



## Vorteile des Service

- Stoppen Sie neu auftretende Zero-Day-Attacken mit einem mehrstufigen Abwehrkonzept.
- Sichern Sie Ihre Endgeräte mit Technologie auf Enterprise-Niveau.
- Schützen Sie Ihre Mitarbeiter vor Cyberbedrohungen, ohne dass sich dies negativ auf ihre Produktivität auswirkt.

## Highlights des Service

- Schutzorientiertes Konzept für die Endgerätesicherheit mit Echtzeitabwehr auf unterschiedlichen Ebenen
- Fachkundiges Management durch zertifizierte Sicherheitsexperten
- Zeitnahe, handlungsrelevante Analysen und Erkenntnisse

## Serviceübersicht

HP Proactive Security trägt mit einem mehrstufigen Service für die Endgerätesicherheit zum Schutz Ihres Unternehmens bei. Dieser Service ist insbesondere auf mittelständische Unternehmen zugeschnitten.<sup>1</sup> Mit einem Konzept für das Management der Endgerätesicherheit, bei dem der Schutz oberste Priorität hat, senkt Proactive Security das Risiko, Opfer von Cyberangriffen zu werden. Die Benutzer erhalten damit außerdem die Freiheit, sicher vom gewünschten Ort aus zu arbeiten, ohne dass dadurch die Arbeitsbelastung der IT steigt.

Proactive Security beinhaltet mehrstufigen Schutz vor Malware auf Enterprise-Niveau. Dabei werden Deep Learning und Isolationstechnologien mit handlungsrelevanten Erkenntnissen und dem Management durch Cybersicherheitsexperten kombiniert und als Managed Service bereitgestellt.

## Merkmale und Spezifikationen

### Schutz

HP Proactive Security sorgt für umfassenden Schutz von Computing-Endgeräten auf unterschiedlichen Ebenen und integriert dabei HP Sure Sense Advanced sowie HP Sure Click Advanced.<sup>2</sup>

Die auf Deep Learning basierende Schutztechnologie von HP Sure Sense Advanced wurde auf Grundlage von mehreren Hundert Millionen Malware-Beispielen trainiert und kann nun selbst sorgfältig maskierte Malware-Dateien leicht erkennen und auch dateilose Bedrohungen anhand ihrer Eigenschaften statt eindeutiger Signaturen herausfiltern. Die Lösung ist in der Lage, nicht nur bekannte Malware zu stoppen, sondern auch völlig neue Zero-Day-Malware erfolgreich aufzuspüren – ohne dass der Client aktualisiert werden muss.

HP Sure Click Advanced nutzt Isolationstechnologie auf Enterprise-Niveau als letzte Verteidigungslinie, um Sicherheitsbedrohungen einzudämmen, die andere Abwehrmechanismen für Endgeräte umgehen konnten. E-Mail-Anhänge, heruntergeladene Dateien und selbst Inhalte von USB-Laufwerken werden durch die Anwendungsisolation auf den PCs der Benutzer in separaten Mikro-VMs geöffnet. So lassen sich diese vor Cyberangriffen schützen, während gleichzeitig die Bedrohungsaktivität während der Isolation überwacht wird. Damit gewinnen Sie einen detaillierteren Einblick in die Attack-Kill-Chain.

Durch die Kombination dieser beiden intelligenten und sich ergänzenden Technologien bietet HP Proactive Security proaktiven, mehrstufigen Echtzeitschutz für Ihre Geräte.

## Merkmale und Spezifikationen (Forts.)

### Erkenntnisse

HP Proactive Security stellt den Kunden über HP TechPulse, eine leistungsfähige Analyseplattform auf Grundlage künstlicher Intelligenz, handlungsrelevante Erkenntnisse bereit.<sup>3</sup> Ihre IT-Teams können den Schutzstatus von Geräten überwachen, Berichte einsehen und Warnungen im Hinblick auf ungeschützte Geräte und blockierte Bedrohungsaktivitäten erhalten – über ein einheitliches, zentrales Dashboard.

### Management

Anders als reine Softwarelösungen wird HP Proactive Security als Managed Service bereitgestellt. HP Sicherheitsexperten implementieren und steuern in Ihrem Auftrag die Konfigurations- und Sicherheitsrichtlinien, unter anderem das Management der Bedrohungsquarantäne. Nach dem Onboarding der Geräte überwachen die HP Sicherheitsexperten den Schutzstatus der Gerätesicherheit und führen forensische und Kill-Chain-Analysen von völlig neuen Zero-Day-Bedrohungen durch, damit Sie besser vor künftigen Angriffen geschützt sind.

