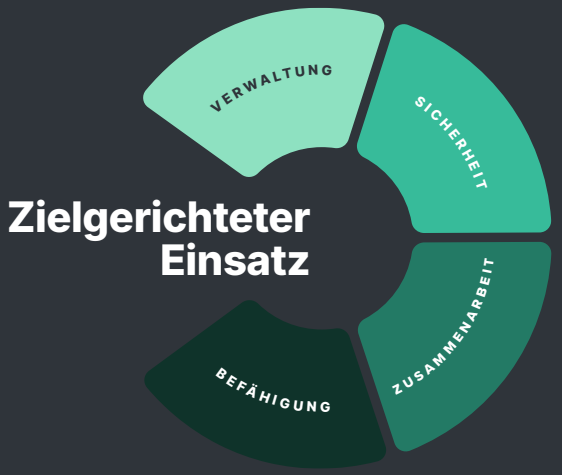
jamf



Wie man Geräte an Grund- und weiterführenden Schulen (K12) schützt und die Privatsphäre der Schüler:innen wahrt

Schulen setzen Technologie auf vielfältige Weise ein: zur Verbesserung des Lernens, zur Erleichterung der Planung von Unterrichtseinheiten für Lehrkräfte, zum Katalogisieren von Schülerdaten usw. Das bedeutet, dass Schulen über eine Vielzahl von Daten verfügen, einschließlich sensibler, persönlich identifizierbarer Informationen (PII), auf die es Cyberkriminelle häufig abgesehen haben.

Angesichts eines **Anstiegs von 75 %** zwischen 2023 und 2024 ist **der Bildungsbereich** mit sage und schreibe **3.574 Angriffen pro Woche** die am häufigsten von Cyberangriffen betroffene Branche weltweit. Angreifer haben es auf die Daten der Lernenden abgesehen - und Cybersicherheit ist entscheidend, um sie zu schützen. Eine Sicherheitskompromittierung kann die Schüler:innen in mehrfacher Hinsicht beeinträchtigen:

- Ihre Daten können offengelegt und ausgenutzt werden.
- Daten über ihren Hintergrund, ihr Wohlbefinden, ihre Disziplin, ihre Einstellung und vieles mehr können sie von ihren Mitschüler:innen entfremden.
- Das Lernen muss meistens unterbrochen werden, während die Systeme wiederhergestellt werden - was oft viel Zeit und Geld kostet.

Schulen bekämpfen Bedrohungen, indem sie relevante Endpoint-Daten zur Einhaltung von Vorschriften oder zur Reaktion auf Vorfälle protokollieren. Und viele entscheiden sich für Apple Geräte wegen ihrer integrierten Sicherheitsfunktionen.

Obwohl Apple Geräte eine sichere Grundlage bieten, finden Cyberkriminelle immer wieder Wege, diese Funktionen zu umgehen. **Daher ist es notwendig, Sicherheitslösungen übereinander zu schichten.**

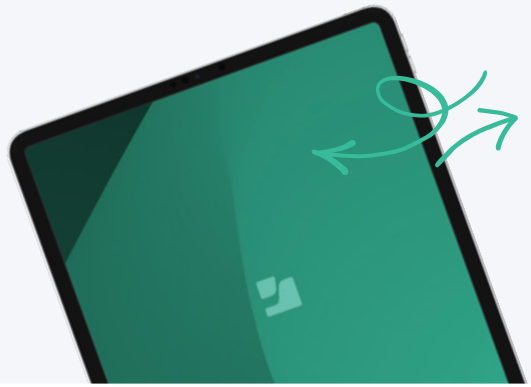
Es gibt viele Optionen auf dem Markt, aber man sollte sich genau überlegen, was man braucht, bevor man sich für eine Lösung entscheidet. Einige Lösungen können den Bedrohungen, die wir zu verhindern suchen, sehr ähnlich sein, da sie:

- zu aufdringlich und störend sind
- den Datenschutz untergraben
- das Vertrauen in die Institution verringern

Das ist der Punkt, an dem der **Zweck** ins Spiel kommt. Im zweiten E-Book unserer Serie über einen zielgerichteten Einsatz sprechen wir darüber, was es bedeutet, Datenschutz und Sicherheit **zielgerichtet** zu erreichen. Wir sprechen darüber, warum das so wichtig ist, wie man sein individuelles Ziel findet und wie Jamf dabei helfen kann.

