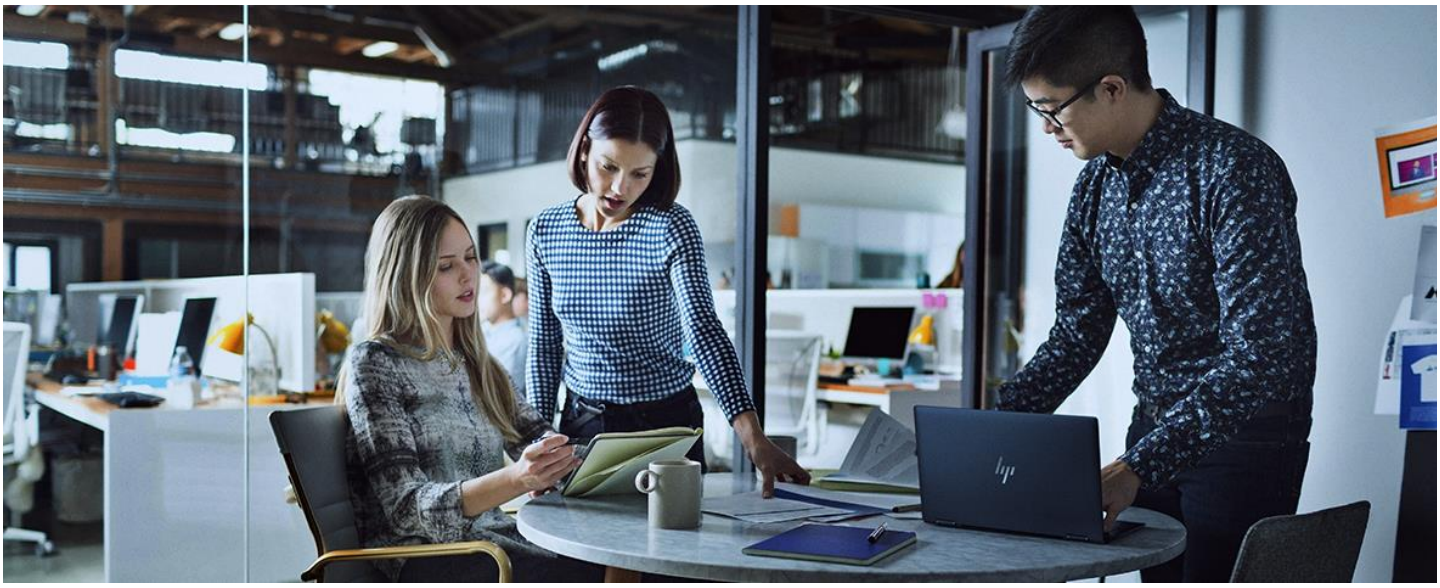
خدمة HP WOLF PRO SECURITY

HP WOLF SECURITY



نظرة عامة على الخدمة

تساعد خدمة HP Wolf Pro Security في الحفاظ على أمان مؤسستك من خلال خدمة أمان لأجهزة الشبكة المتصلة متعددة المستويات بحجم مناسب للأعمال التجارية المتنامية والناضجة.[1] بفضل نهج الحماية في المقام الأول لإدارة حماية الأجهزة المتصلة بالشبكة، ستنخفض مخاطر الهجمات ويمنح المستخدمين حرية العمل دون تعطيل إنتاجيتهم أو زيادة عبء عمل تكنولوجيا المعلومات.

تجمع خدمة HP Wolf Pro Security مستويات معززة من الحماية ضد البرامج الضارة على مستوى المؤسسات. فهي تجمع بين برامج مكافحة الفيروسات المتقدمة من الجيل التالي استنادًا إلى أحدث تقنيات الذكاء الاصطناعي مثل التعلم العميق ومنع سرقة الاعتماد وتقنيات العزل بدرجة الدفاع مع رؤى قابلة للتنفيذ في الوقت الفعلي ومراقبة مستمرة للتهديدات بواسطة خبراء الأمن السيبراني.

