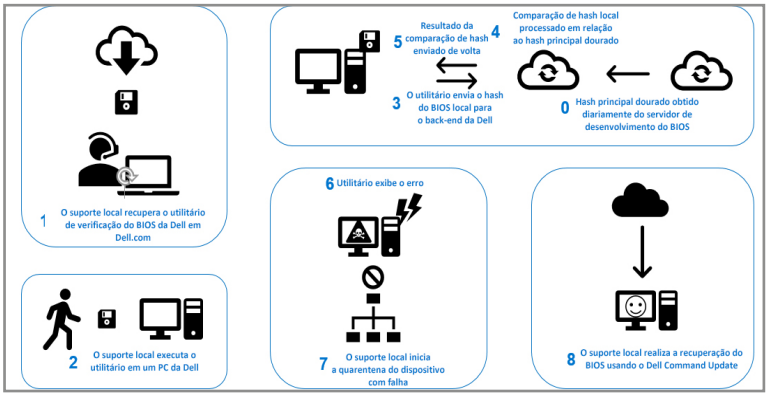
Dell SafeBIOS

SEGURANÇA INTEGRADA NOS PCS COMERCIAIS MAIS SEGUROS DO SETOR

O DELL SAFEBIOS REDUZ O RISCO DE VIOLAÇÃO DO BIOS COM DETECÇÃO DE ATAQUES DE FIRMWARE INTEGRADA

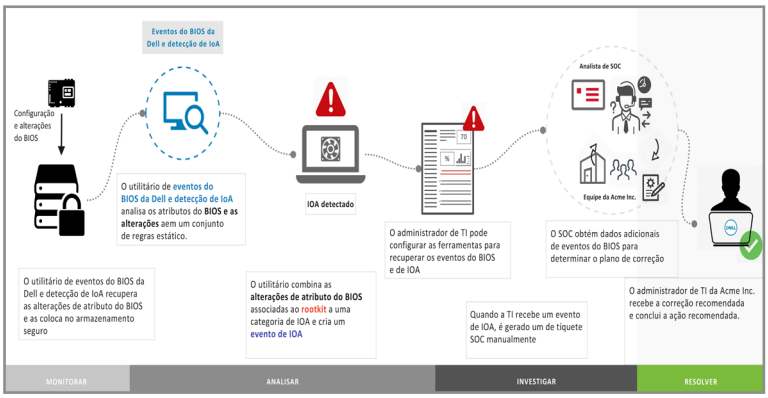
Alerta de violação do BIOS aprimorado

A manutenção da segurança dos dados da organização, seja a propriedade intelectual ou as PIL (Personally Identifiable Information, informações de identificação pessoal) do cliente, é fundamental para a segurança dos dados. Os hackers estão cada vez mais sofisticados e, como as ameaças comuns estão sendo frustradas com mais frequência, os criminosos digitais buscam maneiras mais avançadas de obter essas informações críticas. Com soluções de segurança de endpoint cada vez mais sofisticadas, como antivírus de última geração e detecção e resposta de endpoint gerenciados, os vetores de ataque são restritos e os adversários são obrigados a procurar pontos de invasão alternativos.



A proteção do BIOS é essencial para a postura de segurança de uma organização.

As soluções de segurança de endpoint populares se concentram principalmente no sistema operacional local e nos aplicativos em camadas acima dele, o que deixa o nível mais baixo da pilha do PC, o BIOS, vulnerável a ataques mal-intencionados que podem incapacitar todo o sistema. Quando o malware controla o BIOS, ele detém o PC e o acesso à rede. O comprometimento do BIOS tem um impacto muito grande, atacando a raiz da confiança do PC e, portanto, é muito persistente. Se um invasor obtiver acesso ao BIOS, ele poderá comprometer todos os recursos de segurança de endpoint de um dispositivo, bem como toda a rede de uma organização. Esse tipo de ataque é altamente técnico e, quando executado, muito prejudicial. Essa grande vulnerabilidade tornou-se uma área de preocupação cada vez maior, pois os invasores buscam novos vetores de ataque.