Bedrohungen für die Sicherheit

Externe Bedrohungen



Kryptojacking

Kryptojacking-Malware übernimmt Geräte, um Kryptowährung zu generieren. Betroffene Geräte sind oft mit den für das Kryptojacking erforderlichen Prozessen überfordert, die im Hintergrund laufen, sodass sie für nichts anderes mehr zu gebrauchen sind - auch nicht zum Lernen.

Ransomware

Ransomware greift die Daten auf einem System oder Gerät an, verschlüsselt sie und verhindert den Zugang dazu. Die Nutzer:innen müssen ein Lösegeld bezahlen, um wieder Zugang zu erhalten. Manche Ransomware exfiltriert auch Daten, um sie zu verkaufen, oder verlangt ein zusätzliches Lösegeld für ihre Rückgabe - ohne Garantie. Dies kann den Schulbetrieb zum Erliegen bringen und die geplanten Unterrichtseinheiten der Lehrkräfte und die Lernerfahrung der Schüler:innen auf den Kopf stellen.

Phishing

Bei Phishing-Angriffen werden Social Engineering-Taktiken eingesetzt, um Informationen von Nutzer:innen abzugreifen, z. B. Anmeldeinformationen. Dabei kann es sich um eine sorgfältig konstruierte E-Mail oder eine sehr ähnlich aussehende Website handeln, die Nutzer:innen zur Eingabe ihrer Daten verleitet. Wenn sie nicht geschützt sind, können vor allem jüngere Schüler:innen auf diese Angriffe hereinfallen.

Malware

Bei Malware handelt es sich um Software-Code, der für bösartige Zwecke entwickelt wurde. Er kann Informationen stehlen, Angreifer:innen Zugang zu Ihren Systemen verschaffen und andere schädliche Programme auf Ihrem Gerät installieren.

Man-in-the-Middle (MitM)

MitM-Angriffe entstehen, wenn Cyberkriminelle die Kommunikation zwischen zwei Parteien abfangen. Die Angreifer:innen können sich z. B. als das WLAN Ihrer Schule ausgeben und Daten von ahnungslosen Nutzer:innen sammeln, die sich damit verbinden.

Spyware

Bei Spyware handelt es sich um Malware, die den Datenschutz verletzt und jede Aktion der Nutzer:innen überwacht, indem sie Passwörter, den Browserverlauf und vieles mehr sammelt.

Vertiefen Sie Ihr Wissen: Verteidigung gegen gängige, externe Bedrohungen

Tippen Sie unten, um mehr zu erfahren

Kostenlose Downloads, die ihren Preis nicht wert sind

Malware in Schulen für Einsteiger:innen >

Quillt Ihr Posteingang über?

Spam in Schulen für Einsteiger:innen >

Halten Sie Ihre CPUs von den Krypto-Minen fern.

Kryptojacking in Schulen für Einsteiger:innen >

Haben Sie verdächtige Links in Ihrem Posteingang entdeckt? Fallen Sie nicht darauf herein.

Phishing in Schulen für Einsteiger:innen >

jamf

Interne Bedrohungen

Social Engineering
Social Engineering-Angriffe nutzen die Naivität oder das mangelnde Wissen der Nutzer:innen aus, um an Informationen zu gelangen. Schüler:innen, Lehrkräfte und Admins laufen Gefahr, Opfer von Datendiebstahl und Sicherheitsverletzungen zu werden, wenn Angreifer sich mit gefälschten Nachrichten oder durch Identitätswechsel unbefugten Zugang verschaffen.

