



HP Wolf Pro Security

Datenblatt



HP WOLF SECURITY

Umfassende
PC-Sicherheit,
leicht gemacht.



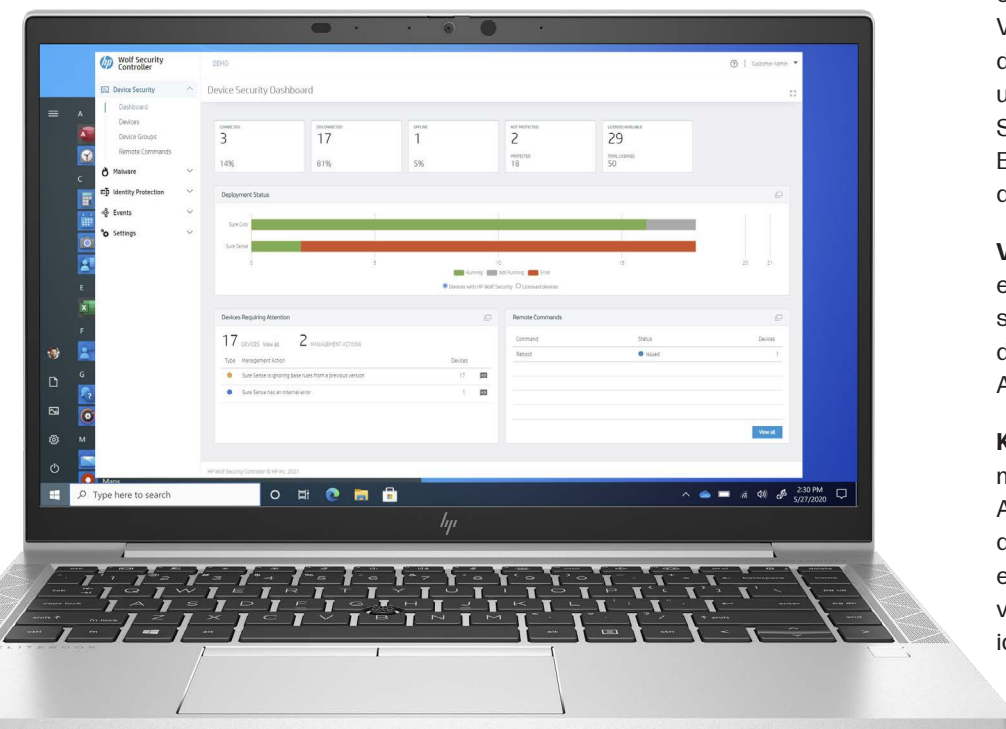
Kleine und mittelständische Unternehmen sind oft aufgrund unzureichender Ausstattung und Schulung des Sicherheitspersonals anfällig für Cyberangriffe, einschließlich Phishing und Ransomware. Diese Angriffe wiederum können zu kostspieligen Problemen führen, unter anderem auch zu kompromittierten Systemen, gestohlenen Daten und langen Ausfallzeiten.

HP Wolf Pro Security (WPS) unterstützt kleine und mittelständische Unternehmen bei der Bewältigung dieser Herausforderungen mit einer einfachen Lösung, die die maximale Sicherheitsabdeckung bietet, ohne dabei die Arbeitsbelastung der IT-Abteilung zu erhöhen oder die Produktivität der Mitarbeiter:innen zu beeinträchtigen.

Einfache Sicherheit, die einfach bereitzustellen und zu bedienen ist

HP WPS ist eine umfassende Endpoint Security Lösung, die auf Einfachheit ausgelegt ist. Sie umfasst eine unkomplizierte Verwaltung von Richtlinien, eine mühelose Pflege von Lösungen und ein kontinuierliches Alarmmanagement, wodurch sie einfach bereitzustellen und zu verwalten ist.

HP Wolf Security Controller



Der Cloud-basierte Controller, bekannt als HP Wolf Security Controller¹, bietet ein zentrales Command Center für die Verwaltung der Sicherheit und des Zustands der gesamten PC-Flotte des Unternehmens und gibt Administrator:innen die Möglichkeit, Sicherheitsrichtlinien jederzeit anpassen und Erkenntnisse über Bedrohungen von überall aus überprüfen zu können.

