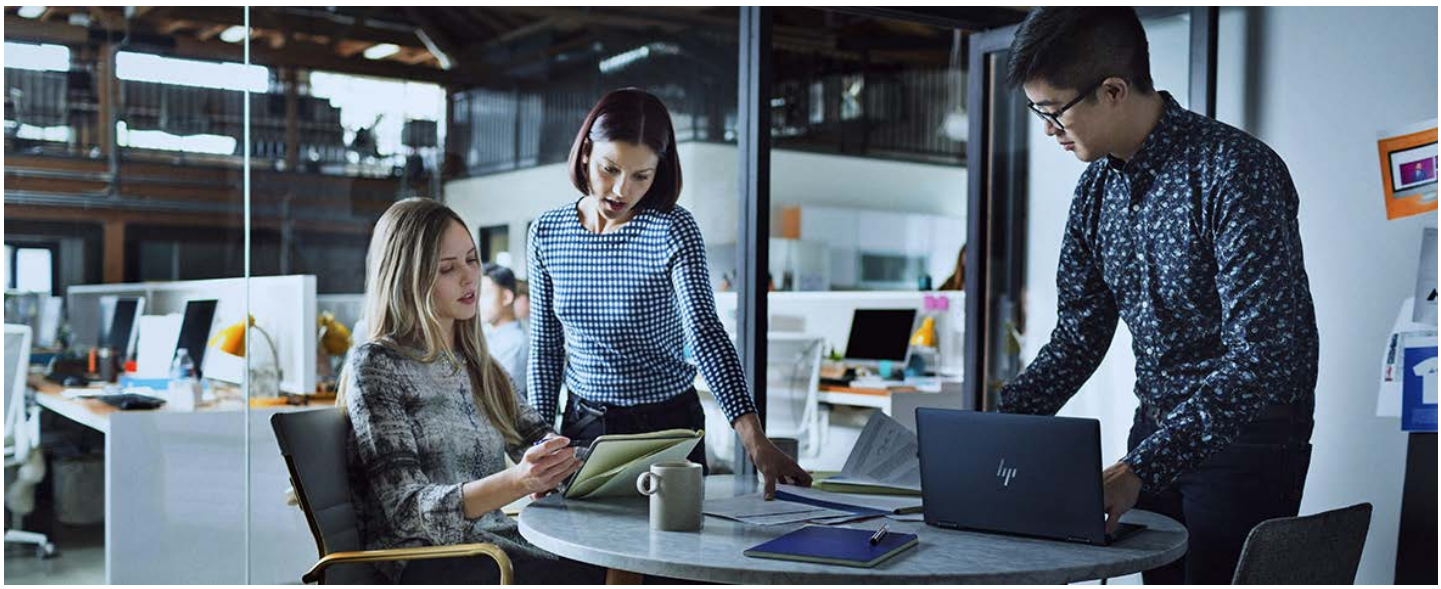
HP WOLF PRO SECURITY SERVICE

HP WOLF SECURITY



SERVICEÜBERSICHT

Vorteile des Service

- Stoppen Sie bislang unbekannte Zero-Day-Angriffe und den Diebstahl von Zugangsdaten durch verstärkende Schutzebenen.
- Sichern Sie sich Ihre Endgeräte mit Isolationstechnologie auf Unternehmensniveau.
- 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 mehreren Ebenen.
- Expertenüberwachung und -verwaltung durch branchenzertifizierte Sicherheitsprofis.
- Zeitnahe, handlungsrelevante Analytik und Erkenntnisse

HP Wolf Pro Security Serviceträgt auf mehreren Ebenen für Endgerätesicherheit zum Schutz Ihres Unternehmens bei. Dieser Service ist insbesondere auf wachsende und reifende Unternehmen zugeschnitten.[1] Mit einem Konzept für das Management der Endgerätesicherheit, bei dem der Schutz oberste Priorität hat, sinkt das Risiko, Opfer von Cyberangriffen zu werden. Die Benutzer können sicher von jedem gewünschten Ort aus zu arbeiten, ohne dass ihre Produktivität eingeschränkt wird oder die die Arbeitsbelastung für die IT-Abteilung zunimmt.