Veraltete Geräte und Apps
Veraltete Geräte und Apps verfügen oft nicht über die neuesten Erweiterungen und Funktionen im Bereich der Sicherheit. Mit den richtigen Tools können automatische Updates Ihren Sicherheitsstatus auf einfache Weise verbessern.

Schatten-IT
Von Schatten-IT spricht man, wenn Nutzer:innen nicht zugelassene Software installieren oder Sicherheitskontrollen auf andere Weise umgehen. Durch die Bereitstellung einer Vielzahl genehmigter Apps und die Möglichkeit, neue Apps anzufordern, lässt sich die Wahrscheinlichkeit von ungewollten Installationen verringern.

Menschliches Versagen
Menschliches Versagen kann zu Datenschutzverletzungen oder zur Offenlegung von Daten führen - etwa wenn jemand eine Haftnotiz mit seinen Anmeldeinformationen hinterlässt oder versehentlich eine E-Mail an den falschen Empfänger schickt.

Fehlkonfigurationen
Durch Fehlkonfigurationen kann es zu Schwachstellen in Ihrem System kommen. So können beispielsweise eine Durchsetzung von schwachen Passwörtern, eine unzureichende Filterung von Inhalten und fehlende Zugangskontrollen Angreifer:innen den Zugang erleichtern.

Schulen unterliegen gewissen Vorschriften

Wie viele andere Institutionen unterliegen auch Schulen den Datenschutzgesetzen. So verhindert beispielsweise der **Family Educational Rights and Privacy Act** (FERPA) in den USA die Weitergabe von personenbezogenen Daten in Bildungsunterlagen ohne schriftliche Zustimmung. US-amerikanische Schulen, die durch E-Rate-Rabatte oder vom Bildungsministerium finanziert werden, unterliegen dem **Children's Internet Protection Act** (CIPA) bzw. dem **Protection of Pupil Rights Amendment** (PRPA). Schulen in der EU müssen die **DSGVO** einhalten und das Vereinigte Königreich hat **gesetzliche Leitlinien für Schulen** zum Schutz von Kindern implementiert.

Das bedeutet, dass die Schulen wahrscheinlich bereits über gewisse Sicherheitstools verfügen, um diese Anforderungen zu erfüllen. Ist das ausreichend? Nutzen Sie diese Instrumente wirklich, um Ihre Ziele zu erreichen, oder kreuzen Sie nur ein Kästchen an? Im Idealfall verbessern diese Tools das Lernen und vereinfachen den Unterricht - bei gleichzeitiger Gewährleistung von Sicherheit und Datenschutz. Aber die Realität sieht manchmal ganz anders aus.

jamf

Ziel definieren

Externe Bedrohungen, interne Bedrohungen, Compliance-Anforderungen und Datenschutzbedenken machen Sicherheit zu einer Toppriorität. Um Geräte wirksam zu schützen, müssen Sie aber auch den Zweck hinter dem Einsatz verstehen.

Entscheidungsträger in Schulen wollen, dass Schüler:innen lernen und Lehrkräfte unterstützt werden. Technologie kann dabei helfen, wenn sie mit einem klaren Ziel vor Augen ausgewählt wird. Man darf nicht zulassen, dass die Bildungstechnologie einfach außer Kontrolle gerät und Datenschutzstandards aus Gründen der „Sicherheit" verletzt. Andererseits sollten die Geräte nicht so stark abgeriegelt werden, dass sie nur deshalb sicher sind, weil niemand auf nützliche Informationen zugreifen kann.

Es ist nicht immer einfach, Ihre Ziele auf Ihr Sicherheitssystem zu übertragen. Die Beantwortung dieser Fragen ist ein guter Ansatzpunkt.