Vorkonfigurierte „out-of-the-box“-Richtlinien ermöglichen eine schnelle Bereitstellung, sind einfach zu verstehen und erfordern für die meisten Umgebungen wenig laufende Anpassungen.

Kontinuierliche Sicherheitswarnungen machen Endbenutzer:innen auf böswillige Aktivitäten aufmerksam, benachrichtigen sie aber nur dann, wenn ihre Aufmerksamkeit erforderlich ist, und machen es einfach, verdächtige Aktivitäten auf dem PC zu identifizieren.

Schützen sie ihre mitarbeiter:innen, ohne sie auszubremsten

Mitarbeiter:innen sind keine Sicherheitsexpert:innen, und es ist unrealistisch zu erwarten, dass sie immer „auf der Hut“ sind, um Social-Engineering-Angriffe zu erkennen. Sicherheitsmaßnahmen, die Mitarbeiter:innen daran hindern, ihre Arbeit zu erledigen, reichen für kein Unternehmen aus, das von seinen Mitarbeiter:innen erwartet, dass sie sicher und produktiv arbeiten.

HP WPS bietet eine umfassende Endpoint Security, die PC-Anwender/die PC-Anwenderin schützt und den Mitarbeiter:innen ein positives Benutzererlebnis bietet, was zu einer verbesserten Produktivität führt, während sie gleichzeitig daran arbeitet, ihre Daten, Passwörter und die Systeme des Unternehmens zu schützen.

Mit einer Sicherheitslösung, die hinter den Kulissen arbeitet, **können Ihre Mitarbeiter:innen unbesorgt arbeiten**, ohne dass ihre täglichen Aufgaben dabei behindert werden.

Mitarbeiter:innen können aufhören, als „Sicherheitssensoren“ zu fungieren, und Anhänge und Links sicher öffnen, da sie wissen, dass HP WPS Technologie zur Eindämmung von Bedrohungen verwendet, um diese Bedrohungen sofort zu isolieren.

Dank der Technologie zur Eindämmung von Bedrohungen **können Ihre Mitarbeiter:innen von überall aus sicher arbeiten**, eine Technologie, die selbst dann funktioniert, wenn der PC nicht mit dem Internet verbunden ist, um einen ständigen Schutz zu gewährleisten.

Zuverlässiger schutz, der sich bei allen bedrohungen bewährt hat

HP WPS verwendet eine Sicherheitstechnologie, die HP Kund:innen nachweislich erfolgreich schützt.

Auf PCs mit der Wolf Security-Technologie von HP wurden bereits über 10 Milliarden E-Mail-Anhänge, Webseiten und Downloads geöffnet, ohne dass auch nur eine einzige Kompromittierung gemeldet wurde.

HP WPS umfasst drei Funktionen, die alle über den Wolf Security Controller verwaltet werden.

Die hardwaregestützte Eindämmung von Bedrohungen² isoliert und dämmt Malware-Angriffe über Social Engineering oder andere Methoden ein und verhindert somit, dass sie den PC oder irgendetwas anderes im Netzwerk infizieren.

Der Anti-Phishing-Schutz von Anmeldeinformationen ist ein Schutz der Anmeldedaten, der den Diebstahl von Anmeldeinformationen verhindert, indem er Phishing-Angriffe blockiert, bei denen versucht wird, Benutzer zur Eingabe ihrer Passwörter auf gefälschten Websites zu verleiten.

Das Antivirenprogramm der nächsten Generation erkennt aufkommende Bedrohungen mit Deep-Learning-KI und stoppt zusätzlich bekannte Malware.



Die vorteile einer einfachen sicherheitslösung, die auf benutzerfreundlichkeit und mitarbeiterproduktivität ausgelegt ist

HP Wolf Pro Security eignet sich am besten für Unternehmen, die ihre IT-Supportinvestitionen und -mitarbeiter auf die Maximierung der Benutzererfahrung und Produktivität konzentrieren möchten. Durch den Austausch herkömmlicher Antivirenprogramme durch HP WPS ist das Unternehmen besser geschützt, und die Notwendigkeit, Sicherheitsexperten im Personal zu halten, wird reduziert, wodurch wiederum Ressourcen frei werden, die für wichtigere Aufgaben verwendet werden können.

