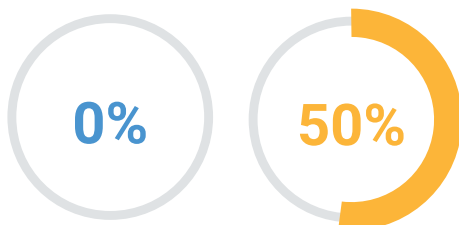


Vertrouwen in IoT- en verbonden apparaten

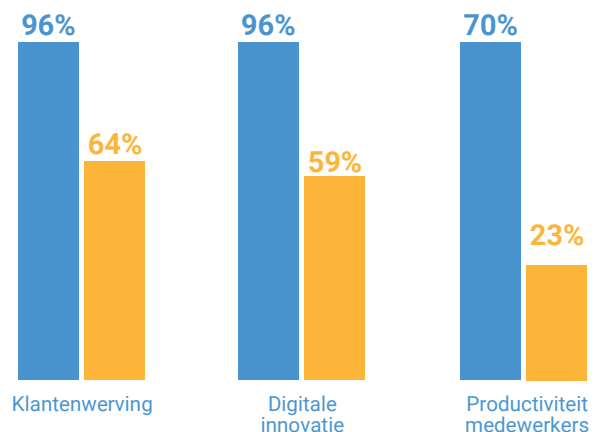
Daarna hebben we naar de professionals op het gebied van IoT- en verbonden apparaten gekeken. Ook hier doen de koplopers het aanzienlijk beter dan de achterblijvers. De koplopers ondervinden nul complianceproblemen dankzij vertrouwen in IoT- en verbonden apparaten, terwijl de helft (50%) van de achterblijvers die problemen wel had.

Ook vinden de koplopers dat hun vertrouwen in IoT- en verbonden apparaten meer ten goede komt aan de organisatie in zijn geheel, waarbij ze bijna allemaal (96%) aangeven dat het bijdraagt aan klantacquisitie en digitale innovatie en de meeste (70%) zeggen dat het de medewerkersproductiviteit verbetert. Bij de achterblijvers zijn deze cijfers respectievelijk 64%, 59% en 23%.

Ondervond minder complianceproblemen



Vertrouwen in IoT heeft aanzienlijk bijgedragen aan de organisatie:

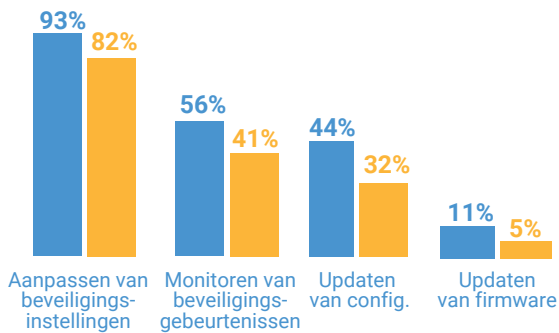


Wat doen ze anders?

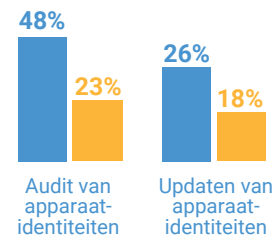
Ten eerste kunnen de koplopers hun geïnstalleerde apparaten beter monitoren en er beter veranderingen in aanbrengen. Ook zijn ze beter in het auditen en updaten van apparaatidentiteiten.

En ten slotte zegt GEEN van de achterblijvers volledig klaar te zijn voor vertrouwensproblemen met het IoT, terwijl 19% van de koplopers zegt dat wel te zijn.

Kan geïnstalleerde apparaten beter wijzigen:



Capabeler met betrekking tot:



Beter voorbereid op IoT-vertrouwensproblemen



Vertrouwen in software

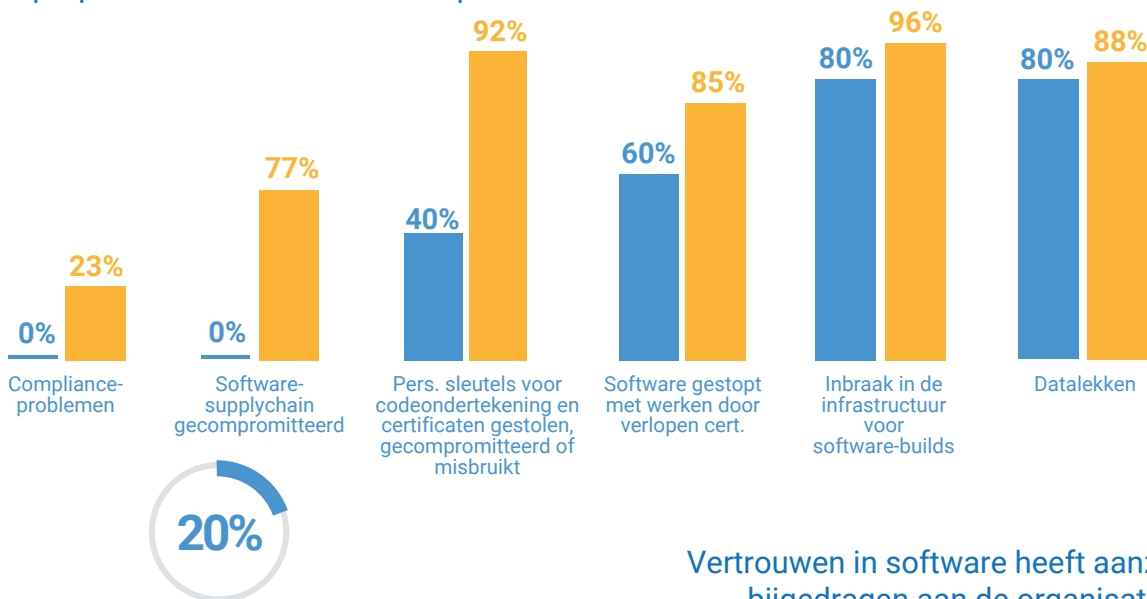
Daarna keken we naar de professionals op het gebied van Vertrouwen in software. De koplopers doen het hier ook beter dan de achterblijvers en ondervinden aanzienlijk minder problemen als gevolg van het gebrek aan vertrouwen in software. Zo kreeg geen van de koplopers te maken met complianceproblemen of een gecompromitteerde software-supplychain, ten opzichte van respectievelijk 23% en 77% van de achterblijvers.

Daarnaast geeft één op de vijf (20%) aan dat ze zeer vergevorderd zijn met vertrouwen in software, terwijl geen van de achterblijvers dat is.

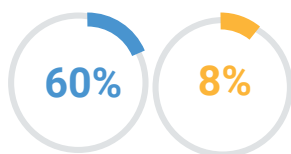
De koplopers doen het ook veel beter voor wat betreft compliance (60% in vergelijking met slechts 8% van de achterblijvers).

De koplopers zeggen vaker dan de achterblijvers dat hun inspanningen op het gebied van vertrouwen in software een positieve impact hebben gehad op de organisatie en ten goede zijn gekomen aan zaken zoals digitale innovatie, klantinnovatie en de productiviteit van medewerkers.

Koplopers ondervinden minder problemen met vertrouwen in software:

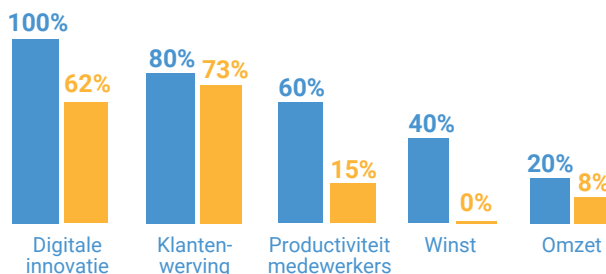


Koplopers zijn zeer vergevorderd met vertrouwen in software, terwijl GEEN van de achterblijvers dat is



Koplopers doen het zeer goed op het gebied van compliance

Vertrouwen in software heeft aanzienlijk bijgedragen aan de organisatie:



Hoe onderscheiden de koplopers zich?

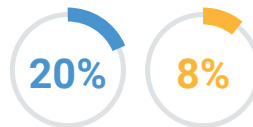
De koplopers zeggen tweemaal zo vaak dat ze een formeel goedkeuringsproces hebben voor het gebruik van cryptografische sleutels (80%, ten opzichte van 38% van de achterblijvers).

Ook zeggen de koplopers veel vaker dat ze zeer gemakkelijk een lijst kunnen genereren van alle softwareonderdelen en de configuratie daarvan in de software die ze produceren (20%, ten opzichte van slechts 8% van de achterblijvers).