Sie sollten Folgendes berücksichtigen:

1. **Wo werden die Geräte der Nutzer:innen eingesetzt: In der Schule? Zu Hause? Woanders?**

2. **Werden Geräte von mehr als einer Person benutzt? Werden sie in der Schule oder zu Hause gemeinsam genutzt?**

3. **Werden Geräte für das selbstständige Lernen außerhalb des Klassenraums verwendet?**

4. **Haben die Schüler:innen Zugang zu ihren E-Mails auf dem Gerät?**

5. **Welche Haltung zum Schutz der Privatsphäre der Schüler:innen ist für Ihren Einsatz erwünscht?**

6. **Erhalten alle Schüler:innen Schulungen zur digitalen Kompetenz, einschließlich Cybersicherheitsschulungen zu Malware, Phishing und anderen Bedrohungen?**

Die Berücksichtigung dieser Aspekte kann Admins dabei helfen, Sicherheit, Datenschutz und Lernen in Einklang zu bringen.

jamf

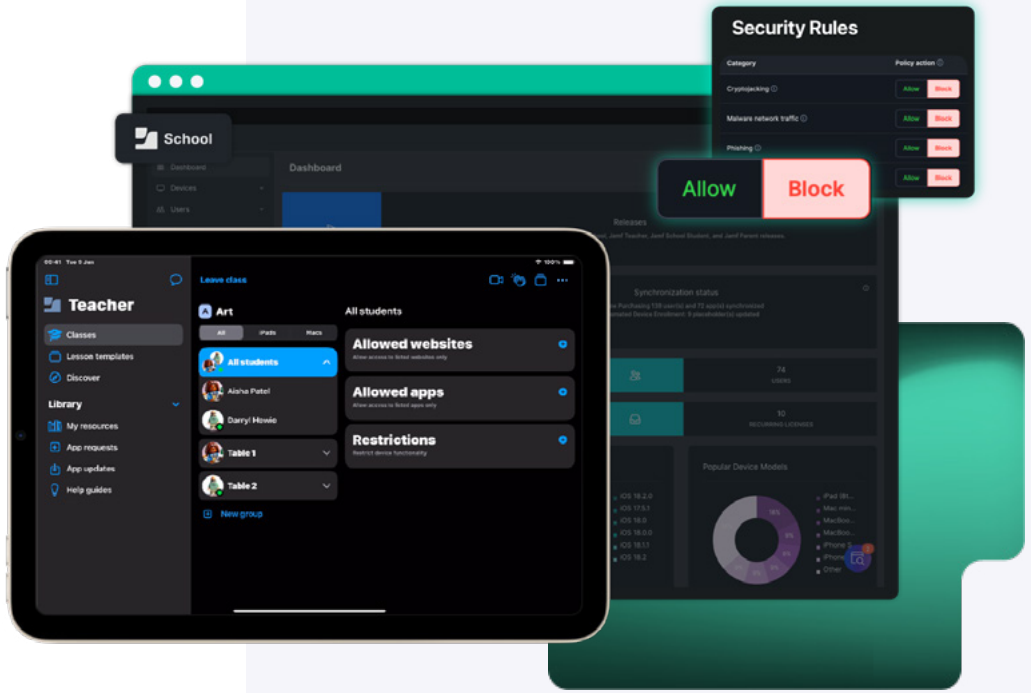
Hält selbst die unheimlichsten Angreifer:innen in Schach

Schutz vor Bedrohungen aus dem Internet

Jedes Gerät, das mit dem Internet verbunden ist, ist anfällig für potenzielle Angriffe wie Malware, Phishing-Versuche, Command-and-Control-Server und mehr. Schüler:innen können mit diesen Methoden auf Websites, in infizierten Apps oder in Nachrichten, die sie erhalten, in Kontakt kommen.

Mit Funktionen zum Schutz vor Bedrohungen aus dem Internet können Sie sich effektiv dagegen wehren. Selbst wenn die Schüler:innen mit diesen Bedrohungen in Berührung kommen, kann Jamf verhindern, dass sie die Geräte kompromittieren. Das schützt Ihre Daten und sorgt für die Sicherheit der Schüler:innen - auch wenn diese die Gefahr nicht erkennen. Der Schutz vor Bedrohungen aus dem Internet hat folgende Vorteile:

- Die Geräte sind geschützt, unabhängig von der Erfahrung der Schüler:innen mit Technologie.
- Die Daten der Schulen werden nicht über unsichere Verbindungen übertragen.
- Die Geräte sind selbst vor den neuesten Bedrohungen geschützt.



