Versneld herstel na ransomware met Dell PowerProtect Backup Services

Herstel na ransomware in uren, niet dagen

Belangrijke kenmerken

Ransomware-aanvallen komen steeds vaker voor en worden steeds geavanceerder en duurder

- Onvermogen om snel niet-geïnfecteerde back-ups of bestanden te identificeren en te herstellen
- De infectie verspreidt zich en treedt opnieuw op door hersteldata
- Dataverlies, onvermogen om een volledige dataset te herstellen
- Problemen bij het coördineren van de indeling van incidentrespons
- Vraagt om snellere RPO/RTO-tijden
- Kostbare downtime voor bedrijven die leidt tot verlies van omzet en schade aan de merkreputatie
- Wettelijke boetes voor onvoldoende databescherming

Uitdaging

Ransomware is een ernstige bedreiging voor elke onderneming. Cyberaanvallen komen vaak voor en kunnen catastrofale schade veroorzaken. 79% van de organisaties maakt zich zorgen over een verstorende gebeurtenis in de komende twaalf maanden1. Bedrijven die hun data verliezen, lopen het risico om na een ramp failliet te gaan. Ransomware-aanvallen vinden niet alleen vaker plaats, maar zijn ook technologisch geavanceerder en duurder geworden.

De oplossing

Snel en betrouwbaar herstel elimineert elke reden om zelfs maar te denken aan het betalen van losgeld. Wanneer een beveiligingsincident of cyberaanval plaatsvindt, moeten organisaties de schaderadius en hoofdoorzaak begrijpen voordat ze kunnen herstellen. Met onberispelijke, air-gapped snapshots van workloads en virtuele machines die 24/7 beschikbaar zijn, continue bewaking van gebruikers- en data-afwijkingen, integratie met beveiligingstools en geautomatiseerd herstel van schone data, kunt u uw beveiligingsmentaliteit verbeteren en een verwoestende beproeving omzetten in een overleefbaar incident.

De mogelijkheden

Voor alle workloads:

• Zorg ervoor dat onveranderlijke, air-gapped back-ups 24/7 beschikbaar zijn

• Herstel schone data on-premise of in de cloud met RPO/RTO van uren, niet dagen of weken

• MDDR-service (Managed Data Detection and Response) biedt 24x7x365 realtime bewaking van back-upomgevingen

• Wanneer u workloads en VM's in elke AWS-regio/account herstelt met data van uw productieorganisatie en er veel kopieën van maakt en deze op meerdere plaatsen opslaat, loopt uw organisatie grote risico's.

Versneld herstel bij ransomware voor belangrijke workloads:

• Bewaak en detecteer afwijkingen proactief met op ML gebaseerde algoritmen

• Organiseer reactie- en herstelactiviteiten via SIEM- en SOAR-integraties

• Scan snapshots op malware vóór herstel en verwijder geïnfecteerde snapshots en bestanden uit back-ups

• Herstel automatisch de meest recente schone versie van elk bestand in een opgegeven tijdsbestek van een gouden snapshot

Bescherming

De eerste stap in het voorkomen van schade door ransomware is het waarborgen van een air-gapped en onveranderlijke kopie van uw data. Dell PowerProtect Backup Services is gebouwd op een zeer veerkrachtige cloudinfrastructuur en maakt het onmogelijk voor ransomware om back-updata te versleutelen. Zero Trust-architectuur, inclusief meervoudige verificatie, envelopversleuteling en afzonderlijke accounttoegang, zorgt ervoor dat ransomware geen gecompromitteerde primaire omgevingsreferenties kan gebruiken om de back-upomgeving of -data te saboteren. Tot slot bieden functies voor het voorkomen van overtollige verwijdering en soft-delete (prullenbak) een extra beveiligingslaag om back-ups te beschermen tegen verwijdering.

Detectie

Door zo snel mogelijk een ransomware-aanval te detecteren, kunnen incidentresponsteams worden geholpen en kan verspreiding van infectie worden voorkomen. De module voor versneld herstel bij ransomware van Dell PowerProtect Backup Services biedt een beveiligingscommandocentrum om de staat van uw back-upomgeving te bewaken. Met toegangsinzichten en anomaliedetectie kunt u snel ongebruikelijke activiteiten in uw omgeving en data identificeren. Bekijk de locatie-, identiteits- en activiteitsgegevens voor alle toegangspogingen door gebruikers en API's. Detecteer afwijkingen met bedrijfseigen ML-algoritmen die waarschuwingen geven voor ongebruikelijke data-activiteit (bijv. verwijdering, versleuteling, enz.). Het algoritme leert de patronen voor uw specifieke back-upomgeving, zodat er geen regels hoeven te worden ingesteld of afgestemd. Het maakt ook gebruik van op entropie gebaseerde inzichten om vals-positieven te verminderen

Respons

Wanneer een beveiligings- of IT-analist een verdachte gebeurtenis detecteert, of erger nog, bevestigt dat er een ransomware-incident heeft plaatsgevonden, wordt de responssnelheid van cruciaal belang. Hoewel er veel waardevolle beveiligingstools voor primaire omgevingen zijn die voor detectie- en responsorganisatie kunnen worden gebruikt, verbeteren analyses en wijzigingslogboekdata van secundaire data (back-upsystemen) onderzoek, respons en forensische activiteiten. De module voor versneld herstel bij ransomware van Dell PowerProtect Backup Services biedt robuuste kant-en-klare API-integraties waardoor u de oplossing eenvoudig in uw algehele beveiligingscosysteem kunt invoegen. Het organiseren van responsactiviteiten met behulp van SIEM- en SOAR-oplossingen kan uw gemiddelde reactietijd (MTTR) drastisch verlagen door automatisch acties uit te voeren zoals het in quarantaine plaatsen van geïnfecteerde systemen of snapshots of het scannen van back-ups voor IOC's op basis van een vooraf bepaald ransomwareplaybook.

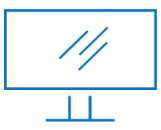
Terugwinnen

Na de initiële responsfase volgt het harde werk van herstel. Voor veel bedrijven is dit een handmatig en tijdrovend proces. De verblijftijd voor kwaadwillende actoren en ransomware kan variëren van weken tot maanden, waardoor het moeilijk is om te weten hoe ver terug moet worden gegaan om schone data te vinden. Zelfs nadat de beste

snapshot is geïdentificeerd, kan verborgen malware leiden tot een nieuwe infectie. Toch is een herstelpunt van 2 weken geleden niet acceptabel voor de meeste zakelijke gebruikers. Toch is het vinden en valideren van recentere data na een ransomware-incident handmatig, vervelend en vaak onoverkomelijk.

Dell PowerProtect Backup Services verlicht deze last met een effectieve back-uparchitectuur en geautomatiseerde tools om herstel te versnellen. Het Dell PowerProtect Backup Services cloudplatform maakt rechtstreeks back-ups van workloads naar de cloud, klaar voor onmiddellijk herstel in het geval van een ransomware-aanval.

Met de versnelde module voor versneld herstel bij ransomware kunt u vol vertrouwen herstellen door de hygiëne van hersteldata te garanderen. U kunt snapshots scannen op malware en IOC's met behulp van ingebouwde antivirusdetectie of met behulp van dreigingsinformatie uit uw eigen forensische onderzoeken of bedreigingen van informatiefeeds. Door snapshots vóór herstel te scannen, voorkomt u een nieuwe infectie.



Meer informatie over PowerProtect Backup Services

Contact met een Dell Technologies expert