HP Wolf Pro Security Service beinhaltet verstärkende Schichten für Malware-Schutz auf Enterprise-Niveau. Der Service kombiniert fortschrittliche Antivirus-Software der nächsten Generation, basierend auf neuester KI-Technologie wie Deep Learning, Schutz vor Zugangsdatendiebstahl und Isolationstechniken auf Verteidigungsniveau mit umsetzbaren Erkenntnissen in Echtzeit sowie kontinuierlicher Bedrohungsüberwachung durch Experten für Cybersicherheit.

MERKMALE UND SPEZIFIKATIONEN

Schutz

HP Wolf Pro Security Service bietet fortschrittlichen, mehrstufigen Schutz für Computing-Endgeräte.

Das KI-System in HP Wolf Pro Security Service nutzt eine Kombination aus maschinellem Lernen, Deep Learning und anderen Techniken, um selbst sorgfältig maskierte Malware-Dateien zu erkennen, ebenso wie dateilose Bedrohungen basierend auf ihren Eigenschaften, statt auf eindeutigen Signaturen. Die Lösung ist in der Lage, nicht nur bekannte Bedrohungen zu stoppen, sondern ebenfalls vollkommen neue Zero-Day-Malware erfolgreich zu erkennen, ohne dass der Client aktualisiert werden muss.

FEATURES UND SPEZIFIKATIONEN (FORTSETZUNG)

Darüber hinaus schützt HP Wolf Pro Security Service Mitarbeiter vor der häufigsten Art von Verstößen: Phishing-Attacken zum Diebstahl von Zugangsdaten. Der Identitätsschutz von HP Wolf Pro Security verhindert die Passworteingabe durch Benutzer auf Websites, die für den Diebstahl von Zugangsdaten erstellt wurden, und die ein Benutzer möglicherweise durch versehentliches Anklicken eines Phishing-Links in einer E-Mail, einem Chat-Client, einem PDF-Dokument oder einer anderen Datei aufruft.

Die Isolationstechnologie auf Enterprise-Niveau von HP Wolf Pro Security ist die letzte Verteidigungslinie zur Eindämmung selbst unsichtbarer Bedrohungen,die andere Endgeräte-Verteidungsmechanismen des Kunden umgangen haben und von diesen nicht erkannt wurden.. Dieser hardwaregestützte Isolationsschutz ermöglicht ein sicheres Öffnen, Bearbeiten, Drucken und Speichern von E-Mail-Anhängen, Datei-Downloads und selbst Inhalten von USB-Laufwerken innerhalb ihrer eigenen sicheren virtuellen Mikromaschine. Während sie geöffnet sind, werden die Anwendungen automatisch hinsichtlich Bedrohungsaktivitäten überwacht und der HP Wolf Security Controller liefert eine vollständige Analyse der Angriffs-Kill-Chain für Bedrohungsvorfälle, um Ihnen ein besseres Verständnis der Natur der Bedrohung
und einen besseren Schutz vor zukünftigen Angriffen zu ermöglichen.

Durch die Kombination dieser fortschrittlichen und sich ergänzenden Technologien bietet HP Wolf Pro Security Service proaktiven Echtzeitschutz auf mehreren Ebenen für Ihre Geräte.

Erkenntnisse
HP Wolf Pro Security Service liefert Kunden umsetzbare Erkenntnisse durch den HP Wolf Security Controllereine leistungsstarke Analytikplattform.[2] Ihr IT-Team kann den Schutzstatus der Geräte überwachen, Berichte einsehen und Warnmeldungen über ungeschützte Geräte sowie blockierte Bedrohungsaktivitäten erhalten – all dies über ein einheitliches Cloud-basiertes Dashboard.