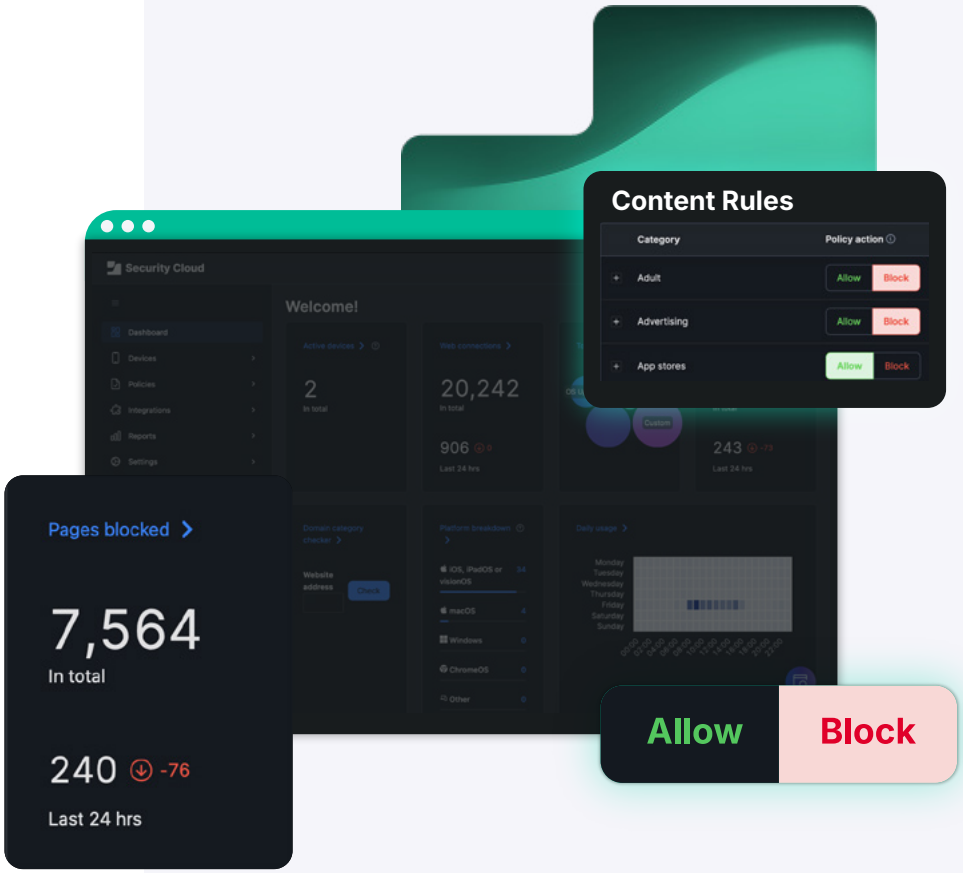
Konzentriertes und sicheres Surfen

Inhaltsfilter

Da ihnen das Internet jederzeit zur Verfügung steht, werden die Schüler:innen schnell dazu verleitet, sich abzulenken. Dies kann dazu führen, dass ihr Lernprozess gestört wird oder, schlimmer noch, sie oder ihre persönlichen Daten gefährdet werden.

Die Filterung von Inhalten sorgt dafür, dass Schüler:innen ihre Aufgaben erfüllen und nicht in Gefahr geraten, indem der Datenverkehr auf der Grundlage voreingestellter Kategorien wie Nachrichten, Unterhaltung, Spiele und nicht jugendfreie Inhalte blockiert wird. Vorteile von Inhaltsfiltern:

- Die Schüler:innen können sich besser auf das Lernen konzentrieren.
- Die Lehrkräfte müssen nicht um Aufmerksamkeit konkurrieren.
- Die IT-Abteilung muss sich weniger Sorgen um gefährdete Geräte machen.



