Factsheet

SECURITY VERKOPEN?

Kwestie van scherpe keuzes maken

Security is ‘big business’. Toch is het verkopen ervan beslist geen eenvoudige zaak. Met deze tips geeft u uw securitybusiness een boost.

UITDAGINGEN

De verkoop van security gaat niet altijd zonder slag of stoot. Een greep uit de grootste uitdagingen:

1. U kunt niet ‘alles’ verkopen aan ‘iedereen’

Het is erg verleidelijk om zoveel mogelijk klanten te bedienen. Toch is dat voor vrijwel de meeste partners een doodlopende weg. U kunt niet ‘alles’ verkopen aan ‘iedereen’. Security verkopen betekent keuzes maken. U moet namelijk de klant, de markt en de daarbij horende specifieke standaarden, compliance-issues, workflows en risico’s begrijpen. Het is onmogelijk om voor elke branche de juiste expertise te ontwikkelen.

2. Security is een complexe zaak

De wereld van cybersecurity is zeer complex en divers. Allereerst gaan de ontwikkelingen razendsnel. Cybercriminelen ontdekken dagelijks nieuwe kwetsbaarheden en ontwikkelen nieuwe aanvalsmethoden. Er zijn een groot aantal middelen om hier een stokje voor te steken, van endpointoplossingen tot firewalls en van back-upsoftware tot SIEM. Ieder onderdeel moet passen in het grotere geheel.

Daarbij gaat security veel verder dan enkel techniek. Het bewustzijn van medewerkers en aandacht voor veilige processen zijn minstens zo belangrijk. Dat maakt een toch al ingewikkelde puzzel nog complexer.

3. De markt is overvol

Security is een groeimarkt, dus iedereen pikt graag een graantje mee. Naast gerenommeerde partijen met degelijke oplossingen wemelt het van de cowboys. Zij leveren soms oplossingen die (in sommige gevallen bewust) meer kwaad doen dan goed. Het selecteren van kwalitatief goede oplossingen is niet eenvoudig.

4. Securitymiddelen mogen de productiviteit niet in de weg staan

Voor geen enkele organisatie is security het doel. Het is slechts een middel om de business zo goed mogelijk draaiende te houden. Het laatste waar klanten (en

hun medewerkers) op zitten te wachten zijn security-middelen en -maatregelen die hun dagelijkse werkzaamheden verstoren.

DE JUISTE AANDACHTSPUNTEN

De verkoop van securityoplossingen vereist een doordachte aanpak. Dit zijn de belangrijkste aandachtspunten om uzelf goed te presenteren bij uw klant:

1. Leer uw klant kennen

De securitymarkt is ingewikkeld, met veel partijen die min of meer hetzelfde bieden of dat zeggen te doen. Eindklanten raken daardoor al snel overweldigd. Niet voor niets hebben zij behoefte aan een 'gids'. Ze willen een partner die hun markt, hun zorgen, hun uitdagingen en hun behoeften begrijpt.

Dat betekent niet alleen dat u zich moet verdiepen of zelfs specialiseren in die specifieke sector, maar ook in de situatie van de klant. Hoe ziet de huidige securityomgeving eruit? Wat zijn de zwakke plekken, en op welke technologie zijn de huidige securityoplossingen gebaseerd? Met een gedetailleerd inzicht in de specifieke klantsituatie vergroot u uw geloofwaardigheid en de kans op een succesvolle verkoop.

2. Zorg voor 'proof points'

Natuurlijk zijn er altijd klanten die u op uw blauwe ogen geloven. Maar een aanzienlijk deel vraagt u aan te tonen dat uw aanpak of oplossing eerder heeft gewerkt. Het is daarom belangrijk dat u daarvan bewijs kunt leveren. Bijvoorbeeld in de vorm van een testimonial of uitgewerkte klantcase. Deze verhalen zorgen voor herkenbaarheid bij de eindklant ('In die situatie zit ik ook!') en bovendien wint u er vertrouwen mee. Werk aan de winkel voor de (content)marketingafdeling, dus. Heeft u geen eigen marketingteam of zoekt u hierbij hulp? Tech Data kan u hierbij ondersteunen.

3. Wees realistisch

Security is geen 'set and forget', en 100 procent veiligheid bestaat niet. Dat zijn misschien twee overbekende clichés voor wie vertrouwd is met de materie. Voor veel eindklanten zijn dit echter beslist geen clichés. Zij verwachten dit misschien wel. Het is belangrijk om die teleurstelling voor te zijn. Maak geen beloftes die u niet waar kunt maken. Verhelder het feit dat het opbouwen van een goede securityomgeving in fasen verloopt. Bijvoorbeeld door de klant aan de hand van een 'maturitymodel' vertrouwd te maken met de verschillende fasen, en met een nulmeting vast te stellen waar ze nu staan. Maak realistische plannen die u afzet tegen een net zo realistische tijdlijn.

4. Vertaal techniek naar de praktijk

Veel securityfabrikanten hebben de mond vol van specificaties en technologieën die ze toepassen. Lijstjes met versies van besturingssystemen, bandbreedtes, ondersteunde protocollen en hippe termen als AI en machine learning sieren veel leveranciers-websites. Dat is allemaal zeer informatief, maar wel enkel voor de kenner. De klant wil gewoon 'dat het werkt' en 'dat de gegevens veilig blijven'. Het is aan u om al die technische opsmuk en dat jargon te vertalen naar de consequenties voor de dagelijkse praktijk. Dat vergt technische kennis en kennis van de klantsituatie. Investeer in beide.

