HP DaaS Proactive Security



Vorteile des Service

- Sicherere Endpunkte
- Schutz vor böswilligen Websites und Anhängen
- Schutz Ihrer Daten und Geräte

Highlights des Service

- Innovative Isolierungstechnologie zum Schutz vor Malware[2]
- HP TechPulse Analysen für Sicherheitsinformationen und -berichte
- Aon CyQu-Analyse zur Bewertung Ihrer Sicherheitslage[3]

Serviceübersicht

Erweitern Sie die sicheren Managementfunktionen von HP Device as a Service (DaaS) durch HP DaaS Proactive Security.[1] Dieser Zusatzservice bietet Echtzeit-Malwareschutz für Computing-Endgeräte, Sicherheits- und Bedrohungsanalysen sowie hochspezialisierte Expertise zur Verbesserung Ihrer Sicherheitslage. Die Technologie zur Bedrohungsisolierung schützt vor Malware, die über E-Mails, Browser und Office- oder PDF-Dateien eingeschleust wird. Sie stellt eine Ergänzung zu den durch HP TechPulse Analysen bereitgestellten Sicherheitsinformationen und -berichten dar. Damit können Sie sich vor Bedrohungen schützen, indem Sie sich über Bedrohungen informieren und entsprechend darauf reagieren.

Leistungen und Spezifikationen

Innovative Isolierungstechnologie

Viren, Ransomware und andere Malware stellen nach wie vor eine schwerwiegende Bedrohung für die IT-Infrastruktur dar. Ergänzen Sie definitionsbasierte Virenschutzlösungen durch eine Technologie zur Echtzeit-Bedrohungsisolierung, die mit Mikro-VMs (Virtual Machines) dazu beiträgt, das Netzwerk vor Zero-Day-E-Mail-, Browser- und Dateiattacken zu schützen.[2] Damit können Benutzer Anhänge und Websites anzeigen, ohne die Sicherheit Ihres Netzwerks zu gefährden und ohne ihre Arbeitsabläufe zu unterbrechen oder ihr Verhalten zu ändern.

HP TechPulse Analysen

Bleiben Sie mit HP TechPulse immer auf dem Laufenden und gewinnen Sie einen ganzheitlichen Überblick über den Schutzstatus Ihrer Geräte sowie detaillierte Erkenntnisse zu versuchten und abgewehrten Angriffen – alles über ein zentrales Dashboard, das über das HP DaaS-Portal verfügbar ist.

HP Service-Experten

Verbessern Sie Ihre Sicherheitslage, beugen Sie Angriffen vor und verhindern Sie nachteilige Folgen für Ihr Unternehmen mithilfe unserer spezialisierten Service-Experten, die Berichte überwachen, Bedrohungen analysieren und Sie bei der Planung unterstützen. HP Service-Experten führen vierteljährlich Bedrohungsanalysen durch und reagieren auf Sicherheitswarnungen.[4]

Aon

Wir arbeiten mit Aon zusammen, um zusätzliche Lösungen für die Cyber-Sicherheit bereitstellen zu können. Dazu gehören Assessments, die Reaktion auf Vorfälle sowie Versicherungsservices. Mit Aon Cyber Quotient (CyQu), einem Tool für die Selbstanalyse und zur Sicherheitsbewertung können Sie Ihre Sicherheitslage im Vergleich zu anderen Unternehmen in der Branche einschätzen. Zudem stellt Aon im Fall einer Sicherheitsverletzung zur Beratung einen Ansprechpartner für die Reaktion auf den Vorfall eine Stunde kostenlos bereit.[3]

DaaS Proactive Security Tarife

Serviceleistungen	Standard-Tarif (selbst verwaltet)	Enhanced-Tarif (von HP verwaltet)
Schutz vor Bedrohungen aus E-Mail-Anhängen, Phishing-Links und Downloads	✓	✓
Sicherheitsinformationen von HP TechPulse	✓	✓
Bewertung, Reaktion auf Vorfälle und Versicherungsschutz durch Aon CyQu[3]	✓	✓
Durchsetzung von Isolierungsrichtlinien: HP Service-Experten kümmern sich um den Status innovativer Schutztechnologien	—	✓
Analyse: HP Service-Experten führen für isolierte Bedrohungen eine Kill-Switch-Analyse durch und geben bei Bedarf Empfehlungen zu bewährten Vorgehensweisen für Benutzer und Geräte, die von einer Vielzahl von Bedrohungen betroffen sind	—	✓
Untersuchung von Sicherheitsereignissen und entsprechende Benachrichtigung: HP Service-Experten benachrichtigen Sie, wenn Geräte aufgrund von Manipulationen durch Endbenutzer oder Änderungen an der Systemkonfiguration nicht mehr geschützt sind	—	✓

Spezifikationen für die Servicebereitstellung

Serviceoptionen

- **Standard:** Die selbst verwaltete Standardversion von DaaS Proactive Security ist für die DaaS-Tarife Standard, Enhanced und Premium verfügbar. Bei der selbstverwalteten Option übernehmen Sie die Verantwortung für die Registrierung Ihrer Geräte und die Kontaktaufnahme mit HP, für den Fall, dass Sie Unterstützung benötigen.
- **Enhanced:** Die Enhanced-Version von DaaS Proactive Security ist nur verfügbar, wenn Sie den DaaS-Tarif Enhanced oder Premium haben. Beim Enhanced-Tarif unterstützt Sie ein Manager des HP Onboarding-Programms bei der Installation und Konfiguration des Services, und HP Service-Experten mit Erfahrung im Bereich der Cyber-Sicherheit sorgen für kontinuierliche Überwachung und Support.