Expertenüberwachung und -verwaltung[3]
Im Gegensatz zu reinen Software-Lösungen wird HP Wolf Pro Security Service als überwachter Service bereitgestellt. HP Sicherheitsexperten implementieren und steuern in Ihrem Auftrag die Konfigurations- und Sicherheitsrichtlinien, unter anderem die kontinuierliche kontinuierliche Umsetzung von Sicherheitsrichtlinien der Bedrohungsquarantäne. Nach dem Onboarding der Geräte überwachen die HP Sicherheitsexperten den Schutzstatus der Geräte und führen forensische sowie Kill-Chain-Analysen bisher unbekannter Zero-Day-Bedrohungen durch, damit Sie besser vor künftigen Angriffen geschützt sind.

Kategorie	Merkmale
Schutz	HP Sure Sense Pro – KI-basierter Schutz vor Bedrohungen für Windows 10[4]
	HP Sure Click Pro[5] – Isolation von Anhängen und Downloads für Windows 10
	HP Identity Protection verhindert die versehentliche Offenlegung von Benutzerpasswörtern auf Websites für den Diebstahl von Zugangsdaten
Sicherheitsanalytik	Geräteschutz-Dashboard
	Bedrohungsdaten aus HP Sure Click Pro und HP Sure Sense Pro
	Detaillierte Informationen zum Geräteschutzstatus
	Vollständige Kill-Chain-Analyse der Bedrohungen auf Basis des MITRE ATT&CK™ Frameworks[6]
Kontinuierliches Service-Management	Controller-Einrichtung, Einstellung und Richtliniendurchsetzung
	Bedrohungsanalyse und -informationen
	Quarantäne- und Exklusionsmanagement
	Untersuchung zum Status des Security Agents
	Update-Bereitstellung für den Security Agent
Weitere Merkmale	SIEM-Integration über Syslog-Feed

BEREITSTELLUNGS-SPEZIFIKATIONEN

Kunden müssen die Sicherheits- und Analytik-Client-Software auf verwalteten Geräten installieren. Eine Internetverbindung ist für den Zugriff auf Analytik und Berichte sowie für den Empfang von Richtlinien-Aktualisierungen und Software-Upgrades erforderlich. 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.[2]

HP ermöglicht dem HP Wolf Security Controller Zugriff auf Sicherheitsinformationen, einschließlich eines Dashboards, Berichten, Vorfällen und mehr.

Zertifizierte HP 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, das Management von Updates der Sicherheitsagenten, die Untersuchung von Problemen rund um den Agent-Status 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 arbeitsfreien Tagen bei HP) von 6:00 Uhr bis 18:00 Uhr (MT).

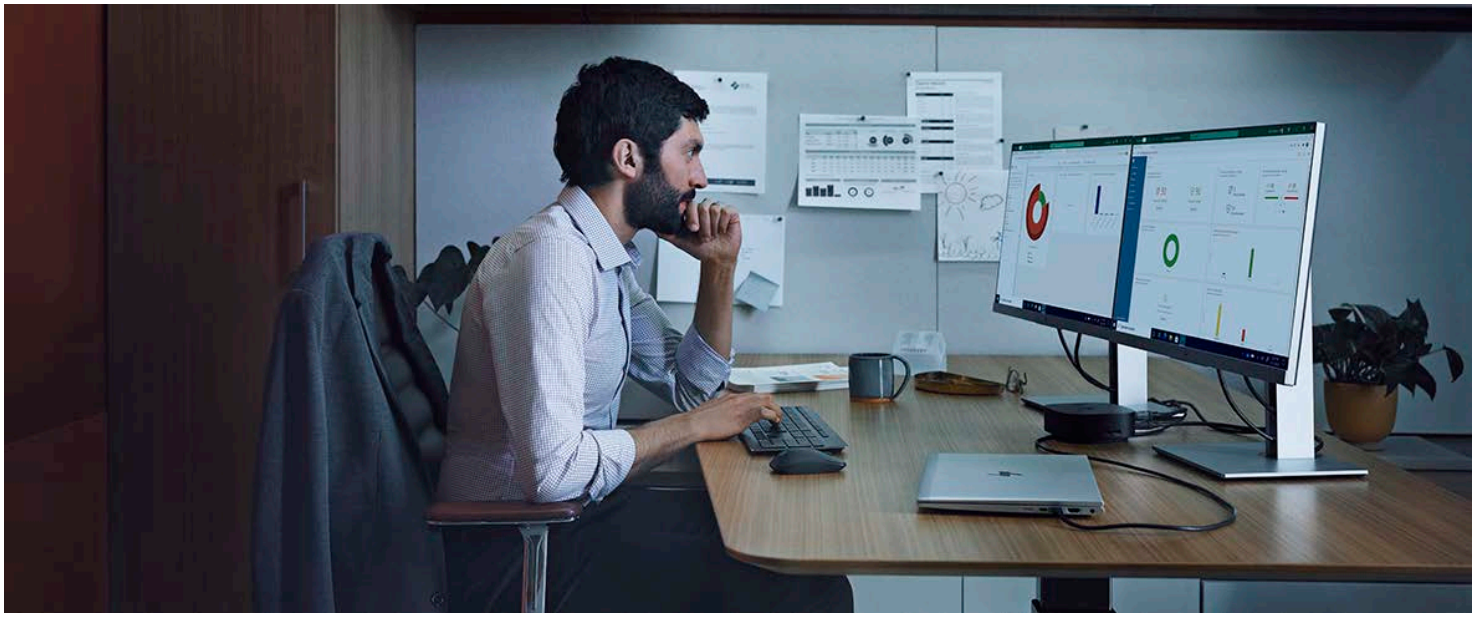
Lateinamerika: Support in englischer und spanischer Sprache von Montag bis Freitag (außer an arbeitsfreien Tagen bei HP) von 07:00 Uhr bis 18:00 Uhr, GMT - 5.

