real solutions
Haarlem

Acronis
Advanced pacs

Om de bedrijfskritische gegevens van klanten te beschermen, is back-up alleen niet genoeg – klanten hebben een geïntegreerde benadering van cyberbeveiliging nodig. In combinatie met Acronis Cyber Protect Cloud stelt het Advanced Cloud Back-up Pack jou in staat om de Cloudback-upmogelijkheden uit te breiden die jouw klanten nodig hebben om hun gegevens proactief te beschermen. En daarmee kan je zelf ook meer volume maken, tijd besparen en geld verdienen.

Acronis biedt momenteel negen (9) geavanceerde pakketten. Dit zijn Advanced Management, Advanced Security, Advanced Security+EDR, Advanced Email Security, Advanced Backup, Advanced Disaster Recovery, Advanced Data Loss Prevention, Advanced Automation, Advanced File, Sync & Share. Volledige details van deze geavanceerde pakketten hier zijn te vinden.

Een van de genoemde pakketten, Advanced Automation, wordt binnenkort uitgebracht. Later dit jaar horen we daar vanuit Acronis alles over. Als je er nu vragen over hebt, stuur mij dan een e-mail of bel mij rechtstreeks en indien nodig, brengen we je in contact met de juiste support van Acronis.

Enkele voorbeelden van hoe jij je klanten accounts (tenant(s) kunt verrijken met kenmerken en functies van geavanceerde pakketten vind je hieronder en daarmee krijg je ook antwoorden op veel voorkomende vragen.

Ga direct naar

Wil je liever direct contact?

Natuurlijk, we staan voor je klaar!

Neem contact op via

Telefoon MS Teams

of kom gezellig langs in Haarlem voor een persoonlijk gesprek.

real solutions
Haarlem

Acronis
Advanced pacs

Wat we veel horen is dat de tenant alleen gebruik maakt van back-up en geen geavanceerde pakketten heeft ingeschakeld.

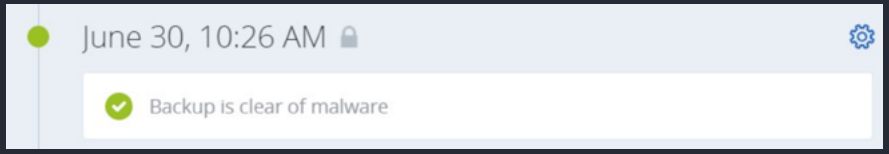
Dit is voornamelijk te wijten aan het feit dat Acronis oplossingen in het verleden alleen een back-up konden maken en niet van factureringsmodus konden wisselen. Je moest andere producten gebruiken voor diensten (patchbeheer, extern bureaublad, ransomware, EDR, monitoring, enz.) die je aan uw klanten aanbood.

Wij adviseren, samen met Acronis om geavanceerde back-up, geavanceerde beveiliging / geavanceerde beveiliging + EDR en geavanceerd noodherstel in te schakelen.

Waarom?

- Door geavanceerde back-uo voor de huurder in te schakelen, heb je de mogelijkheid om off-host gegevensverwerkings-functionaliteit te gebruiken (meer informatie)
- Maak een back-upreplicatieplan om een agent een back-upbestand of een back-uplocatie naar een andere locatie te laten repliceren. Valideer back-ups met behulp van deze methoden: Controlesomverificatie, Uitvoeren als virtuele machine, VM-hartslag en Screenshot-validatie. Back-ups of locaties opschonen op basis van planning en bewaarregels. Conversie naar VM om back-up direct te converteren naar VMware ESXi-, Microsoft Hyper-V-, Scale Computing HC3-, VMware Workstation- of VHDX-bestanden.
- Door geavanceerde beveiliging in te schakelen, heb je de mogelijkheid om een back-upscanplan te maken (meer informatie)

om back-ups op malware te scannen (inclusief ransomware). Op deze manier weet je dat je veilig bestanden/mappen of de hele machine kunt herstellen.



- En door Geavanceerde beveiliging + EDR in te schakelen (die wordt geleverd met alle functies van Geavanceerde beveiliging), kan je gemakkelijk herstel en meer toevoegen wanneer er threads optreden.
- Door Advanced Disaster Recovery in te schakelen, heb je de mogelijkheid om naar de Acronis Cloud over te schakelen en door te gaan wanneer jouw lokale apparaat is gecrasht of niet beschikbaar is. Je hoeft dus geen nieuwe lokale hardware aan te schaffen om een Disaster Recovery-omgeving in te stellen.
- In geval van een calamiteit kan je overschakelen naar de laatste volledige back-up die zich in de Acronis Cloud bevindt. Jow back-upbestand wordt binnen enkele minuten ingericht en opgestart, waarna het beschikbaar is voor gebruik met hetzelfde IP-adres. Jouw endpoints merken niet dat het device nu in de Acronis Cloud draait.
- Als je Advanced Security+EDR en Advanced Disaster Recovery hebt ingeschakeld voor de tenant, kan je na een aanval zelfs een Disaster Recovery-failover starten, waarin Acronis echt uniek is in de branche.