Gebruiken vaker een goedkeuringsproces voor gebruik van sleutels

Koplopers vinden het heel gemakkelijk om een lijst te genereren van alle softwareonderdelen en de configuratie daarvan in hun software



Vertrouwen in eSignatures

De laatste groep die we hebben bekeken, was die van de eSignatures. Het vertrouwen daarin wordt meestal beheerd door niet-technische medewerkers (zoals managers van HR, juridische zaken of verkoop). Zonder de betrokkenheid van de IT-afdeling is er minder technische kennis beschikbaar voor het managen van de inspanningen op het gebied van eSignature, en dat wordt wel duidelijk uit de resultaten.

Zo zeggen meer koplopers dat ze zeer vergevorderd zijn met eSignature dan de achterblijvers, maar het daadwerkelijke percentage (10%) is klein. Ook ondervinden koplopers minder problemen met vertrouwen in eSignature, en zeggen ze dat meer bijdragen aan de organisatie dan de achterblijvers.

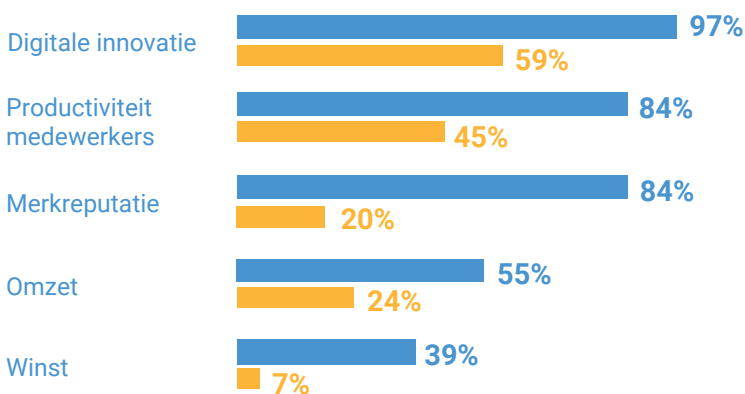


van de koplopers is zeer vergevorderd met Vertrouwen in eSignatures versus GEEN van de achterblijvers

Koplopers ondervinden minder problemen met vertrouwen in eSignatures:

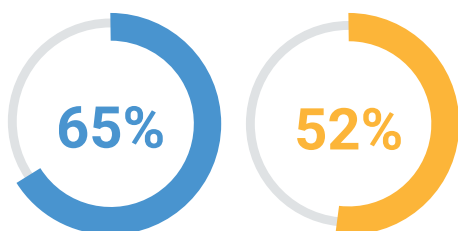


Vertrouwen in eSignatures heeft aanzienlijk bijgedragen aan de organisatie:



Wat maakt de koplopers zo bijzonder?

De verschillen zijn terug te leiden naar één cruciale eigenschap. De koplopers zijn verder gevorderd met het begrip, de implementatie en het beheer van beleidsregels en governance voor eSignatures en eSeals.



De koplopers zijn verder gevorderd met het begrip, de implementatie en het beheer van beleidsregels en governance voor eSignatures en eSeals

CONCLUSIES VAN DIGICERT

Naarmate het aantal bedreigingen stijgt, groeit ook de kloof tussen de organisaties die vooroplopen op het gebied van digitaal vertrouwen en de organisaties die achterblijven. En hoewel de koplopers en achterblijvers wel weten waar ze staan, vormt de schijnveiligheid waarachter de middenmoot zich verschuilt het grootste risico. En als deze kloof blijft groeien doordat men denkt 'dat het wel goed zit', kunnen de gevolgen zeer ernstig zijn.

Wat moeten organisaties doen om enerzijds niet alleen hun overkoepelende inspanningen voor digitaal vertrouwen te optimaliseren, maar anderzijds ook specifiek die op het gebied van vertrouwen in bedrijfs-IT, software, apparaten en documenten?