Geringer Aufwand für die Bereitstellung und die laufende Wartung erfolgt zentralisiert und dadurch einfacher

Geringeres Risiko dank einem auf Prävention ausgerichteten Ansatz für die Endpoint Security, einschließlich KI-Schutz in Echtzeit und hardwaregestützter Zero-Trust-Isolierung

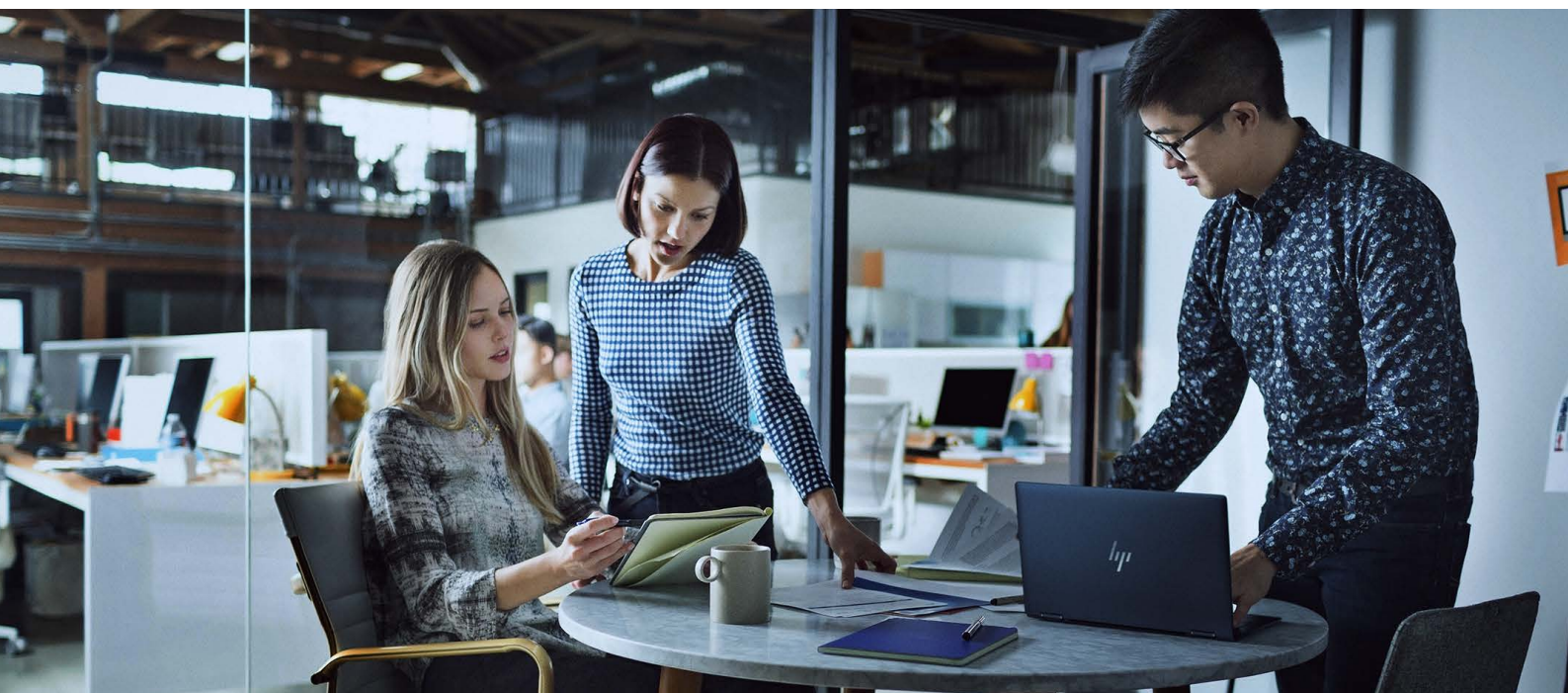
Flexible optionen für jede situation

HP Wolf Pro Security ist in mehreren Verbrauchsoptionen erhältlich, um eine durchgängige Sicherheitslösung bereitzustellen, die Ihren Anforderungen entspricht. Kaufen Sie das Produkt vorinstalliert auf HP Wolf Pro Security Edition-PCs³ oder als eigenständige Software.^{4,5} Sie ist auch für Nicht-HP-PCs verfügbar und bietet Ihnen mehr Flexibilität bei der Bereitstellung von Sicherheit für Ihr Unternehmen auf dem Gerät Ihrer Wahl.

Systemvoraussetzungen für und Komponenten von HP Wolf Pro Security

Wolf Security Controller	Verfügbar für alle Kundeninstallationen ab 25 PCs.
Elemente der Sicherheitssoftware	HP Wolf Pro Security Client für Windows und HP Wolf Security Cloud Controller (Cloud)
Unterstützte Betriebssysteme	Windows 11 (64 Bit); Windows 10 Pro (64 Bit); Windows 10 Enterprise; Windows 10 Enterprise LTSC (nur 64 Bit)
Erforderlicher Arbeitsspeicher/ Laufwerksspeicher	Mindestens 8 GB Systemspeicher (16 GB empfohlen) / 10-20 GB freier Speicherplatz
Sprachunterstützung (Endpoint)	Englisch, Niederländisch, Französisch, Deutsch, Italienisch, Japanisch, Portugiesisch (Brasilianisch), Spanisch, Schwedisch, Serbisch, Kroatisch, Bulgarisch
Sprachunterstützung (Controller)	Englisch, Niederländisch, Französisch, Deutsch, Italienisch, Japanisch, Portugiesisch (Brasilianisch), Spanisch, Schwedisch
Netzwerkanforderungen	Für die Kommunikation zwischen den verwalteten Geräten und dem Cloud-Management-Service für die Bedrohungsanalytik ist eine Internetverbindung erforderlich. Der Schutz funktioniert jedoch auch offline normal und erfordert keine Netzwerkverbindung.
Onboarding-Anforderungen	Damit die Lösung genutzt werden kann, muss sie entsprechend der Anleitung von HP nach dem Kauf aktiviert werden. Während des Onboarding-Prozesses müssen Sie Informationen bereitstellen, die für die Einrichtung der Konten und Sicherheitsrichtlinien erforderlich sind.
