# CASE CM.COM

## Dankzij SentinelOne heeft CM.com de gewenste grip op endpoints zonder performance-problemen

CM.com is een wereldwijde leider in cloudsoftware voor conversational commerce. Het communicatie- en betalingsplatform van CM.com stelt marketing-, sales en customer service-teams in staat om de communicatie met klanten en de betalingen die zij doen via meerdere mobiele kanalen, efficiënt te laten verlopen en te automatiseren. Zo helpt CM.com onder andere de Formule 1 Heineken Dutch Grand Prix als officiële evenementpartner met

het optimaliseren van hun ticketproces en het creëren van een superieure fanervaring. Om alle CM.com-klanten te bedienen, heeft het bedrijf kantoren over de hele wereld en meerdere serverparken om de clouddienst te allen tijde in de lucht te houden. “We willen dat graag op een veilige manier doen en cybercriminelen, die steeds actiever worden met phishingaanvallen, buiten de deur houden”, zegt Sándor Incze, Chief Information Security Officer bij CM.com. “Zo is ons security-team voortdurend bezig met het testen van onze machines en software, én maken we gebruik van security-oplossingen om onze data en die van onze klanten te beschermen.”

**Geen performance-verlies en meer grip op de endpoints**

Voordat CM.com met SentinelOne ging werken om de endpoints te beschermen, maakte het gebruik van traditionele antivirussoftware. Deze software had echter een negatief effect op de performance van de machines. Incze: “Dit zorgde voor veel irritatie bij onze medewerkers en met name bij onze developers. Die ‘dreigden’ met regelmaat om de antivirus-tooling te deïnstalleren, zodat ze hier geen last van hadden. Maar wij wel. Want vanuit security-oogpunt was dat natuurlijk een zorgelijke ontwikkeling. We wilden meer controle op wat er op onze devices gebeurt. Niet meer dan logisch, omdat de laptops die onze medewerkers gebruiken eigendom zijn van CM.com.”

Op een securitybeurs kwam CM.com in contact met SentinelOne. Na het zien van een demo van de Endpoint Protection-oplossing was CM.com overtuigd dat de oplossing de extra bescherming bood die het bedrijf zocht. “We hadden een aantal belangrijke voorwaarden gesteld aan de nieuwe oplossing en SentinelOne bleek hieraan te kunnen voldoen. Zo was de oplossing makkelijk en snel te deployen, zonder dat dit impact heeft op performance van onze machines.” Daarnaast biedt de oplossing het security-team veel meer controle over wat er op onze endpoints gebeurt. “Zo kun je de tooling van SentinelOne niet deïnstalleren zonder centrale adminrechten, wat onze medewerkers verplicht om SentinelOne op hun laptop of desktop te hebben draaien”, zegt Incze. “SentinelOne voorkomt dat medewerkers zelf alle keuzevrijheid hebben om software te downloaden. Denk aan oplossingen die er op het eerste oog veilig uitzien, maar misschien wel door cybercriminelen op het web zijn geplaatst. Dit vergroot ook het risico dat je ransomware binnenhaalt. Met de oplossing van SentinelOne zijn we hier veel beter tegen beschermd. En vinden er toch vreemde gedragingen plaats in onze omgeving, dan is SentinelOne in staat om deze tijdig te detecteren en ons te waarschuwen.”

**Dashboard biedt overzichtelijke informatie en uitgebreide filtermogelijkheden**

Incze is onder de indruk van de overzichtelijke informatie en uitgebreide filtermogelijkheden die het dashboard van SentinelOne biedt. “In het geval van een groot datalek, zoals die van Microsoft Exchange, kunnen we snel en makkelijk achterhalen of we zijn geïnfecteerd of niet. Met de filters kunnen we tot op gebruikersniveau inzicht krijgen, bijvoorbeeld om te achterhalen op welke systemen een gebruiker voor het laatst heeft ingelogd.” Bij twijfel kan CM.com binnen no-time op afstand een machine van het netwerk halen. Een proces dat volgens Incze niet alleen een stuk

efficiënter verloopt, maar ook meer service biedt voor de medewerker, die niet wordt geremd in zijn werk. Incze: “Wanneer we voorheen een virus hadden geconstateerd of malware vermoedden, moest een medewerker eerst zijn laptop uitzetten en onze kant opsturen, zodat we de harde schijf eruit konden halen. Nu kunnen we, ongeacht de locatie van een gebruiker, op afstand testen of zelfs commando’s uitvoeren om een machine te updaten, te scannen of om logfiles te maken. Van geval tot geval beoordelen we of deze manier van werken, die forensische sporen zeker aantast, toepasbaar is.