الميزات والمواصفات

الحماية

توفر خدمة HP Wolf Pro Security حماية متقدمة ومتعددة المستويات لأجهزة الحاسبات المتصلة بالشبكة.

يستفيد نظام الذكاء الاصطناعي المستخدم في HP Wolf Pro Security Service من مزيج من التعلم الآلي والتعلم العميق والتقنيات الأخرى مما يمكّنه من التعرف بسهولة على ملفات البرامج الضارة المخفية بعناية فائقة فضلاً عن اكتشاف التهديدات التي لا تحتوي على ملفات بناءً على خصائصها بدلاً من الاعتماد على التوقيعات الفريدة. إذ يمكن لهذا الحل اكتشاف برامج ضارة مجهولة وجديدة بنجاح، بالإضافة إلى إيقاف التهديدات المعروفة، فهو يقوم بذلك بدون أي تحديثات مطلوبة للعميل.

فوائد الخدمة

- إيقاف هجمات ساعة الصفر غير المعروفة سابقًا وسرقة بيانات الاعتماد مع مستويات دفاع معززة.
- تأمين الأجهزة المتصلة بالشبكة باستخدام تقنية العزل على مستوى المؤسسات.
- المساعدة على حماية الموظفين من التهديدات الإلكترونية بدون وضع حواجز أمام إنتاجيتهم

أبرز ميزات الخدمة

- نهج الحماية في المقام الأول لتوفير الحماية للأجهزة المتصلة بالشبكة مع الدفاع الفوري متعدد المستويات
- تمت مراقبته وإدارته بخبرة من قبل متخصصين في مجال الأمن المعتمدين.
- تحليلات ورؤى فورية وقابلة للتنفيذ.

الميزات والمواصفات (متابعة)

بالإضافة إلى ذلك، تحمي خدمة HP Wolf Pro Security الموظفين من أكثر أنواع الاختراقات شيوعًا: هجمات التصيد الاحتيالي. تحظر ميزة حماية الهوية في HP Wolf Pro Security المستخدمين من إدخال كلمات المرور على مواقع جمع بيانات الاعتماد والتي ربما أطلقها المستخدم عن طريق الخطأ من رابط تصيد في بريد إلكتروني أو عميل دردشة أو ملف PDF أو ملف آخر.

تعد تقنية العزل على مستوى المؤسسات من HP Wolf Pro Security هي خط الدفاع الأخير حيث تحتوي حتى التهديدات غير المرئية التي ربما تكون قد أفلتت من دفاع أجهزة الشبكة المتصلة الأخرى الخاصة بالعميل وتجعلها غير ضارة. حماية العزل التي يتم فرضها على الأجهزة تسمح بمرفقات البريد الإلكتروني وتنزيلات الملفات وحتى المحتوى من محركات أقراص USB ليتم فتحها وتحريرها وطباعتها وحفظها بأمان داخل الجهاز الافتراضي المصغر الآمن الخاص بهم. أثناء فتح التطبيقات ، تتم مراقبتها تلقائيًا بحثًا عن أي نشاط تهديدي وتوفر HP Wolf Security Controller تحليلاً كاملاً لسلسلة قتل الهجوم لحوادث التهديد لمساعدتك على فهم طبيعة التهديد بشكل أفضل والحماية من الهجمات المستقبلية.

ومن خلال الجمع بين هاتين التقنيتين المتقدمتين التكميليتين، توفر خدمة HP Proactive Security ميزات أمان استباقي فورية متعددة المستويات لأجهزتك.

الرؤى

توفر خدمة HP Wolf Pro Security رؤى قابلة للتنفيذ للعملاء من خلال HP Wolf Security Controller وهي منصة قوية لتحليلات الأمان.[2] يمكن لفرق تكنولوجيا المعلومات لديك مراقبة حالة حماية الأجهزة وعرض التقارير وتلقي تنبيهات حول الأجهزة غير المحمية ونشاط التهديد المحظور - كل ذلك من لوحة تحكم موحدة قائمة على خدمة سحابية.