Nutzungsbedingungen für die HP Wolf Pro Security Edition	HP Wolf Pro Security Edition ist auf ausgewählten SKUs vorinstalliert verfügbar und beinhaltet abhängig vom erworbenen HP Produkt eine Lizenz mit einer bestimmten Laufzeit, die Ihnen beim Kauf und in Ihrer Bestellbestätigungs-E-Mail mitgeteilt wird. Die HP Wolf Pro Security Edition Software wird unter den Lizenzbedingungen der Endbenutzer-Lizenzvereinbarung (EULA) für die HP Wolf Security Software lizenziert, die Sie unter https://support.hp.com/us-en/document/ish_3875769-3873014-16 finden. Diese EULA unterliegt folgenden Änderungen: „7. Laufzeit. Sofern gemäß den in dieser EULA enthaltenen Bedingungen nicht anderweitig vorzeitig gekündigt wird, ist die Lizenz für die HP Wolf Pro Security Edition 4 Monate nach dem Versanddatum des HP Produkts durch HP wirksam und bleibt für den Zeitraum gültig, der Ihnen beim Kauf und in Ihrer Bestellbestätigungs-E-Mail mitgeteilt wurde („Erstlaufzeit“). Am Ende der Erstlaufzeit können Sie (a) eine Verlängerungslizenz für die HP Pro Wolf Security Edition von HP.com, dem HP Vertrieb oder einem HP Channel Partner erwerben oder (b) mit der Verwendung der Standardversionen von HP Sure Click und HP Sure Sense ohne Zusatzkosten und ohne zukünftige Softwareaktualisierungen oder HP Support fortfahren. Ungeachtet des Vorstehenden erlischt die Lizenz spätestens ein Jahr nach Ablauf der festen Laufzeit der betreffenden Lizenz.“
für HP Wolf Pro Security (Abonnement)	HP Wolf Pro Security ist als Jahresabonnement erhältlich. Die von Ihnen angegebene Kreditkarte wird jedes Jahr automatisch belastet, sofern Sie Ihr Abonnement nicht kündigen. Sie können Ihr Abonnement kündigen, indem Sie eine E-Mail mit dem Betreff „cancel WPS“ an smbcs@hp.com senden. Ab Anfang 2022 können Sie Ihr Abonnement auch in Ihrem Online-Konto kündigen, indem Sie auf „Meine Abonnements“ und dann auf „Meine Abonnements verwalten“ gehen. Stornierungen müssen mindestens zwei (2) Werktage vor dem Datum der automatischen Verlängerung eingereicht werden. Die vollständigen Nutzungsbedingungen finden Sie unter https://www.hp.com/us-en/shop/cv/wolfprosecuritysubscriptiontermsofservice .

