



HP DaaS Proactive Security



Vantagens do serviço

- Torna os dispositivos endpoint mais seguros
- Protege contra websites e anexos maliciosos
- Protege os seus dados e privacidade

Destaques do serviço

- Protege contra websites e anexos maliciosos²
- As análises da HP TechPulse fornecem informações e relatórios de segurança
- A avaliação CyQu da Aon ajuda a avaliar a sua posição de segurança³

Descrição do serviço

Melhore as capacidades de gestão segura do HP Device as a Service (DaaS) com HP DaaS Proactive Security.¹ Fornece proteção contra malware em tempo real para dispositivos de computação endpoint, análises de segurança e ameaças e conhecimento especializado para reforçar a sua segurança. A tecnologia de isolamento de ameaças protege contra malware introduzido através de e-mail, browsers e ficheiros do Office ou PDF. Amplia as informações e os relatórios de segurança fornecidos pelas análises da HP TechPulse. Como tal, ajuda-o a proteger, entender e responder a ameaças.

Características e especificações

Tecnologia avançada de isolamento

Vírus, ransomware e outros malwares continuam a representar uma grande ameaça para a infraestrutura das TI. Vá para além das soluções de antivírus baseadas em definições com a tecnologia de isolamento de ameaças em tempo real, utilizando micromáquinas virtuais (MV) para conter ataques de dia zero de e-mail, browser e ficheiros e impedir que afetem a sua rede.² Os utilizadores podem visualizar anexos e websites sem comprometer a segurança da sua rede e sem interromper o fluxo de trabalho ou alterar os seus comportamentos.

Análises da HP TechPulse

Mantenha-se informado e obtenha uma perspetiva holística do estado de proteção dos seus dispositivos e conclusões detalhadas sobre ataques tentados e bloqueados com a HP TechPulse – tudo a partir de um único dashboard (painel de controlo) disponível através do portal HP DaaS.

Especialistas em Serviços HP

Reforce a sua posição de segurança, antecipe ataques e evite o impacto negativo na sua empresa com os nossos Especialistas em Serviços HP que monitorizam relatórios, analisam ameaças e o ajudam no planeamento. Os Especialistas em Serviços HP realizam análises trimestrais de ameaças à segurança e respondem aos alertas de segurança.⁴

Aon

Colaboramos com a Aon para disponibilizar soluções adicionais de segurança cibernética que incluem avaliação, resposta a incidentes e serviços de seguro. A Cyber Quotient (CyQu), uma ferramenta da Aon para avaliação do risco cibernético e classificação da segurança destinada a empresas, ajuda-o a avaliar a sua posição de segurança em relação aos concorrentes no setor, e a Aon oferece 0 \$ de adiantamento para resposta a incidentes com 1 hora de consulta, no caso de uma quebra ou violação de segurança.³

Planos HP DaaS Proactive Security

Características do serviço	Plano Standard (autogerido)	Plano Enhanced (gerido pela HP)
Proteção contra ameaças contidas em anexos de e-mail, hiperligações de phishing e transferências de ficheiros	✓	✓
Informações de segurança da HP TechPulse	✓	✓
Avaliação CyQu da Aon, resposta a incidentes e elegibilidade para seguros ³	✓	✓
Aplicação de política de isolamento: Os Especialistas em Serviços HP podem gerir o estado da tecnologia de proteção avançada	—	✓
Análises: Os Especialistas em Serviços HP realizarão uma análise de <i>kill switch</i> de ameaças isoladas e apresentarão recomendações sobre boas práticas para utilizadores e dispositivos que sejam alvo de um grande volume de ameaças, conforme necessário	—	✓
Investigação e notificação de eventos de segurança: Os Especialistas em Serviços HP notificá-lo-ão quando os dispositivos já não estiverem protegidos devido a adulteração por utilizadores finais ou alterações na configuração do sistema	—	✓

Especificações da prestação de serviços

Opções de serviço

- **Standard:** A versão Standard autogerida do HP DaaS Proactive Security está disponível para Planos HP DaaS Standard, Enhanced e Premium. Na opção autogerida, assume a responsabilidade de registar os seus dispositivos e de entrar em contacto com a HP para obter assistência, se necessário.
- **Enhanced:** A versão Enhanced do HP DaaS Proactive Security só estará disponível se também tiver um Plano HP DaaS Enhanced ou Premium. Com o Plano Enhanced, um HP Onboarding Program Manager ajudá-lo-á na instalação e configuração do serviço, e os Especialistas em Serviços HP com competências em segurança cibernética prestarão serviços de monitorização e suporte contínuos.