مراقبة وإدارة الخبراء[3]

على عكس الحلول البرمجية الخالصة، يتم تقديم HP Wolf Pro Security Service كخدمة خاضعة للمراقبة. إذ يقوم خبراء الأمان من HP بتنفيذ وإدارة سياسات التكوين والأمان، بما في ذلك إدارة عزل التهديدات نيابة عنك. وبمجرد تشغيل الأجهزة، يراقب خبراء الأمان من HP حالة حماية أمان الجهاز ويجرون تحليلات استقصائية وتحليلات لمسارات القضاء على التهديدات الجديدة تمامًا التي لم تكن معروفة من قبل لمعرفة مصادرها ومساعدتك في الحماية بشكل أفضل من الهجمات المستقبلية.

الفئة	الميزات
الحماية	منع التهديدات المستندة إلى الذكاء الاصطناعي HP Sure Sense Pro لنظام التشغيل Windows 10 [4]
	عزل المرفقات والتنزيلات من خلال HP Sure Click Pro[5] لنظام Windows 10
	تمنع حماية الهوية من HP الكشف غير المقصود عن كلمات مرور المستخدم على مواقع سرقة بيانات الاعتماد
تحليلات الأمان	لوحة حماية الجهاز
	بيانات التهديدات HP Sure Click Pro و HP Sure Sense Pro
	معلومات مفصلة عن حالة حماية الجهاز
	تم تعيين تحليل سلسلة قتل التهديد الكامل لإطار MITREATT&CK™[6]
إدارة الخدمة المستمرة	إعداد وحدة التحكم وضبطها وتطبيق السياسة
	تحليل التهديدات والرؤى
	إدارة الحجر الصحي والاستثناءات
	فحص صحة وكيل الأمن
	نشر تحديث عامل الأمان
الميزات الأخرى	تكامل نظام أمن المعلومات وإدارة الحوادث SIEM عبر موجز سجل النظام

مواصفات تقديم الخدمات

يجب على العملاء تثبيت برنامج عميل الأمان والتحليلات على الأجهزة المُدارة. مطلوب اتصال بالإنترنت للوصول إلى التحليلات وإعداد التقارير وتلقي تحديثات السياسة وترقيات البرامج. ولا تحتاج هذه البرامج إلى اتصال بالإنترنت لتوفير الحماية بمجرد اكتمال الإعداد. ولن يتم التقاط بيانات حساسة تخص المستخدم، بما في ذلك بيانات الاعتماد والملفات والمحتويات والبيانات الشخصية. وسيتم تخزين البيانات التي تم جمعها في مستودع سحابي آمن.[2]

ستوفر HP وصول HP Wolf Security Controller[2] إلى معلومات إحصاءات الأمان بما في ذلك اللوحة والتقارير والحوادث والمزيد.

وسيدير خبراء الأمان المعتمدين في شركة HP بشكل استباقي أمان الأجهزة المتصلة بالشبكة لديك، بما في ذلك ضبط سياسة الأمان وتطبيقها. وتحليل الحوادث عند اكتشاف تهديد إيجابي حقيقي وإدارة تحديثات برامج الأمان والتحقيق في المشكلات المتعلقة بسلامة البرامج وغير ذلك المزيد.

سيوفر خبير خدمة HP دعم العملاء رفيع المستوى وسيعمل مع فرق HP الداخلية، بما في ذلك "خبراء الأمان" لحل المشكلات التي تبلغ عنها. تتوافر خدمة "خبراء خدمات HP" على النحو التالي:

أمريكا الشمالية: يتوفر الدعم باللغة الإنجليزية من الاثنين حتى الجمعة (باستثناء أيام عطلات HP) من الساعة 6:00 صباحًا حتى الساعة 6:00 مساءً بالتوقيت الجبلي.

أمريكا اللاتينية: يتوفر الدعم باللغة الإنجليزية والإسبانية من الاثنين حتى الجمعة (باستثناء أيام عطلات HP) من الساعة 7:00 صباحًا حتى الساعة 6:00 مساءً بتوقيت جرينتش - 5.