5. Inventariseer de risico's

Met een overvolle securitymarkt is het voor veel eindklanten niet altijd duidelijk wat ze nu precies nodig hebben. Het gebeurt dan ook zelden dat ze met een specifieke wens naar hun partner stappen. Daarom is het de taak van de partner om de rollen om te draaien; de eindklant verwacht namelijk dat u hen vertelt wat zij nodig hebben. Een goede manier om dat te doen is door het uitvoeren van een risico-inventarisatie. Op basis van de uitkomsten is het eenvoudiger om prioriteiten te stellen.

6. Ken de behoefte van alle stakeholders

Bij de aanschaf van securityoplossingen zijn doorgaans meerdere beslissers betrokken. Begrijp hun individuele behoeften zodat u hen allemaal overtuigt. Zo zal een CFO u bevragen over de kosten en de financiering, terwijl de CISO wil weten hoe de securityoplossingen passen binnen het beveiligingsbeleid van de organisatie. De CEO zal met name geïnteresseerd zijn in de gevolgen voor businesscontinuïteit en risicomanagement. De CTO wil alles weten van de technische aspecten, zoals het toepassen van updates en het inpassen van de oplossing in de bestaande infrastructuur.

7. Verkoop niet op (ongegronde) angst

Angst is niet alleen een slechte raadgever, het is ook

>>>

BETREK ONS ZO VROEG MOGELIJK IN HET PROCES OM MET ELKAAR DE BESTE OPLOSSING SAMEN TE STELLEN.

een zeer beproefd salesinstrument in de security-markt. Die aanpak is daardoor nauwelijks onderscheidend. Door de angstkaart te spelen, onderscheidt u zich niet. Bovendien gaat de klant u associëren met gevaar en negativiteit. Beter is de klant zonder hysterie en op objectieve wijze te informeren over de belangrijkste, voor zijn of haar business specifieke risico's. Schets daarbij welke securityoplossingen in welke mate een bijdrage kunnen leveren in het verminderen van die risico's. Benadruk daarbij het belang van businesscontinuïteit (positief) in plaats van het schetsen van allerlei horrorscenario's die misschien wel nooit werkelijkheid worden. Dat zorgt voor vertrouwen en maakt de salespitch wél onderscheidend.

8. Houd rekening met compliance

Iedere klant heeft te maken met compliance-issues. Zo verplicht de Algemene verordening gegevensbescherming (AVG) organisaties gevoelige persoonsgegevens te beschermen. Als dergelijke data op straat terechtkomen, loopt de klant risico op een hoge boete en aanzienlijke reputatieschade. Verder kunnen er allerlei branchespecifieke eisen en normeringen zijn waar de klant aan moet voldoen. Maak in de salespitch dan ook duidelijk op welke manier security kan bijdragen aan het oplossen van deze uitdagingen.

9. Besteed aandacht aan goede integratie

Veel klanten zijn bang dat beveiligingsoplossingen duur, ingewikkeld of moeilijk te gebruiken zijn. Ze voorzien dat deze oplossingen hun workflows verstoren of een last vormen voor hun medewerkers. In werkelijkheid moet een securityoplossing hun corebusiness beschermen, niet belemmeren. Leg de nadruk dan ook op de eenvoudige en efficiënte manieren waarop beveiliging past in de bestaande infrastructuur en processen. Op die manier zien klanten vooral de mogelijkheden, in plaats van de uitdagingen.

10. Betrek Tech Data in het salesproces

Tech Data heeft direct contact met securityleveranciers. We kunnen u uitgebreid ondersteunen bij de verkoop van securityoplossingen:

• Kennis en expertise

We hebben uitgebreide en actuele kennis van security. Daarmee ondersteunen we u bij het verkopen van securityoplossingen en -diensten. Laat onze experts helpen de situatie van uw klant grondig door te lichten, en mee te denken over passende oplossingen. We geven desgewenst passende trainingen en helpen u in het zadel met officiële certificeringen.

• Onestopshop door breed portfolio

We leveren een zeer breed pakket securityoplossingen van zowel de grote leveranciers als van nichespelers. Dat bespaart u een flinke zoektocht.

• Eenvoudige beheer- en facturatietools

Levert u securityoplossingen uit de cloud? We bieden tools die het gebruik ervan inzichtelijk maken. We leveren ze desgewenst onder een 'private label', voor het behoud van uw herkenbaarheid.

• Aanvullende diensten

Onze dienstverlening gaat veel verder dan 'traditionele' distributie. Zo bieden we sales- en marketingondersteuning. Ook bieden we hulp bij de financiering van securitygerelateerde investeringen. Betrek ons zo vroeg mogelijk in het proces, om met elkaar de beste oplossing samen te stellen. Wilt u weten waarmee we u kunnen helpen? Neem dan contact op met ons.

WWW.TECHDATA.NL

Tech Data Nederland B.V.
Tolnasingel 2 · 2411 PV Bodegraven
+31 (0) 88 133 40 00 · tdsecurity@techdata.nl