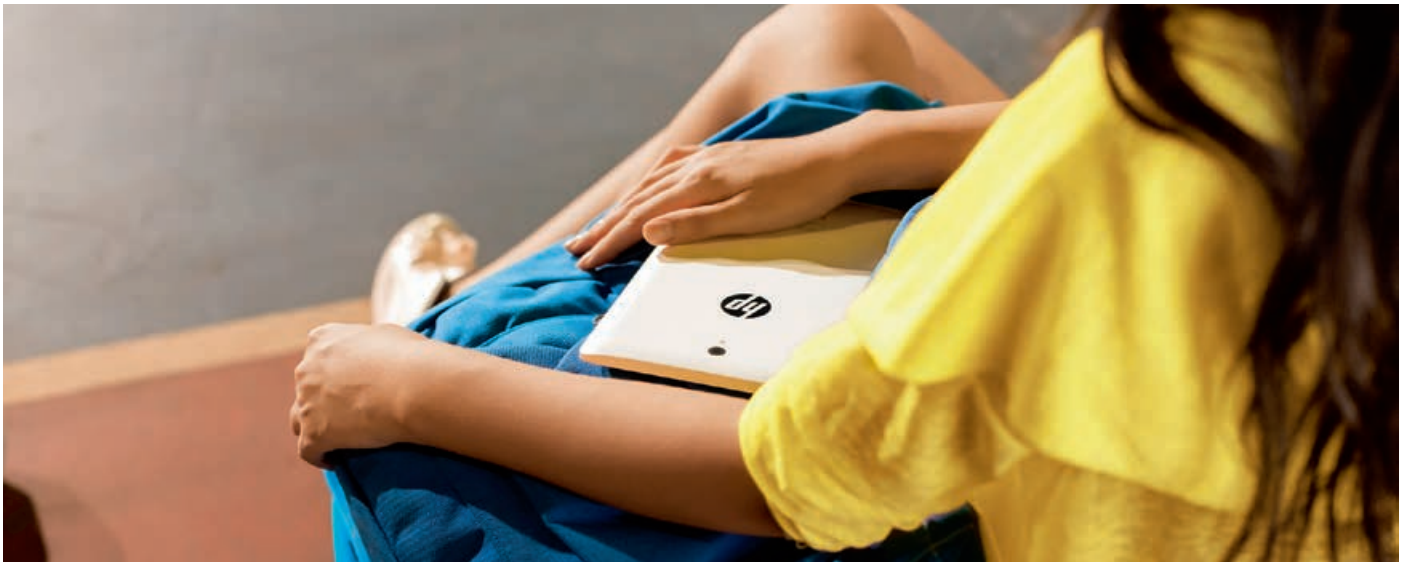
Technologieübersicht

Sicherheit für mobile Geräte

HP Touchpoint Manager



Mit der zunehmenden Verbreitung von mobilen Geräten in Unternehmen erhöht sich auch die Produktivität der Mitarbeiter. Sie können produktiv arbeiten – im Büro ebenso wie an nahezu jedem anderen Ort; ob am Flughafen, während sie auf einen Anschlussflug warten, während eines Geschäftsessen mit einem Kunden, bei einer Konferenz oder daheim. Mit dieser größeren Flexibilität geht jedoch auch ein größeres Sicherheitsrisiko einher. Jeder Mitarbeiter mit einem mobilen Gerät – Smartphone, Tablet oder Notebook – erhöht die Anfälligkeit Ihres Unternehmens, was dazu führen kann, dass vertrauliche Informationen gefährdet, gestohlen oder vernichtet werden.

Mit wenigen einfachen Schritten kann der HP Touchpoint Manager Sie und Ihre Mitarbeiter schützen.[1] Die Lösung ist unverzichtbar für alle Unternehmen, die einen „Bring Your Own Device"-Ansatz (BYOD) verfolgen. Der HP Touchpoint Manager ermöglicht es IT-Administratoren, Sicherheitseinstellungen schnell und konsistent anzuwenden – mit konfigurierbaren integrierten Sicherheitsfunktionen, Optionen für die Wi-Fi-Bereitstellung und Richtlinien für Gruppen von Benutzern und Geräten.

Zu den Sicherheitsprofileinstellungen zählen:

- Erkennen, Überwachen und Bereitstellen von Antivirensoftware (Windows)
  Wird keine Virenschutzsoftware erkannt, aktiviert der HP Touchpoint Manager automatisch Microsoft Windows Defender (Windows 8.0 und höher) oder Microsoft Security Essentials (Windows 7-Systeme).
- Erkennen, Überwachen und Verwalten der Windows-Firewall (Windows)
  Wird keine aktive Firewall-Software erkannt, aktiviert der HP Touchpoint Manager die integrierte Windows-Firewall.
- Zurücksetzen von Geräten nach einer bestimmten Anzahl von fehlgeschlagenen Anmeldeversuchen (Android™/iPhone® und iPad®)
- Auslösen der automatischen Sperrung von Geräten nach einer Inaktivität über einen festgelegten Zeitraum (Android/iPhone und iPad)
- Erzwingen von Einstellungen für die Länge von Kennwörtern/PINs für die Geräte (Android/iPhone und iPad)
- Aktivieren/Deaktivieren der Gerätekamera (Android/iPhone und iPad)

Der HP Touchpoint Manager umfasst vordefinierte Sicherheitsvorlagen basierend auf Best Practices für die Sicherheit, die sich für die Anforderungen aller Unternehmen eignen und ermöglicht darüber hinaus aber auch die Erstellung eigener Sicherheitsprofile.