Responsabilidades da HP

Responsabilidades do Especialista em Serviços HP nos Planos Standard:

- Resolver problemas de instalação e conectividade.
- Prestar assistência e responder a perguntas relacionadas com serviços.
- Adicionar novos URLs à lista de permissões (whitelist) de websites específicos da empresa.

Responsabilidades do Especialista em Serviços HP nos Planos Enhanced:

- Certificar-se de que a tecnologia avançada de isolamento está instalada e ativada.
- Apresentar relatórios trimestrais de análise de ameaças de segurança.
- Investigar os alertas de segurança e adotar as medidas adequadas.
- Monitorizar o serviço e coordenar a resolução de problemas e a assistência.
- Prestar suporte de Nível 2 e Nível 3 e coordenar com o seu Service Desk.

Responsabilidades do cliente

- Rever os dashboards (painéis de controlo), relatórios e incidentes no dashboard do HP DaaS Proactive Management.
- Rever os relatórios de segurança e responder, quando necessário.
- Solicitar e fornecer páginas Web de lista de permissões de URLs.
- Resolver problemas e fazer a triagem de questões de suporte comuns do utilizador final, antes de contactar o Suporte da HP.
- Renovar, alterar ou cancelar a sua conta HP DaaS.
- Preencher o inquérito CyQu online.³

Requisitos do sistema

- O HP DaaS Proactive Security requer dispositivos cliente de vários fabricantes que executam o Windows 10 (versão 1703 ou posterior), com um mínimo de 8 GB de memória e 6 GB de espaço livre em disco.
- O HP DaaS Proactive Security requer HP TechPulse, que está incluída em qualquer Plano HP DaaS ou HP DaaS Proactive Management. O Plano HP DaaS Proactive Security Enhanced requer que os clientes estejam registados num Plano HP DaaS Enhanced ou Premium.
- As comunicações entre dispositivos geridos e o serviço de gestão de nuvem da HP requerem uma ligação ativa à Internet.
- Consulte hpdaas.com/requirements para conhecer detalhes adicionais.

Especificações da prestação do serviço (continuação)

Integração

A integração é o processo de trazer dispositivos abrangidos para a solução HP DaaS Proactive Security. Será designado um HP Onboarding Program Manager (Gestor de programa de integração HP) para gerir o processo de integração se tiver um Plano HP DaaS Enhanced ou Premium. Se tiver um Plano Standard autogerido, um Especialista em Serviços HP criará uma conta para si e fornecerá as informações necessárias da conta num email de boas-vindas, juntamente com as instruções sobre como obter assistência, se necessário.

Pré-requisitos de integração

Antes de fazer a transição dos seus dispositivos para o HP DaaS Proactive Security, deverá fornecer as seguintes informações ao seu HP Onboarding Program Manager, HP Account Manager (Gestor de conta HP) e/ou ao parceiro de serviço:

- Informações do contacto principal (nome, e-mail, telefone, localização)
- O endereço da sua empresa
- O seu nome de domínio DNS do Active Directory
- Uma lista de administradores de relatórios
- Uma lista de dispositivos a gerir pelo HP Proactive Management, incluindo modelos e números de série (somente para Planos HP DaaS Enhanced ou Premium)

Processo de integração

- **Fase 1: Registo:** Receberá uma chave de licença e uma hiperligação para aceder a um formulário de registo online.
- **Fase 2: Recolha de informações:** Será designado um HP Onboarding Program Manager para gerir o seu processo de integração. Este irá agendar uma chamada de conferência para apresentar recomendações sobre como proceder.
- **Fase 3: Recomendações e criação de conta:** A HP criará a sua conta na plataforma HP DaaS Proactive Security, começando com as configurações de segurança padrão e adicionando à lista de permissões (whitelisting) todos os URLs adicionais que exigir.
- **Fase 4: Implementação:** O HP Onboarding Program Manager irá reunir-se consigo para iniciar o registo do dispositivo e resolver quaisquer problemas.
- **Fase 5: Transição para suporte e gestão contínuos (somente Planos Enhanced):** Quando a integração estiver concluída, o serviço transitará para os Especialistas em Serviço HP, que prestarão suporte e gestão contínuos durante a vigência do contrato.