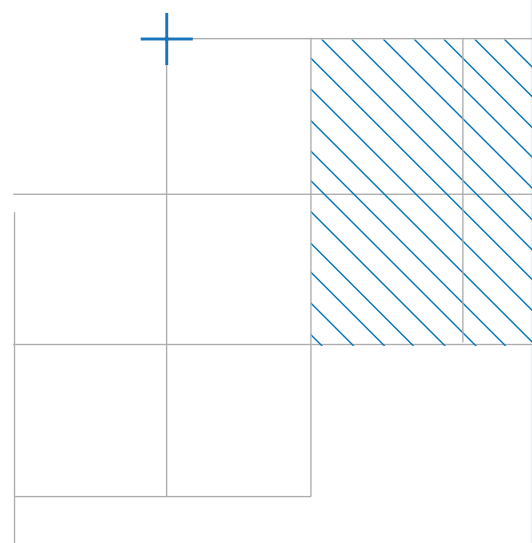
DigiCert is de wereldwijd toonaangevende leverancier van digitaal vertrouwen, die zowel individuen als bedrijven de zekerheid biedt dat hun online aanwezigheid is beveiligd. DigiCert houdt zich al ruim 20 jaar bezig met digitaal vertrouwen en heeft vijf adviezen voor bedrijven die het succes van de koplopers willen evenaren:

Inventariseer

Er wordt weleens gezegd dat je niet kunt managen wat je niet kunt zien en dat geldt zeker voor digitaal vertrouwen. Bouw een compleet beeld op van hoe digitale identiteiten en cryptografische sleutels worden gemaakt, beschermd en gebruikt binnen uw onderneming. Dit kunt u doen met een handmatig discovery-proces voor bedrijfsprocessen, of u kunt gebruikmaken van technologie om een doorlopende scan uit te voeren van uw omgeving en gegevens te verzamelen uit andere bronnen, zoals IT-assetmanagementsystemen.

Stel beleid vast

Er zijn vele beleidsoverwegingen die u kunt maken voor uw inspanningen op het gebied van digitaal vertrouwen. Organisaties moeten beleidsregels opstellen voor de veilige authenticatie van apparaten en gebruikers, zowel op afstand als op kantoor. Stel beleidsregels op die noodzakelijk zijn voor compliance, met name voor producenten van medische apparatuur en andere zwaar gereguleerde industrieën. Als uw organisatie bedrijfskritieke software produceert, definieer dan beleidsregels voor de beveiliging van de software-supplychain. Start of ga verder met zero-trust initiatieven, met name voor cloudworkloads waarbij gevoelige en gereguleerde gegevens worden verwerkt. Dit in aanvulling op basisbeleid voor het gebruik van cryptografie en public key infrastructure binnen de organisatie.



Centraliseer PKI-beheer

Organisaties hebben een zekere mate van cryptografische flexibiliteit nodig, wat inhoudt dat ze cryptografische assets snel kunnen updaten en herstellen. Implementeer tools voor het centraal beheren en automatiseren van digitale certificaten en PKI, om toekomstige onderbrekingen te voorkomen en risico's te minimaliseren. De aanpak biedt verschillende voordelen, zoals betere beveiliging, meer efficiëntie en eenvoudiger beheer.

Prioriteer op basis van impact

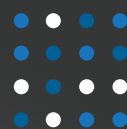
Evalueer uw inventaris om te zien welke assets verband houden met bedrijfskritieke applicaties en processen. Dit zijn de gebieden waar u de eerste verbeteringen moet aanbrengen. Verhelp eventuele kwetsbaarheden in de beveiliging voordat u oplossingen implementeert voor het stroomlijnen van de taken op het gebied van digitaal vertrouwen. Laat bijvoorbeeld gebruikers hun apparaten automatisch en eenvoudig registreren voor veilige externe toegang, zonder hulp van de IT-afdeling. Verbeter de cloudbeveiliging door snel en veilig servercertificaten uit te geven en te installeren om gegevens en communicatie te beveiligen.

Conclusie

Organisaties die prioriteit geven aan digitaal vertrouwen profiteren van een sterker merk, minder cybersecurity-risico's en meer operationele efficiëntie. Ze wekken vertrouwen bij hun klanten, partners en stakeholders met krachtige beveiligingsmaatregelen en transparante governance. Een grote mate van digitaal vertrouwen zorgt ervoor dat u makkelijk kunt omgaan met complexe regelgeving, compliance kunt waarborgen en juridische en financiële risico's kunt verminderen. Daarmee beveiligt u gegevens, vergroot u uw veerkracht en beschermt u zichzelf tegen nieuwe bedreigingen in de moderne digitale wereld.

DIGITAAL VERTROUWEN VOOR DE ECHE WERELD

BEDRIJF



IoT EN APPARATEN

SOFTWARE

DOCUMENT