Sicherheit ohne Grenzen

Funktionalität auf dem Gerät

Mit von Schulen verwalteten Geräten in geschützten Netzwerken können Schulen einen Eindruck davon gewinnen, wie sicher ihre Geräte sind. Aber wie sieht es außerhalb des Schulgebäudes aus, bei den Schüler:innen zu Hause? Oder im öffentlichen WLAN?

Das Sicherheitsbedürfnis bleibt bestehen. Denn die Sicherheit auf dem Gerät ist nach wie vor unerlässlich. Auf iPad und Mac funktionieren die Inhaltsfilter direkt auf dem Gerät, in jedem Netzwerk und an jedem Standort. Schutz auf dem Gerät bedeutet:

- Die Schüler:innen können auch außerhalb der Schule sicher und geschützt lernen.
- Der Browserverlauf wird auf dem Gerät verarbeitet, um die Daten zu schützen.
- Die Sicherheitskontrollen können nicht durch Services von Drittanbietern umgangen werden.

Hier sind nur einige der wichtigsten Vorteile, die Jamf bietet:

- Maschinelles Lernen zur Erkennung von Phishing-Versuchen auf Geräteebene
- Benutzerdefinierte Regeln werden auf dem Gerät ausgewertet, um sicherzustellen, dass die Sicherheitsrichtlinien durchgesetzt werden.
- Kompatibilität mit VPN-, Proxy- und DNS-Diensten von Drittanbietern, ohne Umgehungsmöglichkeit für die Nutzer:innen

Ununterbrochenes Lernen

Endpoint-Schutz

Selbst wenn Sie den besten Schutz haben, kann Malware auf Ihr Gerät gelangen. Die Erkennung dieser Bedrohungen ist eine notwendige Fähigkeit in Ihrem Sicherheitssystem.

Jamf erkennt Bedrohungen verschiedenster Art - Spyware, Kryptojacking-Malware, Phishing-Angriffe und mehr - und kann das Problem schnell beheben. Mit Jamf sind folgende Dinge möglich:

- Das Lernen wird nicht durch außer Betrieb gesetzte Geräte unterbrochen.
- Eine schnelle Wiederherstellung kompromittierter Geräte verringert die Auswirkungen erfolgreicher Angriffe.
- Die Geräte werden vor einer Vielzahl von Malware-Familien und Bedrohungen geschützt.

