EasyComp Zeeland
De Specialist voor uw Computer, Business Systems & Web-service

Datum & Plaats	Onderwerp	Auteur
6 jun. 2020 Middelburg	Cyber AI & EasyComp Cloud: Nieuwe computermodellen, toepassingen, gebruikers en apparaten beveiligen	S.A.C. Abdel Nasser

Voorwoord 2

Bedreigingsvectoren in de cloud 4

- Insider Bedreiging 4
- Gecompromitteerde referenties 5
- Verkeerde configuraties 5

Edge Computing 6

- Onbeveiligde API's 7

Beperkingen van native beveiligingstools en beveiligingstools van derden 7

- Cloudspecifieke tools van derden 8

EasyComp Cloud 8

- EasyComp Zeeland Antigena: Autonome reactie in de cloud 10
- EasyComp Zeeland Threat Visualizer: Volledige zichtbaarheid 10

Scenario's voor implementatie van technologie 12

- Hybride cloud (IaaS) 12
- Cloud-only (IaaS) 12
- Saas 12

Real-World Threat Ontdekkingen 13

- Diefstal van interne gegevens uit de cloud 13
- Externe aanval op cloudperimeter 13

Conclusie 14

Voorwoord

De snelle adoptie van cloud- en SaaS-services heeft de digitale business getransformeerd en de uitdaging van de verdediging van de onderneming tegen geavanceerde aanvallen fundamenteel hervormd.
Gedreven door de noodzaak om kosten te besparen en de efficiëntie te verhogen, dient de overgang naar de cloud nu als een essentieel kanaal voor digitale transformatieprojecten - van het toepassen van geavanceerde analyses tot big data-sets, tot het ondersteunen van edge computing en apparaten die ten grondslag liggen aan alles van slimme steden tot verbonden auto's.
Maar vanuit een veiligheidsperspectief breiden deze nieuwe computermodellen het aanvalsoppervlak in een alarmerend tempo uit, waardoor nieuwe bedreigingsvectoren worden geïntroduceerd in een steeds meer verspreid bedrijfsnetwerk.
Deze trend vormt een speciale uitdaging voor gespannen beveiligingsteams, die nu moeten omgaan met een omgeving waar ze beperkte zichtbaarheid en controle hebben, en waar hun vertrouwde on-premise beveiligingstools vaak niet van toepassing zijn. Bovendien is het gemak waarmee ontwikkelaars een cloud-exemplaar kunnen draaien en de IT of security team kan het bedrijf blootstellen aan aanzienlijke risico's, veeleisende een nieuwe DevSecOps aanpak die misschien onbekend zijn voor teams die zijn opgegroeid op de traditionele on-premise netwerk model.
Meer in het algemeen worden de beveiligingsuitdagingen die de cloud met zich meebrengt grotendeels beheerst door een gedeeld verantwoordelijkheidsmodel, dat de respectieve gebieden van de cloud afbakent die providers en klanten naar verwachting zullen beheren en beveiligen. Hoewel het deel van het Shared Responsibility Model van de klant varieert tussen IaaS en SaaS, illustreert de algemene strekking van het model duidelijk dat het uitbesteden van bepaalde IT-processen naar de cloud niet neerkomt op het volledig uitbesteden van uw beveiligingsfunctie.
De meeste organisaties herkennen deze realiteit, maar weinig of geen tevreden zijn met de cloud-specifieke beveiligingsoplossingen beschikbaar op de markt, noch kunnen ze hun teams onmiddellijk
een DevSecOps aanpak als alternatief.
Hoewel veel IaaS- en SaaS-providers native beveiligingscontroles bieden om klanten te helpen hun eigen gedeelte van het Shared Responsibility Model te beveiligen, zijn deze controles vaak beperkt in omvang en zijn ze meestal nuttig voor naleving, in plaats van proactief en real-time cyberdefensie.
Zelfs binnen dit beperkte bereik kunnen native beveiligingscontroles alleen effectief zijn als ze adequaat zijn geïmplementeerd door de cloudklant.