أوروبا والشرق الأوسط وأفريقيا يتوفر الدعم باللغة الإنجليزية والفرنسية والألمانية من الاثنين حتى الجمعة (باستثناء أيام عطلات HP) من الساعة 8:00 صباحًا حتى الساعة 6:00 مساءً بتوقيت وسط أوروبا.

دول آسيا المطلة على المحيط الهادي واليابان يتوفر الدعم باللغة الإنجليزية 24 ساعة في اليوم في المنطقة كلها، كما يتوفر الدعم باللغتين الإنجليزية واليابانية في اليابان من الساعة 09:00 صباحًا حتى الساعة 09:00 بواقع 7 أيام في الأسبوع (باستثناء أيام عطلات HP)

مسؤوليات العميل

- توفير المعلومات المطلوبة كي تتمكن HP من إعداد حساب العميل
- انشر وكيل خدمة Wolf Pro Security على أجهزتك المدارة.
- طلب إضافة أو إزالة مواقع تنزيل مواقع الويب المدرجة في القائمة البيضاء والاستثناءات والبريد الإلكتروني وإعدادات المجال (لعزل مرفقات الملفات والحماية من البرامج الضارة المستندة إلى الذكاء الاصطناعي و منع سرقة بيانات الاعتماد).
- طلب إضافة نطاقات عناوين IP للشركات التي لا تخضع للعزل أو إزالتها
- الطلب أو الموافقة على إصدار أو استبعاد الملفات المعزولة أو المحجوبة.
- قم بتسجيل الدخول إلى مدخل HP Wolf Security Controller لعرض اللوحات والتقارير والحوادث.
- مراجعة تقارير الأمان والاستجابة حسب الضرورة.

متطلبات النظام

يدعم HP Wolf Pro Security الأنظمة التي تعمل بأنظمة تشغيل Windows 10 التي تعمل على معالجات ®Intel أو AMD المدعومة. للحصول على أحدث متطلبات النظام، قم بزيارة https://www.hpdaas.com/requirements

متطلبات الشبكة

يلزم اتصال بالإنترنت لإجراء اتصالات بين الجهاز المدار والخدمة السحابية المدارة.

المتطلبات الأساسية

لاستخدام الخدمة، يجب تسجيلها بعد الشراء باتباع الإرشادات المقدمة من HP. أثناء عملية الإعداد، سيُطلب منك تقديم المعلومات اللازمة لإعداد الحسابات وسياسات الأمان.

قيود الخدمة

خدمة HP Wolf Pro Security ليست خدمة مراقبة مستمرة في الوقت الفعلي. يحظر HP Sure Sense و HP Sure Click Pro المحتوى غير الموثوق أو الضار ويعزله تلقائيًا، مما يضمن الحماية على أجهزتك. ولا تتضمن خدمة HP Wolf Pro Security خدمات الإصلاح أو القضاء على التهديدات في حالة حدوث اختراق. وتتوفر خدمات القضاء على التهديدات والمعالجة كخدمات منفصلة من شركاء HP.

الشروط والأحكام

شروط وأحكام خدمات العناية بالأجهزة HP Care Pack قد تنطبق إذا تم شراء الخدمة على أنها خدمة عناية بالأجهزة HP Care Pack.

وتنطبق بنود وشروط HP TechPulse وإشعار حقوق البيانات الشخصية من HP وبيان خصوصية HP جميعها على الخدمة.

لمزيد من المعلومات

اتصل بممثل مبيعات HP المحلي أو شريك القنوات التسويقية للحصول على التفاصيل أو قم بزيارة https://www8.hp.com/us/en/services/pro-security-service.html

1 تخضع خدمات HP لشروط وأحكام خدمات HP المعمول بها والتي يُنص عليها أو يتم توضيحها للعميل وقت الشراء. وقد يتمتع العميل بحقوق تشريعية إضافية وفقًا للقوانين المحلية المعمول بها، ولا تتأثر مثل هذه الحقوق بأي شكل من الأشكال بشروط وأحكام خدمات HP أو الضمان المحدود من HP المرفق بمنتج HP. للحصول على قائمة كاملة بمتطلبات النظام، يرجى زيارة https://www.hpdaas.com/requirements.

