★★★★★

Appliance de Backup em Camadas da ExaGrid

Backups mais rápidos

Recuperações mais rápidas

Expansão sem igual e econômica

Segurança abrangente e recuperação de ransomware

Appliance de Backup em Camadas da ExaGrid

Retention Time-Lock para recuperação de ransomware

Os ataques de ransomware estão em ascensão, tornando-se disruptivos e potencialmente muito custosos para as empresas. Não importa quão meticulosamente uma organização siga as melhores práticas para proteger dados valiosos, os invasores parecem estar um passo à frente. Eles criptografam maliciosamente os dados primários, assumem o controle do aplicativo de backup e excluem os dados de backup.

A proteção contra ransomware é uma preocupação principal para as organizações hoje em dia. O ExaGrid oferece uma abordagem única para garantir que os invasores não possam comprometer os dados de backup.

O desafio é como proteger os dados de backup para que não sejam excluídos e, ao mesmo tempo, permitir que os backups retidos sejam eliminados quando os pontos de retenção forem atingidos. Se você bloquear todos os dados de retenção, não será possível excluir os pontos de retenção e os custos de armazenamento ficarão insustentáveis. Ao permitir que os pontos de retenção sejam excluídos para salvar o armazenamento, você deixará o sistema aberto para que os hackers excluam todos os dados.

A abordagem única do ExaGrid é chamada de bloqueio de tempo de retenção ou Retention Time-Lock (RTL). Ela impede que os agentes de ameaças/hackers excluam os backups e permite que os pontos de retenção sejam eliminados. O resultado é uma potente solução de proteção e recuperação de dados a um custo muito baixo de armazenamento.

ExaGrid é o Appliance de Backup em Camadas com uma área em disco Landing Zone de front-end e um Repository Tier separado que contém todos os dados de retenção. Os dados são gravados diretamente na área em disco Landing Zone do ExaGrid que é "voltada para a rede". Então, ele é direcionado para um repositório de retenção de longo prazo "não voltado para a rede", onde é armazenado como objetos de dados desduplicados para reduzir o custo de armazenamento de dados de retenção de longo prazo. À medida que os dados são armazenados no Repository Tier, eles são desduplicados e armazenados em uma série de objetos e metadados. Assim como acontece com outros sistemas de armazenamento de objetos, os objetos e metadados do ExaGrid nunca mudam, permitindo apenas a criação de novos objetos ou a exclusão de objetos antigos quando a retenção é alcançada.

A abordagem do ExaGrid ao ransomware permite que as organizações configurem um período de bloqueio de tempo que rege o processamento de quaisquer solicitações de exclusão no Repository Tier, uma vez que essa camada não está voltada para a rede e não está acessível a hackers. A combinação de uma camada não voltada para a rede, uma exclusão atrasada por um período de tempo e objetos que nunca mudam são os elementos da solução Retention Time-Lock da ExaGrid. Por exemplo, se o período de bloqueio de tempo para o Repository Tier estiver definido como 10 dias, então, quando as solicitações de exclusão forem enviadas para o ExaGrid a partir de um aplicativo de backup que foi comprometido ou de um CIFS ou de outros protocolos de comunicação hackeados, os dados no Repository Tier ficarão bloqueados por até 10 dias contra qualquer exclusão. Os dados na Landing Zone serão excluídos ou criptografados, no entanto, os dados no Repository Tier não serão excluídos mediante solicitação externa para o período de tempo configurado. Quando um ataque de ransomware é identificado, basta colocar o sistema ExaGrid em um novo modo de recuperação e, em seguida, restaurar todos e quaisquer dados de backup para o armazenamento primário. O período de bloqueio de tempo é separado e adicional aos dias, semanas, meses e anos ou retenção que forem definidos pelo aplicativo de backup e armazenados pelo ExaGrid no repositório de retenção.

A solução fornece um bloqueio de retenção, mas apenas por um período de tempo ajustável, uma vez que atrasa as exclusões. A ExaGrid optou por não implementar o Retention Time-Lock para sempre porque o custo do armazenamento seria incontrolável. O ExaGrid já tem a retenção de backup de longo prazo, então seria redundante ter um armazenamento separado com bloqueio de retenção. A política padrão de 10 dias para exclusões atrasadas ocupa apenas 10% a mais do espaço de armazenamento. O ExaGrid permite o atraso de exclusões de 1 dia a 30 dias.