Als aanvulling op native controls, oplossingen van derden

zoals Cloud Access Security Brokers (CASBs) en Cloud Workload Protection Platforms (CWPPs) kunnen ook nuttig zijn voor het afdwingen van beleid en het bieden van zichtbaarheid in de cross-cloud, maar ze hebben moeite om subtiele bedreigingen en afwijkend gedrag te detecteren dat niet is vastgelegd door vooraf gedefinieerde regels of beleidsregels. Naarmate bedreigingen zich ontwikkelen en geavanceerder worden, hebben organisaties een fundamenteel nieuwe aanpak nodig om cloudomgevingen te beveiligen tegen geavanceerde aanvallen, voordat ze tijd hebben om te escaleren tot een crisis.
Welke scenario's moet u naast deze native en third-party controls ook overwegen voor cloudbeveiliging?
Enkele aanvullende use cases zijn:
Het opspin van een instantie die IT en beveiliging omzeilt
Productiegegevens worden verplaatst naar minder veilige testsystemen
Lateraal verkeer in de cloud
Office 365- en Salesforce-gebruikers verplaatsen gegevens buiten de cloud
Edge-apparaten die cloud als leiding gebruiken
Ongebruikelijke, subtiele veranderingen in het gedrag van gebruikers
Aanvallen die zich op machinesnelheid bewegen en onmiddellijke actie vereisen
Correlatie en contextuele analyse om afwijkingen op te sporen
Het neutraliseren van kwaadaardige e-mails in Office 365, vooral van vertrouwde afzenders in de supply chain

"EASYCOMP ZEELAND CLOUD VERTEGENWOORDIGT EEN NIEUWE GRENS IN AI-GEBASEERDE CYBERDEFENSIE. ONS TEAM HEEFT NU VOLLEDIGE, REAL-TIME DEKKING VOOR ONZE SAAS-TOEPASSINGEN, CLOUDCONTAINERS EN GEDISTRIBUEERDE SENSOREN IN DE HELE STAD."

Aangedreven door machine learning en AI-algoritmen, EasyComp Zeeland's cyber AI-technologie gaat verder dan de beveiliging die native controles en tools van derden bieden. Met behulp van software en sensoren dekt EasyComp Zeeland Cloud alle use cases zoals eerder vermeld door het analyseren van rijke verkeers- en datastromen in cloud- en SaaS-omgevingen. EasyComp Zeeland's AI leert het normale 'patroon van het leven' voor elke gebruiker, apparaat en container - zonder te vertrouwen op eerdere veronderstellingen of handmatige invoer.
Dit evoluerende begrip van 'normaal' stelt het platform in staat om in realtime autonoom externe aanvallen en insiderbedreigingen te detecteren en erop te reageren, terwijl het volledige zicht biedt in het digitale bedrijf in één ruit. Deze whitepaper onderzoekt de beveiligingslacunes die EasyComp Zeeland's platform opvult met behulp van machine learning en AI. Door de volledige omvang van het evoluerende 'levenspatroon' van uw organisatie te leren, is EasyComp Zeeland's AI uniek geschikt om subtiele afwijkingen die wijzen op een bedreiging op te sporen en te neutraliseren
in de cloud, in harmonie met uw steeds veranderende digitale landgoed.

Bedreigingsvectoren in de cloud

Het shared responsibility-model in de cloud geeft een overzicht van de respectieve beveiligingsrollen van Cloud Service Providers (CSP's) en klanten in de belangrijkste servicemodellen: Infrastructure-as-a-Service (IaaS) voor systemen en opslag en Software-as-a-Service (SaaS) voor zakelijke toepassingen.

Met IaaS is de CSP in grote lijnen verantwoordelijk voor het beveiligen van de basisinfrastructuurcomponenten - waaronder netwerken, servers, VM's en containers - terwijl van de klant wordt verwacht dat hij het gastbesturingssysteem, alle toepassingssoftware en de configuratie van native beveiligingscontroles beheert. Met SaaS is de CSP verantwoordelijk voor de infrastructuur en applicaties, terwijl de klant ervoor moet zorgen dat de gebruikers- en netwerkactiviteit goed wordt beheerd en beveiligd. Dit leidt tot een specifieke set van bedreigingsvectoren waar de cloudklant zich tegen moet kunnen verdedigen, maar waar de meeste native beveiligingscontroles en aanbiedingen van derden slecht zijn uitgerust om in een vroeg stadium te detecteren.
Gartner voorspelt dat tegen 2022 ten minste 95% van de fouten in de cloudbeveiliging zal zijn opgetreden in het gedeelte van de klant van het Shared Responsibility Model.

Dit is een verrassend cijfer, maar door het uitpakken van de belangrijkste bedreigingsvectoren waardoor deze fouten kunnen optreden, kunnen we beter begrijpen wat de cloudklant kan doen om deze risico's effectief te beperken.

