Brief técnico

Proteja a sua rede com as impressoras mais seguras do mundo[1]

Funcionalidades de segurança de impressão HP

Proteção, deteção e recuperação

A mais recente geração de dispositivos de impressão HP Enterprise é única no mercado, pois oferece um conjunto das três tecnologias-chave concebidas para impedir ataques informáticos e para efetuar autorrecuperações. Estas funcionalidades executam automaticamente um reinício em caso de ataque ou anomalia.

Após um reinício, o HP JetAdvantage Security Manager acede automaticamente ao dispositivo e, caso seja necessário, corrige as definições de segurança do dispositivo para que estas estejam em conformidade com as políticas pré-estabelecidas da empresa.[2] A equipa de TI não precisa de intervir. Os administradores podem receber notificações através das aplicações de gestão da HP, como o JetAdvantage Security Manager e o ArcSight.

HP Sure Start

O BIOS constitui um conjunto de instruções utilizadas para carregar componentes de hardware fundamentais e iniciar o firmware HP FutureSmart de um dispositivo HP do segmento empresarial. A tecnologia HP Sure Start funciona em segundo plano quando os dispositivos são ligados, ajudando a proteger os seus dispositivos de impressão e de processamento de imagem contra ataques. A tecnologia HP Sure Start valida a integridade do BIOS a cada ciclo de arranque. Caso seja detetada uma versão corrompida, o dispositivo é reiniciado com uma cópia de segurança ("golden copy") do BIOS.

Lista de permissões

Os dispositivos empresariais (Enterprise) da HP incorporam firmware FutureSmart. Tal como acontece com o sistema operativo de um computador, o firmware coordena as funções de hardware, executa o painel de controlo, determina que funcionalidades estão disponíveis quando imprime, digitaliza ou envia documentos por e-mail e fornece segurança de rede. Um firmware corrompido pode expor o seu dispositivo e a sua rede a ataques. A lista de permissões assegura que apenas o código autêntico e conhecido da HP, e que não foi alterado, é carregado na memória. Caso seja detetada uma anomalia, o dispositivo é reiniciado para um estado seguro e offline. Em seguida, envia uma notificação para a equipa de TI, de modo que esta volte a carregar o firmware.

Deteção de intrusão em tempo de execução

A maioria das pessoas não deixaria os respetivos computadores em funcionamento sem qualquer supervisão ou proteção. Poucos fornecedores oferecem um nível de proteção básico para os respetivos dispositivos de impressão e de processamento de imagem.[1] A deteção de intrusão em tempo de execução da HP protege os dispositivos enquanto estes estão em funcionamento e ligados à rede, exatamente quando a maioria dos ataques ocorre. Esta funcionalidade verifica a existência de anomalias durante operações complexas de memória e firmware. Em caso de intrusão, o dispositivo é reiniciado automaticamente.

Saiba mais em: hp.com/go/PrintersThatProtect

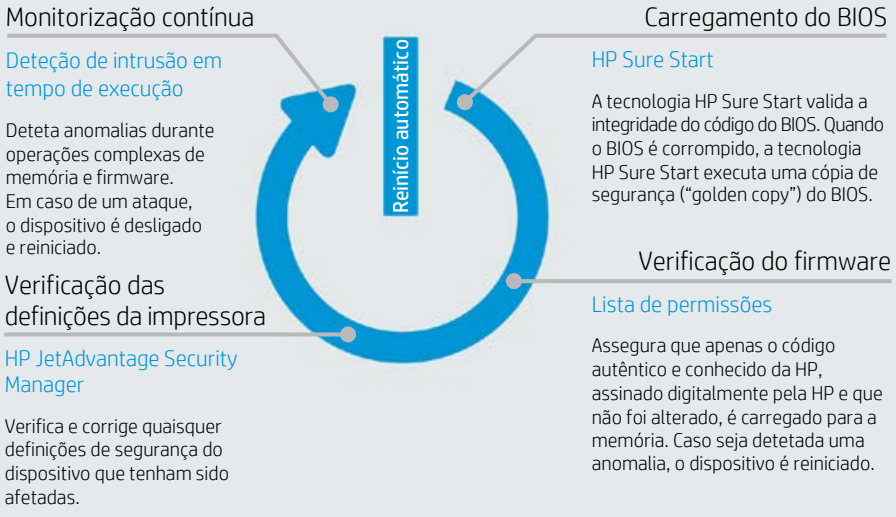
[1] Afirmação baseada numa análise da HP (2015) relativa a funcionalidades de segurança incorporadas das impressoras concorrentes do segmento. Apenas a HP oferece uma combinação de funcionalidades de segurança para verificação de integridade até ao BIOS com capacidades de autorreparação. Poderá ser necessária uma atualização do pacote de serviços FutureSmart para ativar algumas funcionalidades de segurança. Algumas funcionalidades serão disponibilizadas como uma atualização do pacote de serviços HP FutureSmart em modelos de impressoras empresariais (Enterprise) existentes. Para consultar uma lista de produtos compatíveis, aceda a hp.com/go/LJCompatibility.
Para obter mais informações, aceda a hp.com/go/LJsecurityclaims.

[2] O HP JetAdvantage Security Manager tem de ser adquirido separadamente. Para obter mais informações, aceda a hp.com/go/securitymanager.

Como funciona?

As funcionalidades de segurança incorporadas abrangem os três passos principais no ciclo de um dispositivo HP.

O HP JetAdvantage Security Manager completa o ciclo de verificação.



Registe-se para receber atualizações
hp.com/go/getupdated

4AA6-1167PTE, fevereiro de 2016