Integrierte HP Touchpoint Manager Sicherheitsprofile

Lizenzlevel	Sicherheitseinstellungen	Integrierte Sicherheitsprofile *Standard*	*Erweitert*	*Maximum*
Basic	Antivirenüberwachung	Deaktiviert	Aktiviert	Aktiviert
Basic	Firewall-Überwachung	Deaktiviert	Deaktiviert	Aktiviert
Pro	Sperrung von Geräten nach einer Inaktivität von X Minuten	30	15	5
Pro	Kennwörter müssen Buchstaben enthalten	Deaktiviert	Deaktiviert	Aktiviert
Pro	Kennwörter müssen Zahlen enthalten	Deaktiviert	Deaktiviert	Aktiviert
Pro	Löschung aller Daten auf Geräten, nachdem das Kennwort X Mal in Folge falsch eingegeben wurde	Deaktiviert	Deaktiviert	10
Pro	Mindestkennwortlänge	0	4	8
Pro	Kamera deaktivieren	Deaktiviert	Deaktiviert	Deaktiviert
Pro	Geräteverschlüsselung aktivieren	Deaktiviert	Deaktiviert	Deaktiviert
Pro	Kennwörter müssen Sonderzeichen enthalten	Deaktiviert	Deaktiviert	Aktiviert
Pro	Kennwort läuft nach X Tagen ab	Deaktiviert	120	90
Pro	Kennwortverlauf berücksichtigen. X eindeutige Kennwörter erforderlich	Deaktiviert	3	5

Da sich verschiedenen Gruppen von Geräten unterschiedliche Richtlinien zuweisen lassen, können Sie leicht nachverfolgen, welche Einstellungen unternehmensweit angewendet werden.

Mitarbeitern bestimmter Abteilungen, die beispielsweise für Rechnungswesen oder die Gehaltsabrechnung verantwortlich sind, kann eine bestimmte Sicherheitsrichtlinie zugewiesen werden. Die Geräte können aber auch nach Gerätetyp organisiert werden (z. B. alle Tablets). Sobald Sie eine Gruppe erstellen, können Sie einfach per Mausklick ein Sicherheitsprofil auf die Gruppe anwenden. Änderungen lassen sich ebenso schnell vornehmen. Wenn Sie Risiken identifizieren, können Sie nach Bedarf striktere Sicherheitsprofile anwenden.

Darüber hinaus stehen Ihnen weitere Sicherheitsoptionen wie die Funktion „Geräte suchen“ zur Verfügung, mit der Sie Ihr Unternehmen vor Diebstahl oder Verlust schützen, indem Sie Geräte auf einer Karte lokalisieren können, wenn sie mit dem Internet verbunden sind.[2] Dies ermöglicht es Ihnen, zu überprüfen, ob sich die betreffenden Geräte dort befinden, wo sie sein sollten. Und wenn Sie davon ausgehen, dass die Geräte verloren gegangen sind oder gestohlen wurden, können Sie die nötigen Maßnahmen ergreifen, um sie zu lokalisieren oder die darauf befindlichen Daten zu schützen.

Zu den Schutzfunktionen für verlorene Geräte zählen die Folgenden:

- **Akustischer Alarm:** löst einen lauten Alarmton auf dem Gerät aus, um das Auffinden des verlorenen Geräts in der Nähe zu ermöglichen.[2]
- **Gerät sperren:** löst eine Bildschirmsperre aus (Android/iPhone und iPad) oder meldet die Benutzersitzung ab (Windows).[2]
- **Gerätedaten löschen:** löst eine Rücksetzung auf die Werkseinstellungen des Geräts aus (Android/iPhone und iPad) bzw. eine sichere Löschung der Datendateien auf dem Gerät (Windows).[2]

Falls Ihre oder die behördlichen Datenschutzrichtlinien es erfordern, kann die Funktion „Geräte suchen“ auch deaktiviert werden.

Mit dem HP Touchpoint Manager können Sie als IT-Administrator problemlos die von Ihnen verwalteten mobilen Geräte überwachen, Sicherheitseinstellungen anzeigen, den Status überprüfen, Sicherheitsrichtlinien ändern und Maßnahmen auf fehlenden Geräten ergreifen. Die Sicherheitsfunktionen ermöglichen es Ihrem Unternehmen, von den Vorteilen der Mobilität zu profitieren und gleichzeitig sicherzustellen, dass die Unternehmensdaten geschützt sind und von den Mitarbeitern abgerufen werden können, damit diese produktiv arbeiten können.

[1] Der HP Touchpoint Manager unterstützt die Betriebssysteme Android™, iOS und Windows und ist auf PCs, Notebooks, Tablets und Smartphones verschiedener Hersteller nutzbar. Nicht in allen Ländern verfügbar. Weitere Informationen unter hp.com/touchpoint . Touchpoint Manager erfordert den Erwerb einer Lizenz.

[2] Hängt von verschiedenen Voraussetzungen hinsichtlich der Umgebung ab, beispielsweise muss das verloren gegangene Produkt angeschaltet sein und Zugriff auf das Internet haben. Der Service stellt keine Garantie dar.

Für Updates registrieren unter
hp.com/go/getupdated

4AA6-0367DEE, November 2015