Insider Bedreiging

Het merendeel van de industrie erkent dat toonaangevende CSP's en SaaS-leveranciers zijn zeer resistent tegen inbreuken op de beveiliging, althans in hun deel van de Shared Responsibility Model. Maar de unieke uitdagingen die de cloud met zich meebrengt - van een gebrek aan zichtbaarheid en controle, tot de nieuwe onbekende mentaliteit die nodig is voor de wendbaarheid en snelheid van digitale business - hebben de traditionele risico's vergroot die verantwoordelijkheidsgebied van de klant.
In het bijzonder, insider bedreiging vertegenwoordigt een gevaarlijke aanval vector die altijd een risico heeft gevormd, maar die heeft genomen op een nieuwe dimensie en behendigheid via de cloud. Dit soort aanvallen komen uit de organisatie - door ontevreden, onzorgvuldig of gecompromitteerde werknemers, cloudconsultants en andere zakenpartners die misbruik maken van hun toegang tot interne systemen. Kwaadwillende insiders hebben het voordeel van vertrouwdheid met de systemen die ze manipuleren, en kunnen hun tijd nemen bij de

voorbereiding en het plegen van de aanval. Door te lekken of het manipuleren van gegevens langzaam over dagen en weken, deze actoren zijn uniek gepositioneerd om hele cloud-omgevingen te compromitteren en te ontwijken op basis van regels beveiligingstools ontworpen om abnormale activiteit te controleren, in de mate dat deze zijn geïmplementeerd op alle.
Spraakmakende gevallen van insiderdreiging – van edward Snowden's lekken in 2013 tot Tesla's ervaring met insider sabotage in 2018 – hebben schokgolven veroorzaakt in de IT-beveiligingsindustrie en daarbuiten. Het feit dat zogenaamd de meest veilige netwerken kunnen worden geschonden door mensen met voldoende motivatie en technische knowhow heeft een duidelijk signaal naar security professionals dat de dreiging al binnen kan zijn. Met de komst van de cloud worden beveiligingsteams nu geconfronteerd met een kritieke blinde vlek in een zeer gevoelig gebied van het bedrijf, waar insiders vaak kunnen werken zonder argwaan te wekken.

Gecompromitteerde referenties

Om soortgelijke redenen is het risico dat een externe aanvaller legitieme referenties gebruikt om toegang te krijgen ook een cruciaal risico geworden voor organisaties met weinig tot geen zichtbaarheid in de cloud. Door de juiste set referenties te gebruiken en traditionele beveiligingscontroles te omzeilen, kunnen deze bedreigingen de kritieke activa van een hele organisatie in gevaar brengen, vooral omdat werknemers wachtwoorden blijven hergebruiken voor persoonlijke en professionele accounts.
Vaker wel dan niet, werknemer inloggegevens worden opgehaald door middel van datalekken, blootstellingen, of phishing campagnes en verkocht aan de hoogste bieder op het dark web. Eenmaal gekocht, kunnen referenties worden gebruikt om lateraal binnen de cloud te verplaatsen om toegang te krijgen tot kritieke systemen en gegevens. Aanvalsmissies variëren van gegevensexfiltratie of manipulatie, bedrijfsspionage.
Met iaas in het bijzonder worden gebruikersreferenties voor systeembeheerders vaak gezien als de sleutels tot waardevolle cloudassets, waardoor hackers toegang hebben tot gevoelige gegevens in productie- en testomgevingen en zelfs het beheer van de cloudinfrastructuur zelf. Naast het stelen of wijzigen van kritieke gegevens, kunnen cybercriminelen systeembeheerdersreferenties gebruiken om de rekenkracht van de cloud te gebruiken voor hun eigen snode doeleinden, door cloud-exemplaren op te draaien om uitgebreide crypto-mining-activiteiten of Distributed Denial of Service-aanvallen te starten. Vooral voor cloud-only bedrijven vormt deze dreiging een existentieel risico.

Verkeerde configuraties

Naast cyberaanvallen blijft een van de meest voorkomende bedreigingsvectoren in de cloud kritieke misconfiguraties in IaaS-omgevingen. Hoewel menselijke