### Zugriff auf CyQu von Aon

Mit HP Proactive Security erhalten Sie Zugriff auf Cyber Quotient Evaluation (CyQu) von Aon. Über dieses Online-Tool für die Bewertung Ihrer Sicherheitslage erhalten Sie einen Online-Score Ihres Sicherheitsprofils. Sie haben außerdem die Möglichkeit eines Opt-ins für einen Incident-Response-Retainer (kostenlos, incl. einer Stunde Beratung) mit bevorzugter Reaktion auf Vorfälle und einem beschleunigten Antragsprozess für Cyberversicherungspolizen.<sup>4</sup>

Kategorie	Merkmale
Schutz	KI-basierte Bedrohungsabwehr von HP Sure Sense Advanced für Geräte mit Windows 10, Mac OS und Android
	HP Sure Click Advanced zur Anhangs- und Downloadisolierung für Windows 10
Sicherheitsberichte	Compliance-Bericht zur Unternehmenssicherheit
	Bericht zu kompromittierten Geräten
	Compliance-Bericht zur Gerätesicherheit
	Bericht zu nicht berichtenden Geräten
	Sicherheitsbericht von HP Sure Click Advanced
	Aktivitätsbericht von HP Sure Recover
	Einstellungsbericht von HP Sure Recover
	Sicherheitsbericht von HP Sure Sense Advanced
Sicherheitsvorfälle	Systemintegritätsbericht von HP Sure Start
	HP Sure Click – ungeschütztes Gerät
	HP Sure Click – echte positive Bedrohung isoliert
	HP Sure Sense – ungeschütztes Gerät
Kontinuierliches Management	HP Sure Sense – Bedrohung verhindert
	Optimierung und Richtliniendurchsetzung
	Bedrohungsanalyse und -informationen
	Statusuntersuchung von Sicherheitsagenten
Weitere Merkmale	Update von Sicherheitsagenten
	Detaillierter Bedrohungsbericht von Sure Click Advanced <sup>5</sup>
	CyQu von Aon, ein Online-Tool zur Bewertung Ihrer Sicherheitslage mit Opt-in-Möglichkeiten für die Reaktion auf Vorfälle und Cyberversicherungsservices von Aon <sup>4</sup>
	SIEM-Unterstützung mit HP APIs

## Service details

Auf den von HP verwalteten Geräten werden Softwareagenten installiert, die für Echtzeitschutz sorgen und Informationen über die Geräte erfassen. Eine Internetverbindung ist erforderlich, um die Sicherheitsrichtlinien einzurichten oder zu aktualisieren und Ihnen die Informationen bereitzustellen. Nach Abschluss der Einrichtung ist für den Schutz über diese Softwareagenten keine Internetverbindung erforderlich. Vertrauliche Benutzerdaten wie Anmeldedaten, Dateien, Inhalte und personenbezogene Daten werden nicht erfasst. Die erfassten Daten werden in einem sicheren Repository in der Cloud abgelegt.<sup>6</sup>

Ihnen wird ein Portal zur Verfügung gestellt, über das Sie auf Ihre Sicherheitsinformationen zugreifen können, z. B. ein Dashboard, Berichte, Vorfälle etc.

Zertifizierte Sicherheitsexperten verwalten die Endgerätesicherheit proaktiv für Sie. Dazu gehören die Optimierung und Durchsetzung der Sicherheitsrichtlinien, die Analyse der Vorfälle, wenn eine echte positive Bedrohung erkannt wird, die Bereitstellung eines detaillierten Analyseberichts, wenn eine neue, neuartige oder Zero-Day-Bedrohung von Sure Click Advanced gefunden wird, das Management von Updates der Sicherheitsagenten, die Untersuchung von Problemen rund um den Agentenstatus und vieles mehr.

Ein HP Service-Experte leistet First-Level-Kundensupport und arbeitet mit HP internen Teams, einschließlich der Sicherheitsexperten, zusammen, um die von Ihnen gemeldeten Probleme zu lösen. Die HP Service-Experten sind wie folgt verfügbar:

- **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 7:00 Uhr bis 18:00 (GMT - 5).
- **Europa, Naher und Mittlerer Osten und 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 (MEZ).
- **Asien Pazifik und Japan:** Support in englischer Sprache 24 Stunden am Tag und in japanischer Sprache von 9:00 Uhr bis 21:00 Uhr (Japan Standard Time) an 7 Tagen der Woche (außer an bei HP arbeitsfreien Tagen).