De basisregel is dat als we het niet vertrouwen, we het device in quarantaine plaatsen. De gebruiker kan dan zelf het netwerk niet op, maar wij kunnen er wel makkelijk bij. Dit levert op het vlak van IT-beheer veel tijdswinst op. Zo heb ik laatste geklokt dat we iemand binnen tien seconden van het netwerk kunnen halen om hem er vervolgens binnen dertig seconden weer mee te verbinden. Naar je medewerkers toe is dat natuurlijk een veel betere service, omdat ze nauwelijks in hun werk worden gestoord. Ook op dit gebied maakt SentinelOne voor ons echt het verschil.”

**Integratie met Automox maakt patchen snel en eenvoudig**

SentinelOne biedt CM.com ook veel inzicht in de kwetsbaarheden die worden veroorzaakt door verouderde software. Dankzij een slimme integratie met Automox is het in staat om hier ook met één druk op de knop iets aan te doen. “Het inzicht dat SentinelOne ons biedt in verouderde software is natuurlijk erg waardevol, omdat te laat patchen de nodige security-risico’s met zich meebrengt. Het liefst wil je ook meteen iets met die informatie doen en je machines onmiddellijk patchen”, zegt Incze. “SentinelOne biedt die mogelijkheid zelf niet, maar heeft wel een integratie met de patch management-tool van Automox. Zo kunnen we, wanneer kwetsbaarheden door SentinelOne worden aangetoond, ook direct patches uitvoeren om deze te verhelpen. Dit levert een enorme tijdsbesparing op voor ons IT & security-team. En maakt onze IT-omgeving natuurlijk een stuk veiliger.”

---

## CASE PORTAAL

## Portaal: snel inzicht in mogelijke dreigingen dankzij SentinelOne

Portaal is een grote woningcorporatie, die actief is in vijf grote stedelijke gebieden in Nederland. Dit zijn Arnhem, Nijmegen, Amersfoort, Utrecht en Leiden. Daarnaast heeft Portaal een eigen onderhoudsbedrijf. Portaal beheert iets meer dan 50.000 verhuurbare eenheden en heeft 900 man personeel in dienst. Het IT-team bestaat uit 19 mensen.

**Antivirussoftware voldoet niet meer na overstap op laptops**

Portaal stapte in 2020 over van het gebruik van desktops naar laptops. Dit verhoogde de noodzaak om te kijken naar een veilige endpoint-oplossing ter bescherming van de Citrix-werkplekken. Sander van der Straten, Teamleider Servicemanagement bij Portaal: “Tot dat moment maakten we voor het beschermen van onze virtuele desktopomgeving gebruik van de antivirus-software van Webroot. Die voldeed echter niet meer toen het gros van onze medewerkers overstapte op een eigen laptop. We wilden hiermee het werken op afstand makkelijker maken; een gevolg van het uitbreken van de corona pandemie. In plaats van 20 zijn er nu ruim 600 laptops in omloop. Omdat deze laptops zich buiten het eigen netwerk bevinden, wilden we meer grip kunnen houden op wat er op deze laptops gebeurt. Als woningcorporatie beheren we veel privacygevoelige persoonsgegevens van onze

huurders. Goede bescherming van deze data is cruciaal. Het laatste wat we willen is dat data van onze huurders wordt vergrendeld, met alle ellende die daaruit volgt." Zoektocht naar een geschikte endpoint-oplossing Portaal zocht naar een zelfredzame endpoint-oplossing die voldoende informatie bood, zodat snel en tijdig actie kan worden ondernomen wanneer zich een incident dreigt voor te doen. Van der Straten.

"Een duidelijk speerpunt in ons informatiebeveiligingsbeleid was dat we meer inzicht wilden hebben in welke risico's er zijn binnen onze omgeving. Dan is het scannen van bekende signatures met antivirussoftware niet voldoende." Portaal keek in eerste instantie naar de mogelijkheden bij Microsoft. Van der Straten: "Ons bedrijfsbeleid is erop gericht om zoveel mogelijk gebruik te maken van de licenties die we al hebben. Daarom was Microsoft Endpoint Protection de eerste oplossing die we overwogen." Maar het Proof of Concept van deze oplossing stelde Portaal niet tevreden.