fouten nooit volledig kunnen worden vermeden, zijn verkeerde configuraties vaak een natuurlijk gevolg van de flexibiliteit van de implementatie en snelle instantiatie van testcontainers en gegevenssets die door de cloud worden gefaciliteerd, wat gebruikers vaak ertoe brengt om snel te bewegen ten koste van de beveiliging. In de huidige digitale business hebben ontwikkelaars de mogelijkheid om een cloud-exemplaar binnen enkele minuten te implementeren, zonder dat ze beveiligingsteams, IT of QA hoeven te raadplegen. In het verleden betekende een tragere workflow dat deze functies het zich konden veroorloven om in silo's te werken, maar de eenvoud en snelheid van de cloud vereist het leren van een flexibele en all-inclusive DevSecOps-benadering, die er idealiter voor zou zorgen dat beveiligingsoverwegingen worden veroorzaakt op een bepaalde cloudinstantie zonder de ontwikkelaar te vertragen.
En toch zijn niet alle organisaties uitgerust om snel een radicaal nieuwe mindset aan te nemen, en deze rotsachtige overgang heeft vaak geleid tot kritische misconfiguraties die vertrekken
het bedrijf kwetsbaar voor aanvallen. In veel gevallen vinden deze verkeerde configuraties plaats tegen een achtergrond van 'huisdier' en 'vee' cloud-implementaties, waarbij het 'huisdier' de goed beveiligde en gesanctioneerde productieomgevingen vertegenwoordigt, en het 'vee' wegwerp- en malafide testomgevingen vertegenwoordigt die vaak zonder veiligheidsoverwegingen worden verspend. De resulterende verkeerde configuraties kunnen variëren van het vergeten van het implementeren van native beveiligingsbesturingselementen, tot het configureren van een testomgeving om openbaar te zijn wanneer dat niet zou moeten, of zelfs het vergeten van de omgeving was bedoeld om vervolgens te worden verwijderd. In dit laatste geval, ontwikkelaars kunnen zelfs laten echte gegevens of referenties in de open lucht, waar ze kunnen worden opgepikt door routine scans van hackers op zoek naar winst te maken op het dark web.

"VERKEERDE CONFIGURATIE VAN CLOUDPLATFORMS IS DE BELANGRIJKSTE BEDREIGING VOOR CLOUDBEVEILIGING."
CROWD RESEARCH PARTNERS

Edge Computing

Op een breed scala van gebieden, de verbeterde rekenkracht die door de cloud heeft een springplank voor de ontwikkeling van nieuwe en innovatieve technologieën.
Edge computing in het bijzonder staat als een van de meest opmerkelijke off-shoots van de cloud, zelfs als het een radicale verschuiving vertegenwoordigt van het verwerken van gegevens in centrale knooppunten - waardoor computerlogica dichter bij de fysieke gegevensbronnen komt om de latentie te verminderen en de bandbreedte te vergroten.
Data-analyse wordt dus steeds meer naar de rand gebracht, waar gedistribueerde sensoren, IoT-

apparaten en zelfs applicaties snelle, real-time beslissingen kunnen nemen, waarbij ze verwerkte gegevens alleen naar de cloud hoeven te sturen wanneer ze klaar zijn om te worden opgeslagen of verder geaggregeerd. Terwijl de cloud kan een achterbank in deze use case, de explosie van edge computing en apparaten in fabrieken, slimme steden en booreilanden blijft de aanval oppervlak waardoor bedreigingen kunnen uiteindelijk hun weg terug naar de centrale cloud uit te breiden.

Onbeveiligde API's

Onbeveiligde API's zijn uitgegroeid tot een van de meest impactvolle verkeerde configuraties in de cloud, die in 2017 zijn opgenomen in de Top 10 OWASP-beveiligingsrisico's voor toepassingen. Api van een toepassing is uiteindelijk de interface naar back-end gegevens, dus elke kwetsbaarheid in foutrespons behandeling zou natuurlijk een aantrekkelijk doelwit voor cybercriminelen met een scala aan motivaties. Net als bij andere verkeerde configuraties, ontwikkelaars werken op de snelheid van digitale business werken vaak niet hand in hand met beveiliging, en kan soms niet harden API's goed genoeg om rekening te houden met mogelijk misbruik - van spoofing toepassingen voor legitieme gebruikers, om codering van de API om ten onrechte te reageren op aanvallers met zeer gevoelige gegevens.

Beperkingen van native beveiligingstools en beveiligingstools van derden

Tegen deze achtergrond van evoluerende bedreigingen hebben CSP's en externe leveranciers een reeks beveiligingstools ontwikkeld om het gedeelte van het gedeelde verantwoordelijkheidsmodel van de klant te helpen verdedigen. Hoewel deze oplossingen een zekere mate van bescherming kunnen bieden, zijn ze over het algemeen slecht uitgerust om zich te verdedigen tegen geavanceerde bedreigingen in de cloud.
CSP-native beveiligingsbesturingselementen
Naast het beveiligen van hun eigen gedeelte van het Responsibility Model, bieden de meeste cloudproviders native oplossingen om klanten te helpen bij het implementeren van elementaire cyberhygiëne in de cloud. Deze kunnen variëren van firewalls, twee-factor authenticatie en IAM tools, tot log monitoring en threat intelligence integraties.