### Mitwirkungspflicht des Kunden

- Bereitstellung der erforderlichen Informationen für die Einrichtung eines Kontos durch HP
- Implementierung der Proactive Security Agenten auf Ihren verwalteten Geräten
- Anforderung des Hinzufügens oder Entfernens von verwalteten Benutzern und Geräten
- Anforderung des Hinzufügens oder Entfernens von Download-Sites und E-Mail-Domänen zur Whitelist (zur Isolierung von Dateianhängen)
- Anforderung des Hinzufügens oder Entfernens von IP-Adressbereichen des Unternehmens, die nicht isoliert werden sollen
- Anforderung oder Genehmigung der Freigabe oder des Ausschlusses von Dateien, die unter Quarantäne gestellt oder blockiert wurden
- Anmeldung an der HP TechPulse Konsole, um Dashboards, Berichte und Vorfälle zu prüfen
- Prüfen von Sicherheitsberichten und entsprechende Reaktion
- Teilnahme an der Onlinebefragung von CyQu<sup>4</sup>



## Systemanforderungen

Plattform	Betriebssystemanforderungen	Hardwareanforderungen <sup>7</sup>
<b>Windows</b>	Aktuelles allgemein verfügbares Release von Windows 10 oder zwei vorhergehende Hauptreleases	<b>HP Sure Click Advanced<sup>2,8</sup></b> <ul style="list-style-type: none"> <li>• Intel Core i3, i5, i7 (oder eine moderne CPU von AMD) mit aktivierter Virtualisierungstechnologie im BIOS/UEFI</li> <li>• Mindestens 4 GB RAM (8 GB empfohlen)</li> <li>• Mindestens 6 GB freier Plattenspeicherplatz</li> </ul> <b>HP Sure Sense Advanced</b> <ul style="list-style-type: none"> <li>• Mindestens 4 GB RAM</li> </ul>
<b>MacOS</b>	MacOS 10.12 oder höher	<b>HP Sure Click Advanced</b> <ul style="list-style-type: none"> <li>• Auf MacOS-Geräten nicht unterstützt</li> </ul> <b>HP Sure Sense Advanced</b> <ul style="list-style-type: none"> <li>• Keine besonderen Hardwareanforderungen unter MacOS</li> </ul>
<b>Android</b>	Android V5.0 oder höher	<b>HP Sure Click Advanced</b> <ul style="list-style-type: none"> <li>• Auf Android-Geräten nicht unterstützt</li> </ul> <b>HP Sure Sense Advanced</b> <ul style="list-style-type: none"> <li>• Keine besonderen Hardwareanforderungen unter Android</li> </ul>

### Anforderungen hinsichtlich Drittanbietersoftware

Adobe Acrobat Reader DC muss die Standardanwendung für PDF-Dateien sein.

### Netzwerkanforderungen

Für die Kommunikation zwischen den verwalteten Geräten und dem Cloud-Management-Service ist eine Internetverbindung erforderlich.

### Voraussetzungen

Damit der Service genutzt werden kann, muss er entsprechend der Anleitung von HP nach dem Kauf registriert werden. Während des Onboarding-Prozesses müssen Sie Informationen bereitstellen, die für die Einrichtung der Konten und Sicherheitsrichtlinien erforderlich sind.



## Serviceeinschränkungen

HP Proactive Security ist kein kontinuierlicher Überwachungsservice in Echtzeit. HP Sure Sense Advanced und HP Sure Click Advanced blockieren oder isolieren nicht vertrauenswürdige oder schädliche Inhalte automatisch und stellen damit den Schutz auf Ihren Geräten sicher.

HP Proactive Security umfasst keine Services für die Schadensbehebung oder Wiederherstellung im Falle einer Sicherheitsverletzung. Services für die Schadensbehebung und Wiederherstellung sind separat von HP Partnern, einschließlich Aon, erhältlich.

## Geschäftsbedingungen

Die Geschäftsbedingungen von HP Care Pack können gelten, wenn der Service als ein HP Care Pack erworben wurde. Die Geschäftsbedingungen von HP TechPulse, die Hinweise von HP zu den Rechten in Bezug auf personenbezogene Daten und die Datenschutzerklärung von HP finden alle auf den Service Anwendung.