Verantwortlichkeiten von HP

Verantwortlichkeiten von Service-Experten bei Standard-Tarifen:

- Behebung von Installations- und Verbindungsproblemen
- Unterstützung bei und Antworten auf servicebezogene Fragen
- Ergänzung der Whitelist von unternehmensspezifischen Websites mit neuen URLs

Verantwortlichkeiten von Service-Experten bei Enhanced-Tarifen:

- Sicherstellung, dass die innovative Isolierungstechnologie installiert und aktiviert ist
- Vierteljährliche Berichte zu Bedrohungsanalysen
- Untersuchung von Sicherheitswarnungen und Ergreifen entsprechender Maßnahmen
- Überwachung des Services und Koordination von Fehlerbehebung und Unterstützung
- Bereitstellung von Level-2- und Level-3-Support und Koordination mit Ihrem Service Desk

Mitwirkungspflicht des Kunden

- Prüfen von Dashboards, Berichten und Vorfällen im HP DaaS Proactive Management Dashboard
- Prüfen von Sicherheitsberichten und entsprechende Reaktion
- Anfordern und Bereitstellen von URL-Whitelisting-Webseiten
- Durchführen von Maßnahmen zur Fehlerbehebung und Ersteinschätzung häufiger Probleme beim Endbenutzer-Support, bevor dieser sich an den HP Support wendet
- Fristgerechtes Verlängern, Ändern oder Beenden des HP DaaS Kontos
- Teilnehmen an der CyQu Onlineumfrage.[3]

Systemvoraussetzungen

- Für DaaS Proactive Security sind Multivendor-Client-Geräte unter Windows 10 1703 oder höher mit mindestens 8 GB Arbeitsspeicher und 6 GB freiem Festplattenspeicherplatz erforderlich.
- DaaS Proactive Security erfordert HP TechPulse, das in jedem HP DaaS- oder HP DaaS Proactive Management Tarif enthalten ist. Der HP DaaS Proactive Security Enhanced Tarif setzt voraus, dass der Kunde bereits einen Enhanced oder Premium Tarif für HP DaaS abgeschlossen hat.
- Für die Kommunikation zwischen den verwalteten Geräten und dem HP Cloud-Verwaltungsdienst wird eine Internetverbindung benötigt.
- Weitere Informationen finden Sie unter hpdaas.com/requirements.

Spezifikationen für die Servicebereitstellung (Fortsetzung)

Onboarding

Onboarding bezeichnet den Prozess, bei dem die abgedeckten Geräte in die DaaS Proactive Security Lösung eingebunden werden. Wenn Sie den HP DaaS-Tarif Enhanced oder Premium abgeschlossen haben, wird Ihnen für die Betreuung des Onboarding-Prozesses ein Onboarding-Programmmanager zugewiesen. Wenn Sie den Standard-Tarif für die selbst verwaltete Version abgeschlossen haben, erstellt ein HP Service-Experte ein Konto für Sie und liefert Ihnen in einer Begrüßungs-E-Mail die erforderlichen Informationen zum Konto. Außerdem erhalten Sie Hinweise, wie Sie bei Bedarf Unterstützung erhalten können.

Voraussetzungen für das Onboarding

Vor der Umstellung Ihrer Geräte auf DaaS Proactive Security müssen Sie Ihrem Onboarding-Programmmanager, HP Account Manager und/oder Servicepartner die folgenden Informationen zur Verfügung stellen:

- Informationen zum Hauptansprechpartner (Name, E-Mail, Telefon, Standort)
- Adresse Ihres Unternehmens
- Ihr Active Directory DNS-Domänenname
- Eine Liste der Berichtsadministratoren
- Eine Liste mit Geräten, die von HP Proactive Management verwaltet werden sollen, mit Angaben zu Modell und Seriennummer (nur bei den DaaS-Tarifen Enhanced und Premium)

Onboarding-Prozess

- **Phase 1: Registrierung:** Sie erhalten einen Lizenzschlüssel und einen Link zu einem Online-Formular für die Registrierung.
- **Phase 2: Informationsgewinnung:** Ihnen wird ein Onboarding-Programmmanager zur Betreuung des Onboarding-Prozesses zugewiesen. Er organisiert eine Telefonkonferenz, in der Sie Empfehlungen zum weiteren Vorgehen erhalten.
- **Phase 3: Empfehlungen und Kontoerstellung:** HP erstellt beginnend mit den Standardsicherheitskonfigurationen Ihr Konto in der HP DaaS-Sicherheitsplattform und ergänzt die Whitelist mit zusätzlichen, von Ihnen benötigten URLs.
- **Phase 4: Bereitstellung:** Der Onboarding-Programmmanager kommt mit Ihnen zusammen, um die Geräteregistrierung einzuleiten und potenzielle Probleme zu beheben.
- **Phase 5: Umstellung auf kontinuierlichen Support und fortlaufende Betreuung (nur Enhanced-Tarif):** Nach Abschluss des Onboarding-Prozesses wird der Service an HP Service-Experten übergeben, die für den kontinuierlichen Support und die fortlaufende Betreuung während der Vertragslaufzeit verantwortlich sind.

