

# Proteção das imagens médicas do seu paciente

O Superna Eyeglass® Ransomware Defender ajuda a manter imagens médicas protegidas de criminosos cibernéticos

## Como manter os dados de paciente seguros



- O Dell EMC PowerScale é uma plataforma confiável na área da saúde para armazenamento e arquivamento de imagens médicas
- O PowerScale tem recursos de segurança de dados integrados que ajudam a proteger os dados dos pacientes
- A Superna, parceira de confiança da Dell Technologies, pode ajudar a proteger os dados contra ataques de ransomware
- O Superna Eyeglass® Ransomware Defender utiliza a tecnologia integrada de snapshot, API e replicação do PowerScale para proteger os dados
- O Superna Eyeglass® Ransomware Defender auxilia antes, durante e depois de um ataque cibernético, fornecendo assistência ao longo do incidente
- O Eyeglass® Ransomware Defender da Superna protege os dados em vigor e oferece proteção dos investimentos com recursos de automação de air gap integrados
- Os serviços da Faction no Dell EMC PowerScale permitem que o local de recuperação de desastres e/ou o cluster do air gap sejam externos ou na nuvem.

## As informações do paciente estão sob ataque

A área da saúde está passando por uma explosão de dados. De acordo com a IDC, os dados da área da saúde em breve alcançarão o nível de 4 ZB, ultrapassando 10 ZB em 2025. Embora as instituições da área da saúde gerenciem menos do que a média do setor, elas precisam manter os dados por 25% mais tempo<sup>1</sup>. Isso significa que todas as informações de pacientes, incluindo imagens e verificações em PACS ou VNA, devem ser armazenadas e protegidas contra criminosos cibernéticos.

Recentemente, a área da saúde sofreu alguns ataques quando criminosos encontraram maneiras exclusivas de atingir provedores de saúde com ataques de phishing, fraudes cibernéticas ou ransomware, que colocam toda a instituição e seus dados em risco. Esses tipos de ataque estão em ascensão desde 2020, com 28% deles classificados como ransomware<sup>2</sup>. No entanto, uma pesquisa recente da IDC sugere que apenas 60% das organizações da área da saúde se consideraram preparadas para lidar com o aumento de dados e os requisitos de segurança em torno dele<sup>1</sup>. Com cada vez mais imagens médicas sendo gerenciadas por PACS, como microscopia digital e ultrassom à beira do leito, manter esses dados protegidos nunca foi tão importante.

Ataques cibernéticos causam tempo de inatividade, danos na reputação e uma queda na qualidade dos cuidados prestados.

## Imagens médicas ganham vida no PowerScale

Os ambientes PACS ou VNA precisam de um armazenamento de dados não estruturados que ofereça desempenho, escalabilidade e proteção em uma plataforma fácil de gerenciar. O PowerScale é um armazenamento de conexão com a rede (NAS) de scale-out que funciona como um único sistema de arquivos em clusters. Isso permite que os dados sejam acessados em todo o sistema de arquivos. Por trás do PowerScale, está o sistema operacional PowerScale OneFS da Dell EMC, que oferece muitos recursos e funcionalidades essenciais para instituições da área da saúde bem-sucedidas. Leia mais sobre o PowerScale para imagens médicas [aqui](#).

O PowerScale com OneFS oferece recursos de segurança nativos integrados diretamente na plataforma. O PowerScale é compatível com a criptografia de dados em repouso (D@RE) com unidades com criptografia automática, snapshots com SnapshotIQ e replicação de dados com SyncIQ. Esses recursos sozinhos já proporcionam tranquilidade em relação à proteção de dados para as instituições da área da saúde, mas para o ransomware, é preciso proteger os dados além disso.