Erfahren Sie mehr über [HP Wolf Pro Security](#).



Haftungsausschlüsse

1 HP Wolf Pro Security Controller erfordert mindestens 25 Geräte.

2 Zu den unterstützten Browsern für die Eindämmung von Bedrohungen gehören die folgenden Browser für Microsoft Windows: Microsoft Edge, Google Chrome, Mozilla Firefox und Chromium. Zu den unterstützten Anhängen gehören u. a. Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office bzw. Adobe Acrobat installiert ist.

3 Die HP Wolf Pro Security Edition ist auf ausgewählten SKUs bereits vorinstalliert verfügbar und beinhaltet, je nach erworbenem HP Produkt, eine kostenpflichtige Lizenz für 1 oder 3 Jahre. Die Software der HP Wolf Pro Security Edition wird unter den Lizenzbedingungen der HP Wolf Security Software-/Endbenutzer-Lizenzvereinbarung (EULA) lizenziert, den Sie unter: https://support.hp.com/us-en/document/ish_3875769-3873014-16 finden, wobei diese EULA wie folgt geändert wird: „7. Laufzeit. Die Lizenz für die HP Wolf Pro Security Edition tritt mit der Aktivierung in Kraft und gilt für eine Lizenzdauer von entweder zwölf (12) oder sechsunddreißig (36) Monaten („Erstlaufzeit“), sofern sie nicht früher gemäß den Bestimmungen dieser EULA beendet wird. Am Ende der Erstlaufzeit können Sie entweder (a) eine Verlängerungslizenz für die HP Pro Wolf Security Edition von HP.com, dem HP Vertrieb oder einem HP Channel Partner erwerben oder (b) weiterhin eine eingeschränkte Version der Technologie zur Eindämmung von Bedrohungen, Malwareprävention und zum Schutz von Anmeldeinformationen ohne Zusatzkosten und ohne zukünftige Softwareaktualisierungen oder HP Support verwenden.“

4 HP Wolf Pro Security ist als Jahresabonnement erhältlich. Die von Ihnen angegebene Kreditkarte wird jedes Jahr automatisch belastet, sofern Sie Ihr Abonnement nicht kündigen. Sie können Ihr Abonnement kündigen, indem Sie eine E-Mail mit dem Betreff „cancel WPS“ an smbcs@hp.com senden. Ab Anfang 2022 können Sie Ihr Abonnement auch in Ihrem Online-Konto kündigen, indem Sie auf „Meine Abonnements“ und dann auf „Meine Abonnements verwalten“ gehen. Stornierungen müssen mindestens zwei (2) Werktage vor dem Datum der automatischen Verlängerung eingereicht werden. Die vollständigen Nutzungsbedingungen finden Sie unter <https://www.hp.com/us-en/shop/cv/wolfprosecuritysubscriptiontermsofservice>.



HP WOLF SECURITY

© Copyright 2024. 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.

Microsoft und Windows sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Intel und Core sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

4AA8-0275DEE, Mai 2024