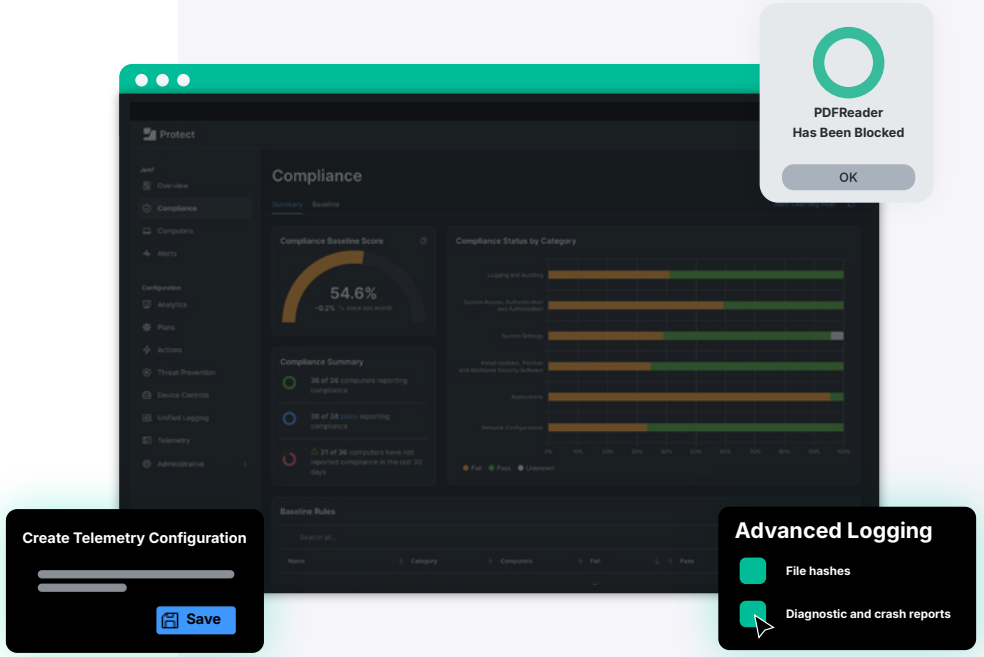
Vollständige Transparenz des Systems

SIEM/SOAR-Integrationen

Es ist unmöglich zu wissen, wie sicher Ihre Geräteflotte ist, wenn Sie keinen Einblick in deren Status haben. Die Integration Ihrer Verwaltungs- und Sicherheitssoftware mit Ihren Lösungen für Security Information and Event Management (SIEM) oder Security Orchestration, Automation and Response (SOAR) ermöglicht einen Einblick in den Status Ihrer Flotte und ist in der heutigen Welt der Geräte-Sicherheit unerlässlich.

Integrieren Sie Ihr SIEM/SOAR mit Jamf und:

- Behalten Sie den Überblick über Geräte-Compliance und Protokolle
- Verschaffen Sie sich einen umfassenden Überblick über Ihr Netzwerk und Ihre Geräte
- Bereiten Sie sich besser auf Geräteprobleme vor: kürzere Wiederherstellungszeiten bei Vorfällen



Bleiben Sie immer auf dem Laufenden und einsatzbereit

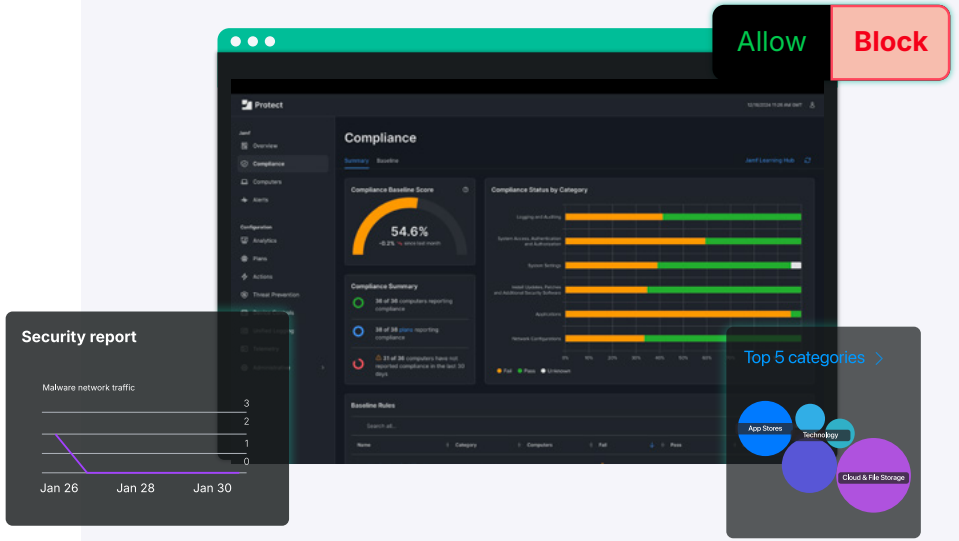
Sicherheitsberichte

Eine einfache Berichterstattung ist für Admins notwendig, um sicherzustellen, dass ihre Geräte registriert sind, den Vorschriften entsprechen und sich korrekt verhalten. Jamf stellt Ihren Admins Berichte zur Verfügung, die:

- anzeigen, welche Geräte im MDM registriert sind und ihren Compliance-Status
- Spam-, Malware-, Kryptojacking- und Phishing-Seiten auflisten, auf die zugegriffen wurde und die blockiert wurden
- Datennutzung basierend auf Tag und Uhrzeit anzeigen
- anzeigen, welche Website-Kategorien von den Nutzer:innen besucht werden