Hoewel deze native controls een goed begin zijn en kunnen bijdragen aan de algemene verdediging van uw organisatie in de dieptestrategie, zijn ze in de praktijk vaak niet voldoende. Aangezien organisaties cloudservices van meerdere providers blijven gebruiken, kunnen native controls niet worden gebruikt om uitgebreide dekking te bieden, omdat ze vaak uitsluitend zijn ontworpen voor de cloudomgeving van de specifieke provider.

De meeste bedrijven die hun workloads migreren naar de cloud maken gebruik van meerdere IaaS-providers, terwijl uit een onderzoek begin 2018 bleek dat het gemiddelde aantal cloud-apps dat in de onderneming wordt gebruikt, is gestegen tot bijna 2.000. Nu 'multi-cloud'-implementaties de norm zijn geworden, is een aanpak van cloudbeveiliging snel achterhaald en neemt de vraag naar provider-agnostische oplossingen toe die het volledige scala aan cloud- en SaaS-omgevingen doorsnijden. Het is ook de moeite waard om te benadrukken dat alle native beveiligingscontroles adequaat moeten worden geïmplementeerd door de klant, die mogelijk niet bekend is met het configureren van deze tools in de cloud. Met een nieuwe bedreiging voor elke dag, traditionele tools ontworpen om bekende bedreigingen ter plaatse zijn niet langer voldoende.

Cloudspecifieke tools van derden

Externe leveranciers zijn ook begonnen met het ontwikkelen van cloud-specifieke beveiligingsoplossingen zoals Cloud Access Security Brokers (CASBs) en Cloud Workload Protection Platforms (CWPPs) om de gaten op te vullen die door native controls zijn achtergelaten. CASBs zijn grotendeels ontworpen om SaaS-toepassingen te beveiligen en bieden functies voor zichtbaarheid van de cloud, DLP en compliance. CWPPs zijn gericht op het dekken van hybride IaaS-omgevingen, het leveren van applicatiebesturingselementen op basis van whitelists, evenals hybride cloudzichtbaarheid en netwerksegmentatiefunctionaliteit binnen containers en workloads.
Casb's en CWP's zijn gespecialiseerd in preventieve controles, naleving en zichtbaarheid binnen het bereik van hun respectieve use cases. Hoewel deze mogelijkheden hun plaats hebben, zullen ze vaak niet om subtiele of gerichte aanvallen te vangen. De meeste leveranciers op dit gebied hebben dit feit erkend, en sommigen hebben geprobeerd om rudimentaire anomalie detectie functionaliteit als een add-on, door de vaststelling van een statische baseline en pre-definiëren goedaardig en kwaadaardig gedrag. Toch kan niet worden verwacht dat deze legacy-aanpak voldoende bescherming biedt tegen geavanceerde aanvallen, zelfs als deze markten
om te rijpen.

EasyComp Cloud

EasyComp Zeeland's cyber AI-technologie biedt een fundamenteel unieke benadering van real-time cyberdefensie in de cloud.

EasyComp Zeeland Cloud is gebaseerd op een basis van onbewaakte machine learning en AI en analyseert rijke gegevensstromen binnen en tussen cloudworkloads en SaaS-toepassingen en leert een normaal 'levenspatroon' voor elke gebruiker, apparaat en container. Door subtiele afwijkingen in gedrag in realtime te correleren, kan EasyComp Zeeland Cloud het volledige scala aan cyberbedreigingen in de cloud herkennen en stoppen, van kwaadwillende insiders en externe aanvallen tot kritieke misconfiguraties

die het bedrijf kunnen blootstellen aan compromissen met een hoog impact in het digitale landgoed.

De kracht van EasyComp Zeeland's technologie ligt in zijn zelflerende aanpak, die niet afhankelijk is van het vooraf definiëren van 'goedaardig' of 'kwaadaardig' gedrag. In plaats daarvan modelleert EasyComp Zeeland Cloud het normale gedrag van gebruikers, containers en apparaten in relatie tot hun verleden, hun peer group en de bredere organisatie, waarbij de berekeningen voortdurend worden herzien in het licht van nieuw bewijs en zwakke indicatoren worden gecorreleerd om een evoluerende maatstaf voor de waarschijnlijkheid van bedreigingen vast te stellen.

EasyComp Zeeland's aanpak is van cruciaal belang in dit nieuwe tijdperk van cloud-gebaseerde cyber-bedreiging, waar insiders met bevoorrechte toegang en externe actoren met admin referenties kunnen vegen door een hele cloud-infrastructuur zonder verrekening alarmen. De cloudprovider kan (en mag niet) worden verwacht dat hij de cloud beveiligt tegen vertrouwde verbindingen, terwijl tools van derden met anomaliedetectiemogelijkheden dit alleen op een botte en platte manier kunnen doen. Door te vertrouwen op vaste leerperioden en vooraf gedefinieerde begrippen van 'goedaardig' en 'kwaadaardig', kunnen deze tools alleen de meest voor de hand liggende bedreigingen. De onbewaakte machine learning en AI van EasyComp Zeeland kunnen daarentegen verder gaan dan wat mensen zich al kennen of zich kunnen voorstellen, en subtiele afwijkingen detecteren die kunnen wijzen op een zich ontwikkelende bedreiging.