Processo de recuperação – Cinco etapas fáceis

- Invocar o modo de recuperação
  - O relógio do Retention Time-Lock é interrompido com todas as exclusões colocadas em espera indefinidamente até que a operação de recuperação de dados esteja concluída
- Entre em contato com o engenheiro de suporte ao cliente da ExaGrid de nível 2 atribuído à conta
  - O administrador de backup pode realizar a recuperação usando a GUI do ExaGrid, mas como isso não é uma operação comum, sugerimos entrar em contato com o suporte ao cliente da ExaGrid
- Determine a hora do evento para que você possa planejar a restauração
- Determine qual backup no ExaGrid concluiu a desduplicação antes do evento
- Execute a restauração desse backup usando o aplicativo de backup

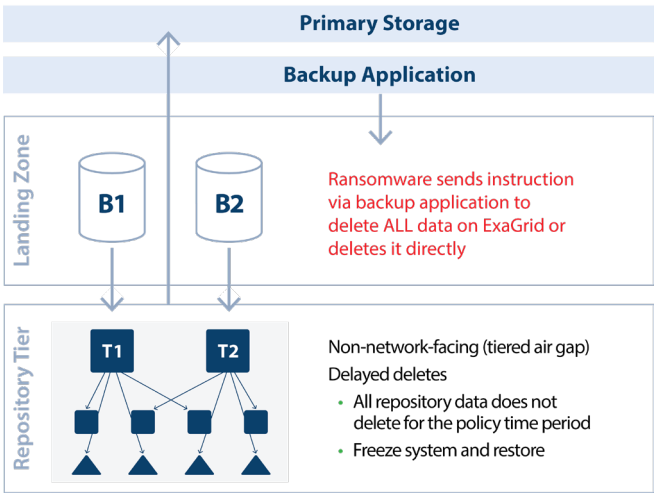
As vantagens do ExaGrid são:

- Gerencie um único sistema em vez de vários sistemas para armazenamento de backup e recuperação de ransomware
- Segundo nível de retenção exclusivo que só é visível para o software ExaGrid e não para a rede
- Os dados não são excluídos, pois as solicitações de exclusão são atrasadas e, portanto, prontas para se recuperar após um ataque de ransomware
- Semanalmente, mensalmente, anualmente e outras eliminações ainda ocorrem para manter os custos de armazenamento de acordo com os períodos de retenção
- A política padrão de 10 dias para exclusões atrasadas ocupa apenas 5% a 10% a mais do espaço de armazenamento
- O armazenamento não cresce para sempre e permanece dentro do período de retenção do backup definido para manter os custos de armazenamento baixos
- Todos os dados de retenção (backups mais recentes e toda a retenção) são preservados e não são excluídos

Exemplos de cenários

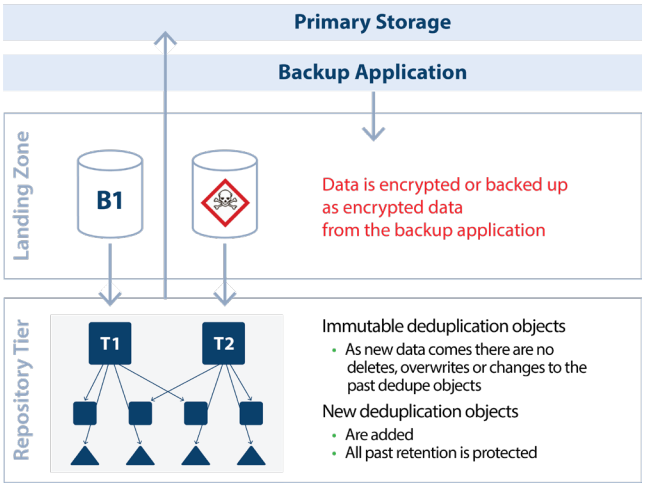
- Os dados são excluídos da área em disco Landing Zone do ExaGrid através do aplicativo de backup ou hackeando o protocolo de comunicação. Como os dados do nível de retenção têm um bloqueio de tempo de exclusão atrasado, os objetos ainda estão intactos e disponíveis para restauração. Quando o evento ransomware é detectado, basta colocar o ExaGrid em um novo modo de recuperação e restauração. Você tem o mesmo tempo para detectar o ataque de ransomware quanto o tempo de bloqueio definido no ExaGrid. Se você definiu o tempo de bloqueio por 10 dias, então você terá 10 dias para detectar o ataque de ransomware e colocar o sistema ExaGrid no novo modo de recuperação para restaurar dados.