"Wanneer zich een incident dreigt voor te doen, willen we door de oplossing onmiddellijk gealarmeerd worden en genoeg informatie krijgen over wat er zich precies voordoet", zegt Van der Straten. "De rapportagemogelijkheden in de oplossing van Microsoft waren hierin beperkt. Je bent dan als team te veel tijd kwijt aan het zelf achterhalen wat er mogelijk aan de hand is in je systeem. We wilden een oplossing die zelfredzaam is en dreigingen snel inzichtelijk maakt. Als IT-afdeling van 19 man sterk hebben we onvoldoende mankracht beschikbaar om zelf op ieder moment van de dag naar een dashboard te kijken. Als een virus al actief is en je bent er niet op tijd bij, dan is het kwaad al geschied."

**SentinelOne biedt gewenste inzicht en uitgebreide filtermogelijkheden**

In de zoektocht naar alternatieven kwam Portaal uit bij de oplossingen van F-Secure, Bitdefender en SentinelOne. Van der Straten: "Ook met deze leveranciers hebben we een Proof of Concept gedraaid. In de oplossing van SentinelOne hadden we uiteindelijk het meeste vertrouwen. In tegenstelling tot andere leveranciers was SentinelOne in staat de oplossing snel en efficiënt uit te rollen. Hierdoor was ons IT-team meteen overtuigd van het gebruiksgemak. Verder is performance-testen met betrekking tot onze Citrix-omgeving erg belangrijk. De lage footprint van de agents, stemde ons dus positief. Bovendien is het dashboard van SentinelOne zeer overzichtelijk: de issues die onze aandacht verdienen worden duidelijk in beeld gebracht en voorzien van een heldere uitleg. Zo is voor ons meteen inzichtelijk of we prioriteit aan een melding moeten geven of dat we het op een later moment kunnen oppakken. En dankzij de uitgebreide filteropties, kunnen we ook gemakkelijk zelf op onderzoek gaan. Dit helpt ons om instellingen te finetunen. Indien nodig kunnen we altijd snel bouwen op de support van SentinelOne."

De oplossing van SentinelOne helpt Portaal ook voorkomen dat medewerkers applicaties downloaden zonder dat IT hier weet van heeft. Van der Straten: "SentinelOne draait op alle laptops van onze medewerkers. Een mooie bijvangst is dat we dankzij de oplossing ook zien van welke (illegale) software onze medewerkers gebruik willen maken. Die wordt door SentinelOne inzichtelijk gemaakt waardoor we ook makkelijker met medewerkers in gesprek kunnen gaan om hun wensen te bespreken. En uiteraard kunnen we zo voorkomen dat onze laptops worden geïnfecteerd. Gelukkig hebben we nog niet te maken gehad met een groot incident, maar mocht het gebeuren, dan hebben we er alle vertrouwen in dat de oplossing van SentinelOne ons beschermt. Het feit dat SentinelOne zijn klanten een garantie biedt, waarbij de klant wordt gecompenseerd in het geval een ransomware aanval toch door de detectie- en preventielaag weet te komen, maakte het besluit van ons management om voor SentinelOne te kiezen natuurlijk nog eenvoudiger."

De oplossing van SentinelOne biedt de mogelijkheid om na het herkennen van verdachte gedragingen mogelijke malware automatisch in quarantaine te plaatsen of zelfs te verwijderen. Van der Straten: “Op dit moment willen we hier zelf nog controle over houden om te kunnen onderzoeken hoeveel false positives aan het licht komen. De verwachting is wel dat we overstappen naar een volledig geautomatiseerd proces, omdat we zien dat SentinelOne de juiste zaken tegenhoudt.”

Portaal was ook blij verrast door het beheergemak van de oplossing. Van der Straten: “Omdat we de stap zetten naar laptops, waren we bang dat het updaten van de agents te veel tijd in beslag zou nemen. Niets bleek minder waar: zo konden we de agent makkelijk deployen door middel van Microsoft Intune en na de deployment makkelijk updaten. Dit kost nog geen vijf minuten. Juist in een heel druk team als dat van ons is dat erg prettig.”