Verantwortlichkeiten des Onboarding-Programmmanagers

- Erstellen des HP DaaS Proactive Management Kontos
- Hinzufügen oder Entfernen von HP DaaS Proactive Management Dashboardbenutzern
- Gewähren des Zugriffs auf das Benutzerkonto
- Sammeln und Konsolidieren der erforderlichen Informationen zur Betriebsumgebung
- Bereitstellen der Dokumentation zum Analyseagenten und Hilfestellung bei dessen Bereitstellung
- Bereitstellen und Implementieren des Onboarding-Projektplans
- Bereitstellen von Informationen zum aktuellen Status
- Überprüfen, ob die Implementierung erfolgreich verlaufen ist
- Übergeben des Kundensupports im Rahmen der HP DaaS Proactive Management Leistung an HP Service-Experten
- Diagnostizieren und Beheben von Problemen bei der Installation
- Kontinuierlicher Support

Serviceeinschränkungen

- Verfügbarkeit von HP Service-Experten im Rahmen des DaaS Proactive Security Enhanced Tarifs:
  - **Nordamerika:** Support in englischer Sprache von Montag bis Freitag (außer an bei HP arbeitsfreien Tagen) von 6:00 Uhr bis 18:00 Uhr, MT.
  - **Lateinamerika:** Support in englischer und spanischer Sprache von Montag bis Freitag (außer an bei HP arbeitsfreien Tagen) von 07:00 Uhr bis 18:00 Uhr, GMT – 5.
  - **Europa/Naher und Mittlerer Osten/Afrika:** Support in englischer, französischer und deutscher Sprache von Montag bis Freitag (außer an bei HP arbeitsfreien Tagen) von 08:00 Uhr bis 18:00 Uhr, CET.
  - **Asien-Pazifik, Japan:** Support in englischer und chinesischer Sprache ist rund um die Uhr verfügbar. Support in japanischer Sprache steht von 9:00 Uhr bis 21:00 Uhr, Japan Standard Time, an 7 Tagen (außer an bei HP arbeitsfreien Tagen) zur Verfügung.
- Aon Services sind derzeit nur in den USA verfügbar.
- Die Plattformen von HP DaaS Proactive Management und HP DaaS Proactive Security werden auf AWS-Systemen (Amazon Web Services) gehostet.

Geschäftsbedingungen

Siehe die HP DaaS **Geschäftsbedingungen**.

Weitere Informationen

Weitere Einzelheiten erhalten Sie über Ihren HP Vertriebsbeauftragten oder Channel Partner oder auf folgender Website **hp.com/go/DaaS**.

Melden Sie sich noch heute an.
hp.com/go/getupdated

Mit Kollegen teilen

1. Systemanforderungen für HP DaaS Proactive Security: Multivendor-Client-Geräte unter Windows 10 1703 oder höher mit mindestens 8 GB Arbeitsspeicher und 6 GB freiem Festplattenspeicherplatz für die Installation der Client-Software. HP DaaS Proactive Security erfordert HP TechPulse, das in jedem HP DaaS- oder HP DaaS Proactive Management Tarif enthalten ist. Der HP DaaS Proactive Security Enhanced Tarif setzt voraus, dass der Kunde bereits einen Enhanced- oder Premium Tarif für HP DaaS oder HP DaaS Proactive Management abgeschlossen hat.
2. Die in HP DaaS Proactive Security enthaltene HP Sure Click Advanced Technologie erfordert Windows 10 und unterstützt Microsoft Internet Explorer, Google Chrome und Chromium. Zu den unterstützten Anhängen zählen u. a. Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office bzw. Adobe Acrobat installiert ist.
3. Aon Services sind nur in den USA verfügbar.
4. Service-Experten sind nur im Rahmen des Proactive Security Enhanced Tarifs verfügbar.

© Copyright 2019 HP Development Company, L.P. Änderungen vorbehalten. Neben der gesetzlichen Gewährleistung gilt für HP Produkte und Dienstleistungen ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Dienstleistungen explizit genannt wird. Aus den Informationen in diesem Dokument ergeben sich keinerlei zusätzliche Gewährleistungsansprüche. HP haftet nicht für technische bzw. redaktionelle Fehler oder fehlende Informationen. Adobe und Acrobat sind Marken von Adobe Systems Incorporated. Google, Chrome und Chromium sind Marken von Google Inc. Microsoft und Windows sind in den USA und/oder anderen Ländern eingetragene Marken der Microsoft Corporation.

4AA7-4656DEE, März 2019