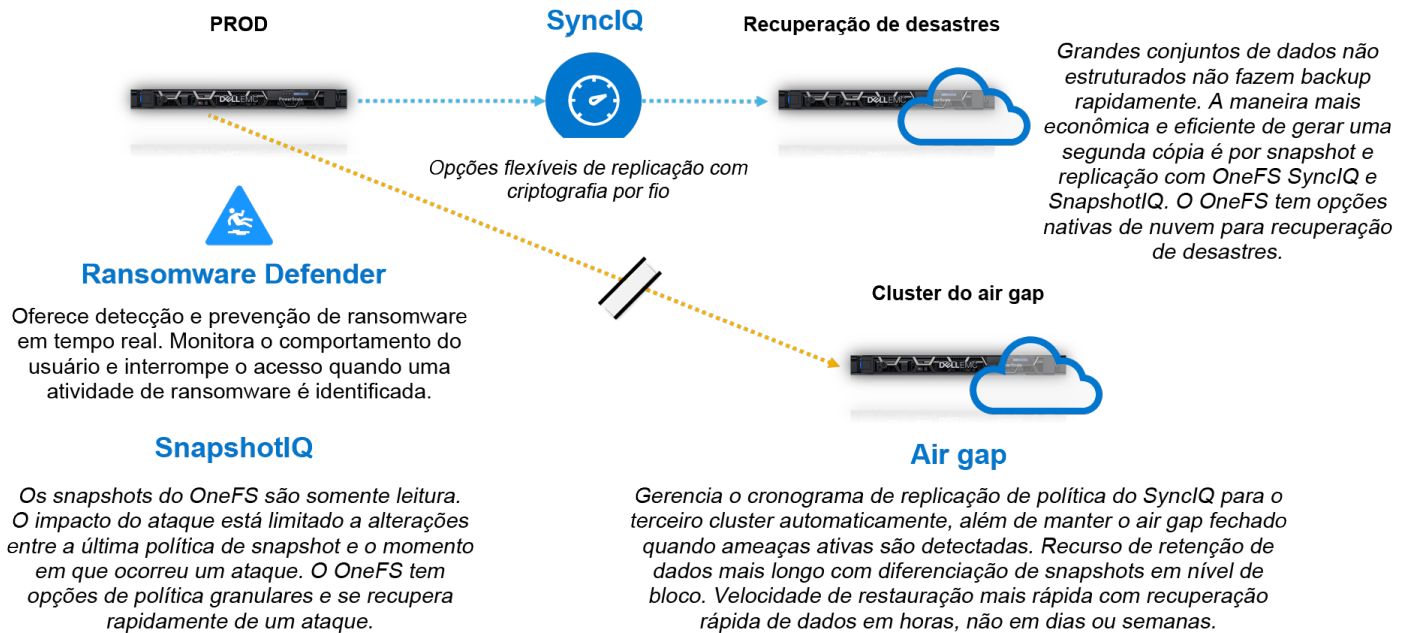
## Superna Eyeglass® Ransomware Defender

O Superna Eyeglass® Ransomware Defender é uma solução de processamento de eventos em tempo real altamente escalável que emprega lógica analítica de comportamento do usuário para detectar e interromper um ataque de ransomware. Ao monitorar os acessos do sistema de arquivos do usuário, o Ransomware Defender detecta alterações nos padrões normais de acesso aos dados dos usuários. Quando os limites definidos pelo administrador são alcançados, o Ransomware Defender pode tomar medidas defensivas para evitar danos maiores e minimizar o tempo de recuperação. Se o Ransomware Defender detectar um comportamento de ataque de ransomware, ele iniciará várias ações defensivas, incluindo impedir usuários de compartilhar arquivos, seja em tempo real ou posterior. Há também regras de bloqueio automático cronometrado para que as medidas sejam tomadas mesmo que um administrador não esteja disponível, assim como o escalonamento automático de resposta se várias infecções forem detectadas em paralelo. A implementação é simplificada com um modo de aprendizagem que pode ser configurado automaticamente com base no monitoramento de carga de trabalho de qualquer ambiente.

O Ransomware Defender integra os recursos de air gap do Cyber Vault à capacidade de suspender as operações de cópia de dados automaticamente quando os dados de origem estiverem ameaçados. Isso proporciona o modo de recuperação mais rápido do setor, eliminando dias e semanas de restauração de dados dos dispositivos de cofre que seriam utilizados por soluções de backup convencionais. O Rapid Recovery da Superna permite que os dados off-line estejam prontos para uso em menos de duas horas, não importa o tamanho do conjunto de dados protegido. Para obter mais informações sobre esta oferta da Superna, clique [aqui](#).

### Como tudo isso funciona

O gráfico a seguir destaca uma arquitetura de referência para uma implementação do Ransomware Defender com o PowerScale para imagens médicas. Com os serviços da Faction no Dell EMC PowerScale, o local de recuperação de desastres e/ou o cluster do air gap podem ser na nuvem.



<sup>1</sup> White paper da IDC, encomendado pela Dell Technologies, Establishing Uncompromising Data Availability for Healthcare Organizations, doc. nº US47447321, de fevereiro de 2021

<sup>2</sup> Davis, Jessica. "Healthcare Cyberattacks Doubled in 2020, with 28% Tied to Ransomware". HealthITSecurity, HealthITSecurity, 25 de fevereiro de 2021, healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware.

Proteção das imagens médicas do seu paciente

© 2021 Dell Inc. ou suas subsidiárias.