Europa, Naher Osten, Afrika: Support in englischer, französischer und deutscher Sprache von Montag bis Freitag (außer an arbeitsfreien Tagen bei HP) von 08:00 Uhr bis 18:00 Uhr (MEZ).

Asiatisch-pazifischer Raum und Japan: Support in englischer Sprache ist innerhalb der gesamten Region 24 Stunden täglich verfügbar. Der Support in englischer Sprache für Japan steht von 9:00 Uhr bis 21:00 Uhr Japan-Standardzeit an 7 Tage pro Woche zur Verfügung (ausgenommen arbeitsfreie Tage bei HP).

Mitwirkungspflicht des Kunden

- Bereitstellung der erforderlichen Informationen für die Einrichtung des Kundenkontos durch HP.
- Bereitstellung des HP Wolf Pro Security Agent auf Ihren verwalteten Geräten.
- Anfragen für das Hinzufügen oder Entfernen von zulässigen Websites für den Download, Ausschlüssen und E-Mail-Domaineinstellungen (für die Isolation von Dateianhängen, KI-basierten Malware-Schutz sowie die Verhinderung von Zugangsdatendiebstahl).
- Anfragen für das Hinzufügen oder Entfernen von IP-Adressbereichen, die nicht isoliert werden sollen.
- Anforderung oder Genehmigung der Freigabe oder des Ausschlusses von Dateien, die unter Quarantäne gestellt oder blockiert wurden.
- Anmeldung im HP Wolf Security Controller Portal, um Dashboards, Berichte und Vorfälle anzuzeigen.
- Prüfen von Sicherheitsberichten und entsprechende Reaktion



SYSTEMANFORDERUNGEN

HP Wolf Pro Security unterstützt Systeme mit Windows 10 und unterstützten Intel® oder AMD Prozessoren. Die aktuellen Systemanforderungen finden Sie unter https://www.hpdaas.com/requirements

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 Wolf Pro Security Service ist kein kontinuierlicher Echtzeit-Überwachungsservice. HP Sure Sense Pro und HP Sure Click Pro blockieren oder isolieren nicht vertrauenswürdige oder schädliche Inhalte automatisch und stellen damit den Schutz auf Ihren Geräten sicher. HP Wolf Pro Security Service Wolf Pro Security Service umfasst keine Services für die Schadensbehebung oder Wiederherstellung im Fall einer Sicherheitsverletzung. Services für die Schadensbehebung und Wiederherstellung sind separat von HP Partnern erhältlich.