In plaats van te vertrouwen op vooraf gedefinieerde regels en beleidsregels, omarmt EasyComp Zeeland Cloud de onzekerheid die inherent is aan de complexe digitale omgeving van vandaag. Alle significante afwijkingen worden gezien en gecorreleerd, wat resulteert in de detectie van echte bedreigingen, zonder overstromingen van valse positieven te veroorzaken.

“EASYCOMP CLOUD WERKT PERFECT VOOR AWS. HET IS LICHTGEWICHT, MAKKELIJK TE GEBRUIKEN, EN MAAKT ONS VEEL COMFORTABELER MET ONZE CLOUD INFRASTRUCTUUR."

EASYCOMP CLOUD VOOR IAAS EN SAAS

EASYCOMP CLOUD KAN EENVOUDIG WORDEN GEÏNTEGREERD MET UW DIVERSE DIGITALE DOMEIN, WAARONDER IAAS-OMGEVINGEN ZOALS AWS EN AZURE, EN SAAS-TOEPASSINGEN ZOALS SALESFORCE, BOX, G SUITE, DROPBOX EN OFFICE 365.

EasyComp Zeeland Antigena: Autonome reactie in de cloud

EasyComp Zeeland's AI detecteert niet alleen, maar kan ook autonoom reageren op in-progress cyberbedreigingen in de cloud. EasyComp Zeeland Antigena, de autonome reactiecapaciteit van het platform, maakt gebruik van kunstmatige intelligentie om gerichte, gemeten actie te ondernemen als reactie op cyberbedreigingen met een hoog vertrouwen – het stoppen van hun verspreiding in realtime en het beveiligingsteam de tijd geven om bij te praten.

De soorten acties die EasyComp Zeeland Antigena kan uitvoeren, zijn afhankelijk van de specifieke cloudomgeving of SaaS-toepassing die wordt gebruikt, zoals blijkt uit de onderstaande lijsten die niet volledig of definitief zijn op alle SaaS- of cloudplatforms.

Om in-progress aanvallen in cloudomgevingen zoals AWS en Azure te neutraliseren, kan EasyComp Zeeland Antigena:

Een virtuele machine beëindigen of de eigenschappen ervan bewerken
Machtigingen voor S3-buckets bewerken in AWS
De programmatische toegang van een gebruiker tijdelijk uitschakelen
Gebruikerswachtwoorden opnieuw instellen om de toegang tot het beheer uit te schakelen
Gebruikersmachtigingen bewerken
Tijdelijk stoppen met het delen van een document

In SaaS-toepassingen zoals Office 365, Salesforce, G-Suite,
en Box, EasyComp Zeeland Antigena kan:

De actieve sessies van een gebruiker doden
Gebruikers tijdelijk uitschakelen
Instellingen voor het delen van bestanden uit bepaalde bestanden en mappen beperken of verwijderen
Een gebruiker beperken om toegang te krijgen tot bepaalde delen van de cloudomgeving
Leden van teams opschorten en zo toegang krijgen tot bepaalde gedeelde bestanden (bijvoorbeeld in Dropbox)

EasyComp Zeeland Threat Visualizer: Volledige zichtbaarheid

De meeste organisaties die infrastructuur en toepassingen migreren naar de cloud worstelen met het migreren van zichtbaarheid en controle. Zelfs beveiligingsteams die native en externe tools goed configureren en implementeren, hebben zelden toegang tot gedetailleerde, realtime zichtbaarheid om continue monitoring te bereiken voor interactieve en gecontextualiseerde bedreigingsonderzoeken.

Om deze zichtbaarheid in uw digitale infrastructuur te bieden, biedt de grafische Threat Visualizer-interface van EasyComp Zeeland één ruit van waaruit afwijkende activiteit in cloudworkloads, SaaS-toepassingen en elders in realtime kan worden gevisualiseerd en onderzocht. De Threat Visualizer is ontworpen voor gebruikers van alle volwassenheidsniveaus, van forensische beveiligingsexperts tot business executives en minder ervaren leden van het IT-team.