Mit diesen Berichten können die Admins:

- im Falle eines Vorfalls sofort handeln
- ihre Verteidigungsstrategie auf das Nutzerverhalten anpassen
- bei Audits oder anderen Anfragen fundierte Aufzeichnungen über ihre Geräteflotte liefern



Modelle des zielgerichteten Einsatzes

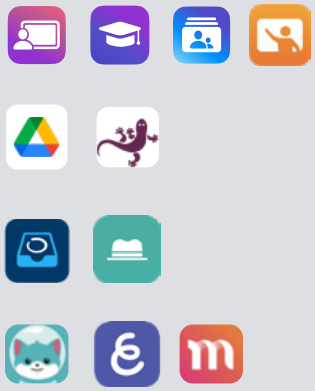
Sobald Sie **Ihr Ziel gefunden** haben, können Sie die Details Ihrer Bereitstellungsstrategie festlegen und haben dann eine Strategie, die:

- das Lernen positiv beeinflusst und verbessert
- Gleichberechtigung für alle Lernenden schafft
- einen sicheren und skalierbaren Einsatz ermöglicht

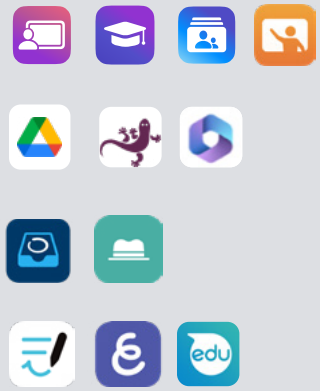
Management und Sicherheit bilden das Fundament: Die IT kann Apps, Geräte und Verfahren bereitstellen, die Lernende und Lehrkräfte unterstützen und engagieren - ohne Kompromisse bei Sicherheit und Datenschutz.

Ihre Strategie für einen zielgerichteten Einsatz könnte folgendermaßen aussehen:

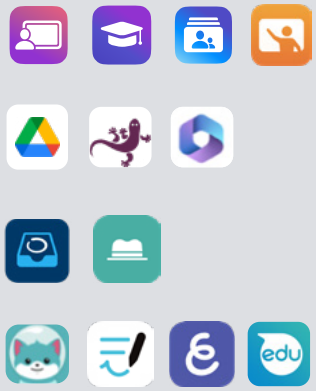
Grundschule
K-5



Sekundarstufe
Mittlere Reife, Gymnasium



Vertrauen
Bezirk



Verwalten und schützen

Engagieren und befähigen

jamf

IT-gestützte Sicherheit und Datenschutz für angstfreies Lernen auf höchstem Niveau

Ein zielgerichteter Einsatz beginnt mit einer klaren Strategie, die Sicherheit und Verwaltung nahtlos integriert und so dafür sorgt, dass Geräte an Grund- und weiterführenden Schulen nicht nur geschützt, sondern auch auf die Bedürfnisse Ihrer Schule abgestimmt sind.

Die Sicherung Ihrer Geräte mit Jamf Security ermöglicht ein sorgenfreies und ununterbrochenes Lernen: Schüler:innen und Lehrkräfte werden gleichermaßen unterstützt, während das Risiko von Datenverlusten und Gerätekompromittierungen reduziert wird.

Mit leistungsstarken Funktionen zur Abwehr von Bedrohungen und Inhaltsfiltern können Sie diese Dinge sicherstellen:

- Die IT kann dafür sorgen, dass die Geräte die Compliance einhalten und vor einer Vielzahl von Bedrohungen geschützt sind.
- Lehrkräfte können sich auf den Unterricht konzentrieren, ohne dass die Geräte ausfallen oder die Schüler:innen abgelenkt werden.
- Sensible Daten von Schüler:innen und Schulen bleiben privat und sind für Cyberkriminelle unzugänglich.

Erfahren Sie, wie die richtige Technologie das Lernerlebnis optimiert.

Jamf jetzt testen

jamf

www.jamf.com/de/