Avaliando as opções de criptografia.

Por Pat Woodward

Com tantas opções de criptografia, escolher a melhor para sua empresa pode ser difícil. Entender a diferença entre as principais tecnologias e as vantagens e desvantagens de cada uma ajudará você a encontrar a solução certa para seu ambiente.

Criptografia total de disco por meio de software

A criptografia total de disco (FDE - do inglês Full Disk Encryption) geralmente criptografa todos os setores de um disco rígido, exceto os arquivos críticos exigidos nos processos de boot. O objetivo é proteger a máxima quantidade de dados possível, mas o master boot record (MBR) não deve ser criptografado para permitir a inicialização do computador. Normalmente, as implementações de FDE têm um sistema de boot complexo para carregar o sistema operacional (SO) criptografado do usuário. As soluções de FDE com frequência incluem recursos como autenticação de usuários por leitura de impressões digitais, Smart Cards, autenticação de vários fatores, reconhecimento facial e outras tecnologias avançadas. No entanto, as soluções de FDE podem dificultar o gerenciamento do sistema operacional do usuário em função da interdependência de software e sistema operacional. A interface de gerenciamento de FDE é geralmente proprietária e exige um console de fornecedor de gerenciamento separado, além de implementações exclusivas para recuperação e migração.

Criptografia de arquivos e pastas

A criptografia baseada em arquivos é diferente da FDE porque criptografa arquivos e pastas, mas não aplicativos e sistemas operacionais. Embora o conceito seja simples, a implementação pode ser complexa, envolvendo ações como criptografar arquivos temporários criados por aplicativos, copiar e colar pastas e arquivos, imprimir arquivos, copiar e colar telas e fazer backups de arquivos.

A criptografia de arquivos e pastas oferece recursos não encontrados em soluções FDE. Políticas de chave flexível podem ser definidas por pasta, tipo de arquivo, usuário base ou base de usuários. As chaves só são solicitadas para que permaneçam na memória durante a abertura do arquivo, depois são descartadas. O desempenho em uma unidade criptografada de arquivo ou pasta é normalmente melhor do que quando o FDE é usado. O gerenciamento é simplificado porque o sistema operacional e os aplicativos não são envolvidos, e a autenticação é geralmente nativa do sistema operacional.

Unidades com criptografia automática

Unidades com criptografia automática (SEDs - do inglês Self-Encrypting Drives) são uma classe de dispositivos de armazenamento que incluem aceleradores de criptografia internos. A interface padrão para esses dispositivos é definida pela Opal Security Subsystem Class Specification 1.0 da Trusted Computing Group. A Opal especifica o suporte de criptografia AES tanto de 128 bits quanto de 256 bits, e a chave de criptografia é mantida nos circuitos internos da unidade e nunca é liberada.

Para ativar a SED, comandos são enviados à unidade para configurá-la para a operação de criptografia. Uma pequena partição na unidade armazena o código de boot, que usa a especificação Opal para autenticar o usuário para a unidade. Não há backup de chave porque a criptografia nunca deixa a unidade. O backup de autenticação deve ser usado, e as ferramentas de restauração, que são específicas para fornecedores diferentes, devem ser capazes de restaurar a sequência de autenticação da SED.

Pat Woodward, CCIE, CISSP, é especialista em Enterprise da Dell, que se concentra em operações em rede e segurança.

A solução de criptografia ideal: o que deve ser considerado.

Para escolher a solução de criptografia ideal para sua organização, é necessário considerar muitos fatores. Quando você entender os tipos de tecnologia, considere estes pontos principais:

- Suporte ao sistema legado: saiba quais são os sistemas existentes em seu ambiente e o método de criptografia que pode ser usado para eles. O FDE e a criptografia de arquivos e pastas funcionam com sistemas novos e legados, enquanto a SED pode ter limites.
- Fácil implantação: as soluções FDE exigem que desfragmentações de disco sejam feitas com frequência a fim de criar arquivos contínuos, ao passo que as soluções baseadas em agentes podem aplicar políticas de forma transparente aos usuários.
- Mídia removível: entenda os riscos que armazenamentos externos apresentam; o FDE e a SED podem exigir que seja usado um produto separado para criptografar dados externos.
- Flexibilidade: o FDE e a SED são soluções abrangentes, enquanto a criptografia baseada em arquivos permite a aplicação de políticas flexíveis.