Een schat aan informatie kan op verschillende manieren worden opgevraagd en blootgesteld met behulp van de interactieve functies binnen de Threat Visualizer, waaronder een dynamisch dashboard waar gebruikers incidenten kunnen filteren op basis van hun ernstniveau, en een interactieve Play-Back-tool waarmee gebruikers incidenten kunnen afspelen en nul in de real-time context rond elke gebeurtenis.

"MET EASYCOMP ZEELAND CLOUD SCHIJNEN WE EEN ZAKLAMP IN DE DONKERSTE HOEKEN VAN ONS NETWERK."

Scenario's voor implementatie van technologie

Scenario's voor implementatie van technologie

Hybride cloud (IaaS)

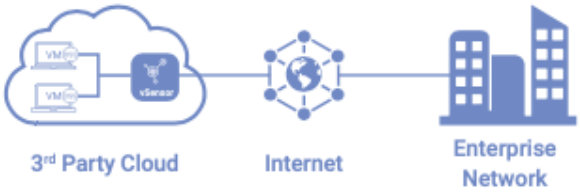
Voor cloud-, edge- en fysieke implementaties worden de lichtgewicht, op host gebaseerde OS-sensoren van EasyComp Zeeland op elk cloudeindpunt geïnstalleerd en geconfigureerd om intelligente kopieën van netwerkverkeer naar een lokale vSensor te verzenden die in dezelfde cloudomgeving wordt geïmplementeerd. De ontvangende vSensor verwerkt de gegevens en voert deze terug naar EasyComp Zeeland-software in de onderneming, die gedrag in de cloud en fysieke omgevingen van de organisatie correleert.
AWS- en Azure-klanten hebben bovendien de de optie om EasyComp Zeeland Connectors te gebruiken om de activiteit van de systeembeheerder te controleren die mogelijk niet zichtbaar is op het niveau van OS-Sensor, zoals aanmeldingen, bestandswijzigingen of gegevensoverdrachten.

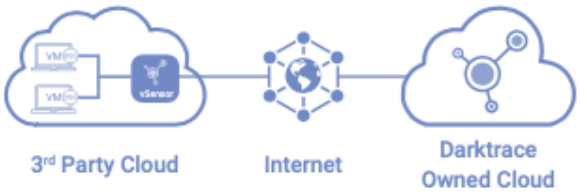
Cloud-only (IaaS)

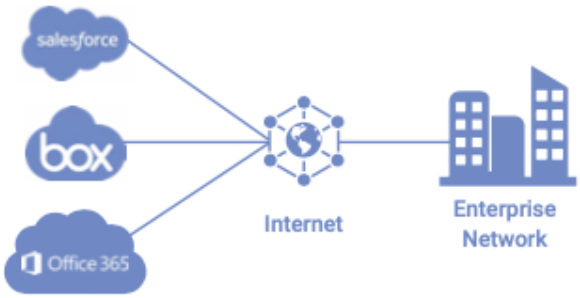
Voor organisaties die hun infrastructuur uitsluitend in de cloud uitvoeren, kan EasyComp Zeeland de implementatie beheren als een speciale service, vSensors en OS-sensoren installeren in de cloudomgeving van de organisatie en gegevens terugvoeren naar een beheerde EasyComp Zeeland-cloudvoor analyse.

Saas

Voor SaaS-implementaties worden EasyComp Zeeland SaaS-connectors op afstand in het bedrijfsnetwerk geïnstalleerd en rechtstreeks via HTTPS-aanvragen verbonden met de beveiligings-API van de SaaS-leverancier. Hierdoor kunnen gebruikersinteracties binnen enkele minuten na het maken door EasyComp Zeeland worden verwerkt en gemonitord, ongeacht of ze nu binnen het netwerk of van externe locaties afkomstig zijn.