real solutions
Haarlem

Acronis
Advanced pacs

Je gebruikt al een Remote Desktop-applicatie

Dan stelt Acronis voor om Geavanceerd beheer in te schakelen, waarna je Patchbeheer, Cyber Scripting, op 'Machine Intelligence' gebaseerde monitoring, Fail safe patching en Remote Desktop en assistentie ook kunt gaan gebruiken.

Het overnemen van het (actieve) scherm van een device is onderdeel van het Advanced Management pack naast de hierboven genoemde extra functionaliteit. Acronis gebruikt één agent, waardoor het eenvoudig is om een Windows-, Linux- of MacOS-apparaat te ondersteunen (meer informatie), zelfs als je wilt geen RDP gebruiken

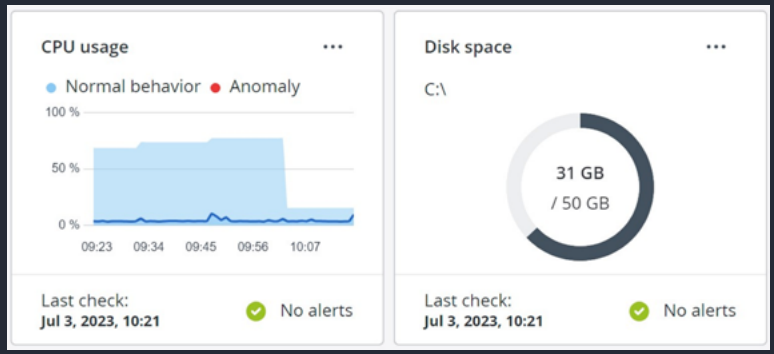
Je wilt eindpunten controleren op schijfruimte

We horen regelmatig van klanten dat het monitoren van schijfruimte, bestandsgrootte en map-grootte is wat ze minimaal willen zien.

Acronis adviseert dan om Geavanceerd beheer in te schakelen. Daarmee heb je de mogelijkheid om elk van de 24 monitoren die momenteel beschikbaar zijn te gebruiken. Dat geeft een duidelijk overzicht.

- Vier (4) daarvan kunnen gratis worden gebruikt. Dit zijn schijfruimte, hardware-wijzigingen, laatste systeemherstart en bestands- en map-grootte.
- De overige twintig (20) opties (bekijk hier) maken deel uit van Advanced management

Dit alles wordt gedaan door een overzichtsplan of Monitoringplan te maken en dit toe te passen op een apparaat. Dit kan op partnerniveau worden gedaan, zodat het plan eenvoudig kan worden geïmplementeerd op elk van de apparaten in de 'tenants' van de klant.



Je hebt al een beveiligingsoplossing

Bij gebruik van een ander beveiligingsplatform komt dit ook met een extra agent die op elk eindpunt moet worden geïnstalleerd, met extra certificering en een andere beheerconsole.

Het alternatief is dus om Advanced Security of Advanced Security+EDR te gaan gebruiken (of toe te voegen), zodat je slechts één agent hoeft te installeren en je de functionaliteit kunt combineren die al beschikbaar is in het Cyber Protect Cloud-platform.

Je kan back-upbestanden scannen op malware en er zijn herstelopties beschikbaar via dezelfde beheerconsole die je al eerder hebt gebruikt.

real solutions
Haarlem

Acronis
Advanced pacs

De afbeelding laat zien welke functionaliteit beschikbaar is bij elke stap.

Cyber Protect Cloud biedt volledige bescherming binnen het NIST-framework met een uniform platform.

Door meer van deze mogelijkheden aan jouw omgeving toe te voegen, kan je eenvoudig stijgen in je Acronis partner status, waardoor jouw totale kosten dalen.

Je gebruikt MS O365-back-up in een factureringsmodus per werkbelasting

Verstandig dat je al gebruik maakt van de Acronis MS-O365-back-upoplossing, waarmee je een uitgebreide retentieperiode.

voor back-ups hebt in plaats van alleen de 30 dagen die Microsoft momenteel nog aanbiedt.

Wij adviseren om Advanced Email Security aan de tenant toe te voegen om inkomend en uitgaand e-mailverkeer te kunnen scannen. Daarmee blokkeer je dus e-mailbedreigingen, waaronder spam, phishing, Business Email Compromise (BEC), account Takeover (ATO), malware, Advanced Persistent Threats (APT's) en zero-days, voordat deze de mailboxen van eindgebruikers bereiken. Extra veilig dus en het beste advies voor je klant.