O Dell SafeBIOS responde a esta mudança de paradigma de segurança

Com a frequência crescente de ataques específicos ao BIOS e as novas variantes de malware com capacidade de reinstalação no BIOS, as organizações precisam de uma maneira mais sofisticada de não apenas proteger os sistemas, mas verificar com confiança que eles não foram comprometidos.

A Dell integra a verificação após a inicialização em seus PCs comerciais, garantindo à TI que o BIOS dos funcionários não tenha sido alterado. Em vez de armazenar as informações do BIOS no próprio hardware, que é suscetível à corrupção, o Dell SafeBIOS oferece um recurso de verificação do BIOS fora do host. O SafeBIOS usa um ambiente de nuvem seguro para comparar uma imagem do BIOS individual em relação às avaliações oficiais mantidas no laboratório do BIOS.

Dell SafeBIOS

Além disso, a Dell automatiza a detecção precoce de eventos do BIOS, além de indicadores de ataques e configurações de alto risco ao apresentar o histórico de configuração do BIOS. A extração e a análise contínuas de configurações e eventos do BIOS apresentarão endpoints vulneráveis e alertarão a TI conforme o risco aumenta, permitindo que façam a correção.

Caso o BIOS seja corrompido ou adulterado, a Dell oferece aos clientes opções flexíveis de recriação de imagem para que o BIOS contaminado possa ser analisado a fim de entender a natureza do ataque, o que permite aos clientes verificar a integridade do BIOS usando o processo fora do host sem interromper o processo de inicialização. O SafeBIOS fornece conhecimento adicional sobre as alterações do BIOS, além de garantias adicionais para manter as ameaças à distância.

Além disso, se um BIOS for comprometido, a imagem dele será capturada automaticamente para análise e correção depois de passar pelo processo de recuperação do BIOS.

Integrações para parceiros
Esses recursos combinados fornecem a capacidade de identificar e resolver de forma mais rápida os possíveis riscos. O recurso independente está disponível atualmente no Suporte Dell.

O VMware Workspace ONE fornece gerenciamento de TI com a nova visibilidade do status do BIOS para gerenciamento unificado de endpoints. A integração com o VMware Workspace ONE permite que a equipe de TI configure fluxos de trabalho automatizados para enviar atualizações over-the-air e restaurar dispositivos para que estejam em conformidade.

A capacidade combinada do VMware Carbon Black Audit and Remediation e do Dell SafeBIOS fornece segurança avançada, tanto no âmbito como fora do SO, e permite a telemetria do status de verificação do BIOS fora do host na oferta de PC comercial da Dell. A solução integrada permite que as equipes de segurança e as de TI automatizem a geração de relatórios do status de verificação, de modo que possam tomar providências para remediar os comprometimentos resultantes da violação do BIOS. Essa parceria reforça o papel da Dell como a fornecedora dos PCs comerciais mais seguros do setor.

O Dell SafeBIOS faz parte do maior portfólio de segurança de endpoint de dispositivos confiáveis Dell com soluções que oferecem suporte a endpoint, tanto no âmbito como fora do SO, para oferecer uma verdadeira abordagem abrangente de proteção dos dados incluindo:

- SafeBIOS: reconheça ataques ocultos e escondidos com o alerta de violação do BIOS por meio da verificação do BIOS fora do host exclusiva da Dell[1], da captura de imagem do BIOS e de eventos e IoA do BIOS.
- SafeID: somente a Dell protege as credenciais do usuário final em um chip de segurança dedicado, mantendo-as ocultas contra malware que busca e rouba credenciais.
- SafeScreen: os usuários finais podem trabalhar em qualquer lugar, mantendo as informações confidenciais privadas com uma tela de privacidade digital integrada.
- SafeData: proteja os dados confidenciais no dispositivo para ajudar a atender às normas de conformidade e proteger as informações na nuvem, o que oferece aos usuários finais a liberdade de colaborar com segurança.
- SafeGuard and Response (com tecnologia VMware Carbon Black e SecureWorks): evite, detecte e responda a malware avançado e ataques cibernéticos para manter a produtividade sem a disrupção e os problemas que um ataque pode causar.

Entre em contato com seu especialista em segurança de endpoint da Dell hoje mesmo pelo e-mail endpointsecurity@dell.com para discutir como podemos ajudar a melhorar sua postura de segurança.

[1] Alegação baseada em análise interna.