Real-World Threat Ontdekkingen

Diefstal van interne gegevens uit de cloud

Een retailer besloot zijn IT-afdeling te herstructureren. Daarbij moesten ze een aantal medewerkers laten gaan. Een van de betrokken medewerkers – een IT-manager – heeft contactgegevens en creditcardnummers uit de klantendatabase gedownload.
EasyComp Zeeland gedetecteerd gegevensoverdrachten
naar een thuisserver via de reguliere gegevensoverdrachtsservice van dat bedrijf. De werknemer was waarschijnlijk van plan om de informatie te verkopen voor een winst.
De database werd bewaard op een cloudservice van derden om flexibel werken mogelijk te maken en hardwarekosten te verlagen. Het bedrijfsmodel van de retailer was sterk gebaseerd op het gebruik van cloudsynchronisatie,
en bestandsoverdrachtdiensten. Deze IT-manager heeft echter laten zien hoe cloudservices kunnen worden misbruikt voor exfiltratie van gegevens met voorkennis.
De marketingafdeling van het bedrijf maakte vaak gebruik van deze cloudservice, maar het was hoogst ongebruikelijk voor een IT-manager om gegevens extern via de cloud te verzenden. EasyComp Zeeland was in staat om dit onderscheid te maken omdat het voortdurend normale activiteit leert voor elke gebruiker en apparaat, en vergelijkt gedrag tussen apparaten om overeenkomsten te identificeren.
EasyComp Zeeland's technologie detecteerde deze lichte afwijking van het normale 'patroon van het leven', waardoor het platform dit bedreigende en subtiele gedrag kon identificeren, hoewel de cloudservice regelmatig werd gebruikt voor legitieme doeleinden.
EasyComp Zeeland ontdekte deze afwijkingen in real time en voorzag het bedrijf van gedetailleerde informatie over de precieze aard van het compromis. De referenties van de werknemer werden ingetrokken en het bedrijf haalde en beveiligde snel de klantgegevens.

Externe aanval op cloudperimeter

Een organisatie voor financiële diensten hostte een aantal kritieke servers op virtuele apparaten in de cloud, waarvan sommige bedoeld waren om openbaar te zijn, en waarvan sommige niet.
Bij het configureren van hun cloudimplementatie lieten ze per ongeluk een belangrijke server blootgesteld aan het internet toen deze achter de firewall moest worden geïsoleerd. Dit kan zijn gebeurd om verschillende redenen, mogelijk als gevolg van een snelle en chaotische migratie, of omdat het beveiligingsteam gewoon niet zo vertrouwd was met de native firewall die door hun CSP.
De blootgestelde server werd voortdurend gebombardeerd door aanvallen van kwaadwillende derden

proberen om toegang te krijgen tot dat apparaat, en via daar, draaien in de cloud en mogelijk terug draaien in het centrum van hun fysieke netwerk. Cruciaal is dat de klant dit niet wist omdat ze geen inzicht hadden in wat er gaande was in hun cloud.
Maar na een snelle installatie ontdekte EasyComp Zeeland al snel dat het apparaat een ongebruikelijke hoeveelheid inkomende verbindingspogingen ontving uit een breed scala van verschillende externe bronnen.
EasyComp Zeeland identificeerde het aanvalspatroon en waarschuwde de klant voor het voortdurende risico, en ze waren in staat om het gat in hun beveiliging af te sluiten en hun cloudperimeter te beveiligen, voordat ze het slachtoffer werden van een meer ernstige Denial of Service-aanval, of voordat deze aanval er daadwerkelijk in was geslaagd om toegang te krijgen en gegevens van daaruit te exfiltreren.
Door hen die zichtbaarheid te geven, was het voor EasyComp Zeeland heel gemakkelijk om hen te helpen snel te begrijpen wat er in de cloud gebeurde. Dit was geen ingewikkeld probleem op te lossen, maar zonder enige zichtbaarheid zouden ze nooit in staat zijn geweest om het te detecteren als het zich ontvouwde.
Cyber AI & EasyComp Zeeland Cloud

Conclusie

Terwijl organisaties steeds meer vertrouwen op cloudservices en SaaS-toepassingen om de bedrijfspraktijken te stroomlijnen, is het bekende paradigma van de netwerkperimeter opgelost, waardoor een poreus en steeds veranderend digitaal landgoed in zijn kielzog blijft.

Hoewel de voordelen van cloud computing ervoor zullen zorgen dat migraties snel blijven, vereisen de unieke beveiligingsuitdagingen die de cloud met zich meebrengt niet alleen een flexibelere mentaliteit, maar ook zelflerende technologieën die kunnen bewegen met de snelheid van cloudimplementaties en subtiele afwijkingen kunnen herkennen die wijzen op een bedreiging, terwijl ze volledige, real-time zichtbaarheid bieden in het digitale bedrijf.

EasyComp Zeeland's wereldleider op het gebied van kunstmatige intelligentie voor cyberbeveiliging maakt het de meest effectieve en bewezen oplossing om ongekende bedreigingen en afwijkende cyberincidenten in de cloud te detecteren. Of het nu gaat om een insiderdreiging, een aanvaller die gevoelige gegevens in testcontainers target of een aanzienlijke misconfiguratie die in de toekomst kan worden benut, de cybertrace van EasyComp Zeeland
AI-platform elimineert blinde vlekken, begrijpt wanneer bedreigingen zich ontwikkelen en helpt uw gegevens te beschermen, waar deze zich ook bevinden.

"EASYCOMP ZEELAND DETECTEERT EN REAGEERT OP BEDREIGINGEN DIE ANDERE TOOLS MISSEN."