GESCHÄFTSBEDINGUNGEN

Die Geschäftsbedingungen von HP Care Pack können gelten, wenn der Service als HP Care Pack erworben wurde. Die Geschäftsbedingungen von HP TechPulse, die Hinweise von HP zu den Rechten hinsichtlich personenbezogener Daten und die Datenschutzerklärung von HP gelten alle für diesen Service.

WEITERE INFORMATIONEN

Für Details wenden Sie sich bitte an Ihren HP Vertreter vor Ort oder besuchen Sie https://www8.hp.com/us/en/services/pro-security-service.html

1 HP Services unterliegen den für den jeweiligen Service geltenden HP Geschäftsbedingungen, die entweder angegeben sind oder dem Kunden zum Zeitpunkt des Erwerbs mitgeteilt werden. Der Kunde kann möglicherweise gemäß länderspezifischen Gesetzen zusätzliche Ansprüche geltend machen. Diese Ansprüche bleiben von den HP Geschäftsbedingungen in Bezug auf den Service oder die HP Herstellergarantie des HP Produkts unberührt. Eine vollständige Liste der Systemanforderungen finden Sie unter https://www.hpdaas.com/requirements.

2 HP verfolgt oder überwacht keine Details, die zeigen, welche URLs ein Benutzer besucht hat. Die Berichte konzentrieren sich auf die Identifizierung von Bedrohungen und ihrer Quelle im HP Wolf Security Controller. Der HP Wolf Security Controller ist DSGVO- und ISO 27001-konform. HP Wolf Pro Security Controller ist nicht als eigenständiges Produkt verfügbar und erfordert HP Wolf Pro security Service. Die vollständigen Systemvoraussetzungen finden Sie unterhttp://www.hpdaas.com/ requirements. Die HP Services unterliegen den gültigen allgemeinen 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 von den HP Geschäftsbedingungen in Bezug auf den Service oder die HP Herstellergarantie des HP Produkts unberührt.

3 Die Bedrohungsanalyse durch HP Sicherheitsexperten ist ein forensischer Prozess, der verfügbar ist, nachdem ein Malware-Ereignis durch den Software-Agent von HP Wolf Pro Security blockiert oder isoliert wurde. Es handelt sich nicht um einen 24x7-Überwachungsservice in „Echtzeit". Weitere Informationen zu diesem Service finden Sie in der HP Wolf Pro Security Service Definition. HP Wolf Pro Security Service Agent isoliert automatisch Inhalte, die nicht vertrauenswürdig oder schädlich sind, und gewährleistet dadurch Schutz, bevor die Analyse gestartet wird. Zudem enthält keiner der Tarife Services für die Schadensbehebung oder Wiederherstellung im Fall einer Sicherheitsverletzung.

4 Eine vollständige Liste der unterstützten Versionen von Windows 10 finden Sie unter https://www.hpdaas.com/requirements. Bitte beachten Sie, dass Windows 7 und 8.1 werden von HP Wolf Pro Security Service nicht unterstützt werden.

5 Die HP Sure Click Pro Technologie ist in HP Wolf Pro Security Service enthalten, erfordert Windows 10 Pro oder Enterprise und unterstützt Microsoft Internet Explorer, Google Chrome, Chromium, Mozilla Firefox sowie neue Edge-Versionen. Zu den unterstützten Anhängen gehören u. a. Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office bzw. Adobe Acrobat installiert ist. Weitere Details finden Sie unter https://www.hpdaas.com/requirements.

6 MITRE behauptet nicht, dass in ATT&CK alle Möglichkeiten für die Arten von Aktionen und Verhaltensweisen aufgeführt sind, die im Rahmen seines Modells und Frameworks von Techniken für feindliche Verhaltensweisen dokumentiert sind. Die Anwendung der in ATT&CK enthaltenen Informationen auf vollständige Technik-Kategorien garantiert keinen vollständigen Schutz, da ATT&CK bisher unbekannte oder Variationen bestehender Techniken möglicherweise nicht dokumentiert.

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

Mit Kollegen teilen

Dieses Dokument bewerten

HP WOLF SECURITY

4AA7-4656DEE, Mai 2021, Rev. 5