jamf

WHITE PAPER

Conditional Access: Über Perimeter-basierte Sicherheit hinaus

Der moderne Arbeitsplatz und Sicherheitslösungen der nächsten Generation

Seit Jahrzehnten errichten Unternehmen als erste Verteidigungslinie „Mauern“ und bestimmen Perimeter für die Netzwerke ihrer Firma. Doch immer flexibler werdende Arbeitsplätze bringen neue Anforderungen im Bereich Sicherheit mit sich. Netzwerke zu erstellen und sie mit einer Firewall zu schützen reicht manchmal nicht aus. Es ist an der Zeit, das traditionelle Modell in Form von Perimeter-basierter Sicherheit zu überdenken.

Arbeitstage, in denen Mitarbeiter um 9 Uhr morgens im Büro ankommen und um 5 Uhr nachmittags pünktlich Feierabend machen, gehören der Vergangenheit an. Die Leute arbeiten einfach nicht mehr ausschließlich von Montag bis Freitag im Büro.

Sie arbeiten zu flexiblen Zeiten von Zuhause, in Cafés und Hotellobbys oder an anderen Orten. Dabei brauchen sie nicht nur Zugriff auf Ressourcen ihrer Firma, sondern auch Zugriff außerhalb von traditionellen Arbeitszeiten.

Die neue Art zu arbeiten kennt keine festen Grenzen. Die Mitarbeiter müssen mit all ihren Geräten und Apps auf Tools und Daten zugreifen können.

Hier kommt die Cloud ins Spiel.

Cloud-Dienste außerhalb der Firewall sind die Bausteine dieser flexiblen Umgebung, in der die Mitarbeiter im Zentrum stehen. Und diese Dienste bieten besseren Zugriff auf Informationen, indem sie es

Benutzern ermöglichen, sich auf jedem Gerät in jede App oder Webseite einzuloggen und Daten abzurufen. Außerdem können Unternehmen mit modernen Cloud-Diensten ihre Vorgänge zu einem Bruchteil der früheren Kosten automatisieren.

Diese Veränderung des Arbeitsplatzes und die wachsende Abhängigkeit von der Cloud ist mehr als nur eine Modeerscheinung, wie es Vladimir Petrosyan, Senior Product Manager von Microsoft, bei seiner Präsentation auf der Jamf Nation User Conference 2017 formulierte:

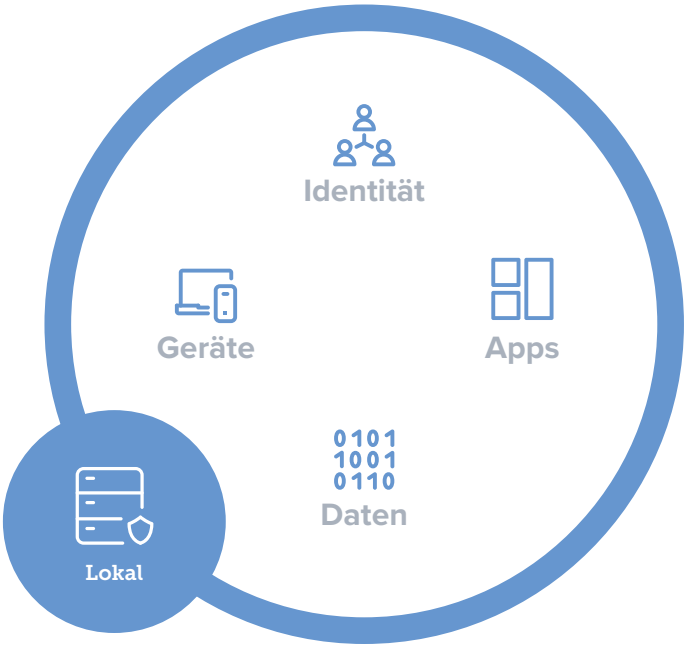
- **85 prozent** der Unternehmen lagern ihre sensiblen Daten in der Cloud
- **80 prozent** der Mitarbeiter nutzen für die Arbeit SaaS-Apps, die nicht zugelassen sind
- **41 prozent** der Mitarbeiter sagen, Business-Apps auf Mobilgeräten verändern die Art, wie sie arbeiten