## Weitere Informationen

Weitere Einzelheiten erhalten Sie über Ihren HP Partner oder Vertriebsbeauftragten vor Ort oder unter [hp.com/proactive-security](https://hp.com/proactive-security)

Melden Sie sich noch heute für Updates an.  
[hp.com/go/getupdated](https://hp.com/go/getupdated)



Mit Kollegen teilen

1. HP Services unterliegen den für den jeweiligen Service geltenden HP Geschäftsbedingungen, die dem Kunden zum Zeitpunkt des Kaufs bereitgestellt oder genannt werden. Der Kunde kann möglicherweise gemäß länderspezifischen Gesetzen zusätzliche Ansprüche geltend machen. Diese Ansprüche bleiben durch die HP Geschäftsbedingungen in Bezug auf den Service oder die HP Herstellergarantie des HP Produkts unberührt. Die vollständigen Systemvoraussetzungen finden Sie unter [hpdaas.com/requirements](https://hpdaas.com/requirements).
2. Die in HP Proactive Security enthaltene HP Sure Click Advanced Technologie erfordert Windows 10 und Microsoft Internet Explorer, Google Chrome oder Chromium. Zu den unterstützten Anhängen zählen u. a. Microsoft Office- (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office bzw. Adobe Acrobat installiert ist. HP Sure Click Advanced kann nicht für vereinfachtes Chinesisch installiert werden.
3. HP verfolgt oder überwacht keine Details, die zeigen, welche URLs ein Benutzer besucht hat. Die Berichterstellung in HP TechPulse konzentriert sich auf die Ermittlung von Bedrohungen und ihrer Quelle. HP TechPulse ist DSGVO- und ISO 27001-konform.
4. Aon Services sind nur in den USA verfügbar. Käufer des HP Proactive Security Service in den USA erhalten die Selbstbeurteilung und den Sicherheitsscore von Aon CyQu. Dies beinhaltet einen kostenlosen Retainer. Außerdem stellt Aon im Fall einer Sicherheitsverletzung einen Ansprechpartner zur Beratung für eine Stunde bereit, um auf den Vorfall zu reagieren. Eine entsprechende Anleitung erhalten Sie von Ihren HP Ansprechpartnern für den Onboarding-Service.
5. Die Bedrohungsanalyse durch HP Service-Experten ist ein forensischer Prozess, der ausgelöst wird, nachdem ein Malware-Ereignis durch den Software-Client von HP Sure Click Advanced blockiert oder isoliert wurde. Es handelt sich nicht um einen 24x7-Überwachungsservice in „Echtzeit“. Der Client-Agent von HP Sure Click Advanced isoliert nicht vertrauenswürdige oder schädliche Inhalte automatisch und stellt dadurch den Schutz sicher, bevor die Analyse gestartet wird. Zudem enthält keiner der Tarife Services für die Schadensbehebung oder Wiederherstellung im Falle einer Sicherheitsverletzung. Services für die Schadensbehebung und Wiederherstellung sind separat von HP Partnern, einschließlich Aon, erhältlich.
6. Die Daten werden bei der Übertragung vom Geräteclient an den Web-Server per SSL geschützt. Auf die Daten kann nur über den HP DaaS Web-Server zugegriffen werden.
7. Der Kunde kann Technologien (HP Sure Sense Advanced oder HP Sure Click Advanced) teilweise implementieren, wenn sein System die Mindestvoraussetzungen nicht erfüllt.
8. Eine vollständige Liste der unterstützten Windows 10-Versionen finden Sie in der Bromium Richtlinie zur Windows-Unterstützung. Hinweis: Windows 7 und 8.1 werden von HP Proactive Security nicht unterstützt.

© Copyright 2020 HP Development Company, L.P. Die hierin enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern. Die Garantien für HP Produkte und Services werden ausschließlich in der entsprechenden, zum Produkt oder Service gehörigen Garantieerklärung beschrieben. Die hierin enthaltenen Informationen stellen keine zusätzliche Garantie dar. HP haftet nicht für hierin enthaltene technische oder redaktionelle Fehler oder Auslassungen. Adobe und Acrobat sind Marken von Adobe Systems Incorporated. Apple und macOS sind Marken von Apple Inc. und in den USA und anderen Ländern eingetragen. Android, 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.