Je kan zelfs het licentiemodel van elk eindpunt wijzigen van een Business Premium-licentie naar een E3- of E5-licentie, waardoor jouw marge nog meer verbetert en je niet betaalt voor een functionaliteit die je niet gebruikt. Dit biedt extra optimalisatie van jouw bedrijfsvoering en van de klant.

Je kan maar één keer per dag een back-up van MS-O365 maken

Wanneer je Advanced Backup - Microsoft 365 gaat toevoegen aan de tenant, wordt het mogelijk om tot zes (6) keer per dag een back-up uit te voeren! (meer informatie) Het voegt ook Groepsbeheer toe (meer informatie) waarmee je ook een Azure AD-groep kunt selecteren om een Cloud-toepassingsplan te maken.
Echt een aanrader!

Waar kan ik zien waarom een MS-O365 SEAT wordt geteld?

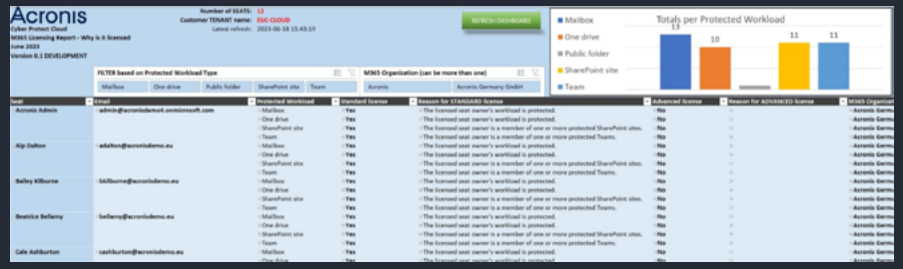
Vanuit de klanttenant heb je de mogelijkheid om het "Microsoft 365 seats-licentierapport" te downloaden. Het formaat is erg eenvoudig, wat betekent dat het kan worden verbeterd door er

real solutions
Haarlem

Acronis
Advanced pacs

opmaak en grafieken aan toe te voegen. Je kan dat gemakkelijk zelf doen met behulp van Power Query en Power Pivot.

Als je niet weet hoe je dat moet doen, dan heeft Acronis een spreadsheet beschikbaar, die je via ons ook kan bemachtigen. (Stuur even een e-mail). Deze importeert het M365-licentierapport en toont de gegevens in een andere weergave met de mogelijkheid om ze te filteren op type werklast. Hier is een screenshot hoe het eruit zou kunnen zien:



Volgt Acronis het NIST-framework?

JA!

Vanuit het Acronis platform kan je bedrijfscontinuïteit bieden binnen het hele NIST-framework

- **Identificeer:** Je moet weten wat je hebt om het volledig te beschermen en het te onderzoeken. Het platform bevat tools voor inventarisatie en gegevensclassificatie om aanvalsoppervlakken beter te begrijpen.
- **Beschermen:** Dicht beveiligingsproblemen met behulp van de feed. Met bedreigingsinformatie, forensische inzichten en native geïntegreerde tools in het bredere Acronis-platform, zoals gegevensbeschermingskaarten, patchbeheer, het blokkeren van geanalyseerde aanvallen en beleidsbeheer.
- **Detecteren:** Continue monitoring van beveiliging gerelateerde gebeurtenissen met behulp van geautomatiseerde gedrags- en handtekening gebaseerde engines, URL-filtering, een feed met informatie over opkomende bedreigingen, gebeurteniscorrelatie en MITRE ATT&CK®.
- **Reageren:** Onderzoek verdachte activiteiten en voer vervolgaudits uit met behulp van een veilige, externe verbinding met werklasten of bekijk automatisch opgeslagen forensische gegevens in back-ups. Herstel vervolgens via isolatie, proces beëindiging, quarantaine en specifieke terug te draaien aanvallen.
- **Herstel:** Zorg ervoor dat systemen, eindpuntgegevens en de klantactiviteiten werken met de volledig geïntegreerde oplossingen voor back-up en noodherstel. Acronis is marktleider op dit gebied.

Kan Acronis ook worden geïntegreerd met andere applicaties?

Acronis werkt continue aan het verbeteren en uitbreiden van het totale aantal beschikbare integraties. De huidige lijst is hier te vinden of in het menu INTEGRATIES nadat je bent ingelogd bij jouw partnertenant. In de komende maanden verwachten we dat Acronis nog meer integraties zal aankondigen. Blijf alert via jouw partnerportal en bij vragen, neem contact op met Real Solutions Haarlem of Acronis zelf.