2 ولا تراقب شركة HP التفاصيل التي تحدد عناوين URL التي زارها المستخدم أو تراقبها. يركز التقرير على تحديد التهديدات ومصدرها في HP Wolf Security Controller. إن HP Wolf Security Controller متوافق مع اللائحة العامة لحماية البيانات (GDPR) و ISO 27001. HP Wolf Security Controller غير متوفر كمنتج مستقل ومطلوب خدمة HP Wolf Pro Security. للاطلاع على متطلبات النظام كاملة، يُرجى زيارة موقع http://www.hpdaas.com/ requirements. تخضع خدمات HP لشروط وأحكام خدمات HP المعمول بها والتي يُنص عليها أو يتم توضيحها للعميل وقت الشراء. وقد يتمتع العميل بحقوق تشريعية إضافية وفقًا للقوانين المحلية المعمول بها، ولا تتأثر مثل هذه الحقوق بأي شكل من الأشكال بشروط وأحكام خدمات HP أو الضمان المحدود من HP المرفق بمنتج HP.

3 تحليل التهديد من قبل خبراء الأمن من HP هو عملية جنائية متاحة بعد أن تم حظر حدث البرامج الضارة أو عزله بواسطة وكيل برنامج HP Wolf Pro Security. وهذه ليست خدمة "فورية" على مدار الأسبوع. لمزيد من المعلومات حول ميزة الخدمة هذه، يرجى الرجوع إلى مستند تعريف خدمة أمان HP Wolf Pro. يعزل وكيل خدمة HP Wolf Pro Security المحتوى غير الموثوق أو الضار تلقائيًا، مما يضمن الحماية قبل التحليل. ولا تتضمن أي من الخطتين خدمات الإصلاح أو القضاء على التهديدات في حالة حدوث اختراق.

4 للحصول على قائمة كاملة بإصدارات Windows 10 المدعومة، يرجى الرجوع إلى https://www.hpdaas.com/requirements. تجدر الإشارة إلى أن HP Proactive Security لا يدعم Windows 7 و8.1.

5 تقنية HP Sure Click Pro مضمنة في خدمة الأمان HP Wolf Pro Security وتتطلب Windows 10 Pro أو Enterprise، وتدعم متصفحات Microsoft Internet Explorer وGoogle Chrome وChromium وMozilla Firefox والمتصفح الجديد Edge. تشمل المرفقات المدعومة ملفات Microsoft Office (لتطبيقات Word وExcel وPowerPoint) وملفات PDF عندما يتم تثبيت Microsoft Office أوAdobe Acrobat. لمزيد من التفاصيل، يرجى زيارة https://www.hpdaas.com/requirements.

6 لا تدعي MITER أن ATT & CK تحصي جميع الاحتمالات لأنواع الإجراءات والسلوكيات الموثقة كجزء من إطار عمل الأساليب ونموذج المواجهة. إن استخدام المعلومات الواردة في ATT & CK لمعالجة أو تغطية الفئات الكاملة من الأنماط لن يضمن تغطية دفاعية كاملة، حيث قد تكون هناك أساليب غير معلنة أو اختلافات في الأساليب الحالية غير موثقة بواسطة ATT & CK.

التسجيل للحصول على التحديثات

hp.com/go/getupdated

المشاركة مع الزملاء

قيّم هذا المستند

© Copyright 2021 HP Development Company, L.P. المعلومات الواردة بهذا المستند عرضة للتغيير بدون إشعار مسبق. وتقتصر الضمانات الخاصة بمنتجات وخدمات شركة HP على تلك المنصوص عليها في بيانات الضمان الصريح المرفق بتلك المنتجات والخدمات. ولا يوجد هنا ما يمكن تفسيره على أنه يشكل ضمانًا إضافيًا. وتخلي شركة HP مسؤوليتها عن أي أخطاء فنية أو تحريرية أو أي أخطاء ناتجة عن السهو والإغفال وردت في هذا المستند.

4AA7-4656ARE، مايو 2021، الإصدار 5

HP WOLF SECURITY