Recuperação acelerada de ransomware com o Dell PowerProtect Backup Services

Recupere-se do ransomware em horas, não em dias

Principais Recursos

Os ataques de ransomware estão se tornando mais frequentes, avançados e caros

- Incapacidade de identificar e restaurar rapidamente backups ou arquivos não infectados
- Contaminação espalhada e reinfectada a partir dos dados de recuperação
- Perda de dados, incapacidade de recuperar um conjunto completo de dados
- Dificuldades para coordenar a orquestração da resposta a incidentes
- Exigências de tempos mais rápidos de RPO/RTO
- Tempo de inatividade comercial dispendioso que leva à perda de receita e danos à reputação da marca
- Multas legais e regulamentares decorrentes da proteção inadequada dos dados

O desafio

O ransomware é uma ameaça séria para todas as empresas. Os ataques cibernéticos ocorrem com frequência e podem causar danos catastróficos. 79% das organizações estão preocupadas com a possibilidade de sofrer um evento disruptivo nos próximos 12 meses1. As empresas que perdem seus dados correm o risco de declarar falência após um desastre. Os ataques de ransomware não só estão ocorrendo com mais frequência, mas também se tornaram mais avançados tecnologicamente e mais caros.

A solução

A recuperação rápida e confiável elimina qualquer motivo para sequer pensar em pagar um resgate. No entanto, quando ocorre um incidente de segurança ou um ataque cibernético, as organizações precisam entender o raio de impacto e a causa raiz antes da recuperação. Com snapshots impecáveis com air-gap de cargas de trabalho e máquinas virtuais disponíveis 24 horas por dia, 7 dias por semana, monitoramento contínuo de anomalias de usuários e dados, integração com ferramentas de segurança e recuperação automatizada de dados limpos, você pode fortalecer sua postura de segurança e transformar uma situação devastadora em um incidente superável.

Os recursos

Para todas as cargas de trabalho:

• Verifique se você tem backups imutáveis e com air-gap disponíveis 24 horas por dia, 7 dias por semana

• Recupere dados limpos no local ou na nuvem com RPO/RTO de horas, e não de dias ou semanas

• O serviço Managed Data Detection and Response (MDDR) oferece monitoramento em tempo real 24x7x365 dos ambientes de backup

• Se você restaurar cargas de trabalho e VMs em qualquer região/conta da AWS usando dados da sua organização de produção e criar muitas cópias deles, armazenando-os em vários locais, estará colocando sua organização em grande risco.

Recuperação acelerada de ransomware para cargas de trabalho importantes:

• Monitore e detecte proativamente anomalias com algoritmos baseados em ML

• Orquestre atividades de resposta e recuperação por meio de integrações de SIEM e SOAR

• Verifique se há malware nos cs antes da recuperação e exclua snapshots e arquivos infectados dos backups

• Recupere automaticamente a versão limpa mais recente de cada arquivo em um período especificado a partir de um snapshot de alta qualidade

Proteção

A primeira etapa para evitar danos causados por ransomware é garantir que você tenha uma cópia imutável e com air-gap dos dados. Desenvolvido em uma infraestrutura em nuvem altamente resiliente, o Dell PowerProtect Backup Services torna impossível que o ransomware criptografe os dados de backup. A arquitetura Zero Trust, incluindo autenticação baseada em vários fatores, criptografia de envelope e acesso separado por contas, garante que o ransomware não possa usar credenciais comprometidas do ambiente primário para adulterar o ambiente ou os dados de backup. Por fim, os recursos de prevenção de exclusão excessiva e exclusão suave (lixeira) oferecem uma camada adicional de segurança para proteger os backups contra exclusão.

Detecção

A detecção de um ataque de ransomware o mais rápido possível pode ajudar as equipes de resposta a incidentes e evitar a disseminação da contaminação. O módulo de recuperação acelerada de ransomware do Dell PowerProtect Backup Services oferece um centro de comando de segurança para monitorar a postura do ambiente de backup. Com insights de acesso e detecção de anomalias, você pode identificar rapidamente atividades incomuns em seu ambiente e dados. Veja o local, a identidade e as informações de atividade de todas as tentativas de acesso por usuários e APIs. Detecte anomalias com algoritmos proprietários de ML que emitem alertas sobre atividades incomuns de dados (por exemplo, exclusão, criptografia etc.). O algoritmo aprende os padrões de seu ambiente de backup específico, portanto, não requer nenhuma configuração ou ajuste de regras. Ele também usa insights baseados em entropia para reduzir os falsos positivos

Resposta

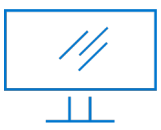
Quando um analista de segurança ou de TI detecta um evento suspeito — ou, pior, confirma a ocorrência de um incidente de ransomware — a rapidez na resposta se torna crucial. Embora existam muitas ferramentas valiosas de segurança de ambiente primário que podem ser usadas para orquestração de detecção e resposta, a lógica analítica e os dados de registro de alterações de dados secundários (sistemas de backup) melhoram as atividades de investigação, resposta e perícia. O módulo de recuperação acelerada de ransomware do Dell PowerProtect Backup Services oferece integrações robustas de API prontas para uso que facilitam a adequação da solução ao seu ecossistema geral de segurança. A orquestração de atividades de resposta usando soluções SIEM e SOAR pode reduzir significativamente o tempo médio de resposta (MTTR), concluindo de forma automática ações como a quarentena de sistemas ou snapshots infectados ou a verificação de backups para IOCs com base em um guia estratégico predeterminado de ransomware.

Recovery

Após a fase de resposta inicial, vem o trabalho árduo de recuperação. Para muitas empresas, esse é um processo manual e demorado. O tempo de permanência dos agentes mal-intencionados e do ransomware pode variar de semanas a meses, o que dificulta saber o quanto é preciso voltar para encontrar dados limpos. Mesmo depois que o melhor snapshot é identificado, o malware oculto pode causar reinfecção. No entanto, um ponto de recuperação de duas semanas atrás não é aceitável para a maioria dos usuários empresariais. Mesmo assim, encontrar e validar dados mais recentes após um incidente de ransomware é um processo manual, tedioso e frequentemente insuperável.

O Dell PowerProtect Backup Services alivia essa carga com uma arquitetura de backup eficaz e ferramentas automatizadas para acelerar a recuperação. A plataforma de nuvem do Dell PowerProtect Backup Services faz backup de cargas de trabalho diretamente na nuvem, pronta para recuperação imediata no caso de um ataque de ransomware.

O módulo de recuperação acelerada de ransomware permite que você se recupere com confiança, garantindo a higiene dos dados de recuperação. Você pode verificar os snapshots em busca de malware e IOCs usando um antivírus integrado ou a inteligência contra ameaças de suas próprias investigações forenses ou feeds de inteligência contra ameaças. A varredura de snapshots antes da recuperação elimina a reinfecção.



Saiba mais sobre o PowerProtect Backup Services

Contato um especialista da Dell Technologies