Responsabilidades do HP Onboarding Program Manager

- Criar a conta do HP DaaS Proactive Management.
- Adicionar ou remover utilizadores do dashboard do HP DaaS Proactive Management.
- Conceder acesso à conta de utilizador.
- Reunir e consolidar as informações necessárias sobre o ambiente.
- Fornecer documentação e orientação para implementar o agente de análise.
- Desenvolver e implementar o plano do projeto de integração.
- Apresentar atualizações sobre o progresso.
- Verificar o sucesso da implementação.
- Fazer a transição do suporte ao cliente da funcionalidade HP DaaS Proactive Management para os Especialistas em Serviços HP.
- Diagnosticar e resolver problemas de instalação.
- Prestar suporte contínuo.

Limitações do serviço

- Disponibilidade dos Especialistas em Serviço HP para o Plano HP DaaS Proactive Security Enhanced:
 - **América do Norte:** Suporte prestado em inglês, disponível de segunda a sexta-feira (excluindo feriados HP), das 06h00 às 18h00 (MT).
 - **América Latina:** Suporte prestado em inglês e espanhol, disponível de segunda a sexta-feira (excluindo feriados HP), das 07h00 às 18h00 (GMT-5).
 - **Europa, Médio Oriente e África:** Suporte prestado em inglês, francês e alemão, disponível de segunda a sexta-feira (excluindo feriados HP), das 08h00 às 18h00 (CET).
 - **Ásia-Pacífico e Japão:** Suporte prestado em inglês e mandarim, disponível 24 horas por dia; Suporte prestado em japonês, das 09h00 às 21h00 (hora padrão do Japão), disponível 7 dias por semana (excluindo feriados HP).
- Os serviços da Aon estão atualmente disponíveis apenas nos Estados Unidos.
- As plataformas HP DaaS Proactive Management e HP DaaS Proactive Security estão alojadas no Amazon Web Services (AWS).

Termos e Condições

Consulte os [Termos e Condições](#) do HP DaaS.

Para mais informações

Contacte o seu Representante de vendas HP local ou Parceiro de canal HP para saber mais detalhes ou acesse a hp.com/go/DaaS.

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



Partilhar com os colegas

1. Os requisitos do sistema para o HP DaaS Proactive Security são: dispositivos cliente de diferentes fabricantes que executam Windows 10 (versão 1703 ou posterior), com um mínimo de 8 GB de memória e 6 GB de espaço livre em disco para instalar o software cliente. O HP DaaS Proactive Security requer HP TechPulse, que está incluída em qualquer Plano HP DaaS ou HP DaaS Proactive Management. O Plano HP DaaS Proactive Security Enhanced requer que os clientes estejam registados num Plano HP DaaS Enhanced ou Premium ou HP DaaS Proactive Management.
2. A Tecnologia HP Sure Click Advanced está incluída no Serviço HP DaaS Proactive Security e requer o Windows 10. Suporta o Microsoft Internet Explorer, Google Chrome e Chromium. Os anexos suportados incluem ficheiros do Microsoft Office (Word, Excel, PowerPoint) e ficheiros PDF, quando o Microsoft Office ou o Adobe Acrobat estão instalados.
3. O serviço Aon está disponível apenas nos Estados Unidos.
4. Os Especialistas em Serviços HP estão disponíveis apenas no Plano HP DaaS Proactive Security Enhanced.

© Copyright 2019 HP Development Company, L.P. As informações apresentadas estão sujeitas a alteração sem aviso prévio. As únicas garantias para produtos e serviços da HP estão definidas nas declarações de garantia expressas que acompanham os respetivos produtos e serviços. Nada do aqui apresentado deverá ser interpretado como constituição de garantia adicional. A HP não é responsável por omissões nem erros técnicos ou editoriais aqui apresentados. Adobe e Acrobat são marcas comerciais da Adobe Systems Incorporated. Google, Chrome e Chromium são marcas comerciais da Google Inc. Microsoft e Windows são marcas comerciais registadas da Microsoft Corporation nos E.U.A. e/ou noutros países.

4AA7-4656PTE. Março de 2019.