Deletion Protection of Backup Data on ExaGrid



- Os dados são criptografados na área em disco Landing Zone do ExaGrid ou são criptografados no armazenamento primário e armazenados em backup no ExaGrid, de modo que o ExaGrid tenha dados criptografados na Landing Zone e os desduplique no Repository Tier. Os dados na Landing Zone são criptografados. No entanto, todos os objetos de dados previamente desduplicados nunca mudam (imutáveis), então eles nunca são afetados pelos dados criptografados recém-chegados. O ExaGrid tem todos os backups anteriores antes do ataque de ransomware que podem ser restaurados imediatamente. Além de poder recuperar do backup desduplicado mais recente, o sistema ainda mantém todos os dados de backup de acordo com os requisitos de retenção.

Encryption Protection of Backup Data on ExaGrid



Caraterísticas:

- Quaisquer solicitações de exclusão são atrasadas pelo número de dias na política de proteção
- Os dados criptografados gravados no ExaGrid não excluem nem alteram os backups anteriores no repositório
- Os dados da Landing Zone que são criptografados não excluem nem alteram os backups anteriores no repositório
- Defina a exclusão atrasada em incrementos de 1 dia, de 0 a 30 dias
- Protege contra a perda de todo e qualquer backup retido, incluindo os mensais e anuais
- A autenticação de dois fatores (2FA) protege as alterações na configuração do Time-Lock
  - Apenas a função Security Officer tem permissão para aprovar alterações na configuração do Time-Lock
  - A autenticação de dois fatores (2FA) com login/senha e QR code gerado pelo sistema protege todas as contas
- Senha separada para o site principal versus o segundo site ExaGrid
- Funções e senhas separadas da equipe de backup e da equipe de segurança
- **Alarme de exclusão**
  - Alarme de exclusão grande: Um valor pode ser definido como um limite pelo administrador de backup (o padrão é 50%), e se uma exclusão for superior ao limite, o sistema emitirá um alarme, e apenas a função Admin pode apagar este alarme.
  - Um limite pode ser configurado por compartilhamento individual com base no padrão de backup. (O valor padrão é 50% para cada compartilhamento). Quando uma solicitação de exclusão chegar ao sistema, o sistema ExaGrid honrará a solicitação e excluirá os dados. Se o RTL estiver ativado, os dados serão mantidos para a política de RTL (para o número de dias definido pela organização). Quando o RTL estiver ativado, as organizações poderão recuperar os dados usando a Point-in-Time-Recovery (PITR).
  - Se uma organização receber um alarme falso positivo frequentemente, a função Admin poderá ajustar o valor de limite de 1% a 99% para evitar mais alarmes falsos.
- Alarme de mudança da relação de desduplicação de dados
  - Se o armazenamento primário for criptografado e os dados forem enviados para o ExaGrid através do aplicativo de backup ou se o agente de ameaças criptografar os dados na Landing Zone do ExaGrid, o ExaGrid verá uma queda significativa na taxa de desduplicação sendo alcançada e enviará um alarme. Os dados no Repository Tier permanecem protegidos.

United States 100 Campus Drive / Marlborough, MA 01752 / (800) 868-6985
United Kingdom 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapore 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

exagrid.com

ExaGrid reserves the right to change specifications or other product information without notice. ExaGrid and the ExaGrid logo are trademarks of ExaGrid Systems, Inc. All other trademarks are the property of their respective holders. ©2024 ExaGrid Systems, Inc. All rights reserved.