Immer mehr Unternehmen versuchen, mit der verändernden Landschaft, die früher von Schatten-IT geprägt wurde, Schritt zu halten. Sicherheitsperimeter und die Art, wie sie die Benutzer schützen, müssen sich also auch weiterentwickeln, genau wie Geräte und Apps. Während lokale Infrastrukturen und Server immer noch für viele wichtigen Apps und Dienste verwendet werden, wird die zunehmende Verwendung von cloudbasierten Tools innerhalb von Unternehmen angetrieben von Content- und Kollaborationsplattformen, Cloud-Office-Suites und der Nutzung von Mobilgeräten, die Daten nicht auf dem Gerät selbst speichern. Tatsächlich arbeiten Mitarbeiter heute nicht nur oft außerhalb der Firewall, die meisten Apps und Daten, auf die sie zugreifen, befinden sich auch in der Cloud. Dazu kommt, dass viele von ihnen versuchen, mit ihren privaten Geräten auf Firmenressourcen zuzugreifen. Auch immer mehr Firmen beginnen, ihre Infrastruktur in die Cloud zu verlegen, was eine verstärkte Sicherheit beim Zugriff auf Unternehmensdienste erfordert. Daher suchen Firmen nach neuen und besseren Alternativen hinsichtlich Compliance und Sicherheit.

Hierbei ist es entscheidend, die richtige Balance zu finden, um die höchstmögliche Produktivität der Benutzer zu gewährleisten und gleichzeitig wichtige Firmendaten zu schützen.

DER WANDEL IN DER SICHERHEIT BEI HEUTIGEN UNTERNEHMEN

Die Anforderungen an unsere Sicherheitslösungen haben sich



Das traditionelle Sicherheitsmodell

verändert. Das Konzept, ein Netzwerk zu errichten und es mit einer Firewall zu schützen, funktioniert nur noch bedingt, da Dienste und Daten nicht mehr lokal verwaltet werden. Geräte werden weltweit genutzt und können überall und zu jeder Zeit direkt auf Cloud-Dienste, E-Mail-Applikationen und andere potenziell vertrauliche Unternehmensressourcen zugreifen.

Oben befindet sich ein Beispiel eines traditionellen, Perimeter-basierten Sicherheitsmodells hinter einer Firewall.

Dies stellt jedoch nur einen kleinen Anteil der Daten und Dienste dar, auf die Mitarbeiter und ihre Geräte heutzutage zugreifen. Die neue Norm ist Speicherung in der Cloud, Produktivitätsapps

Das zeitgemäße Sicherheitsmodell

und Zugriff mit mehreren Geräten außerhalb der Firewall. Wenn wir uns klarmachen, wie allgegenwärtig diese neuen Anwendungsfälle sind und wie sehr wir von ihnen abhängig sind, wird klar, wie verwundbar Unternehmen sind, die weiter auf Perimeter-basierte Sicherheit setzen.

Unternehmen können das traditionelle, lokale Identitätsmanagement nicht mehr verwenden, um auf Dienste zuzugreifen, da sich die Mehrheit der Geräte und Ressourcen, die die Benutzer benötigen, in der Cloud befinden. Um potenzielle Sicherheitslücken zu schließen und die Produktivität der Benutzer zu erhalten – egal wo sie sich befinden – ist es an der Zeit, das traditionelle, Perimeter-basierte Modell zu überdenken und einen identitätsbasierten Ansatz zu verfolgen, der weltweit so flexibel den Zugriff auf Daten ermöglicht wie die Cloud-Dienste, die wir nutzen.

GERÄT UND ZUGRIFF: SICHERHEITSEBENEN

Hinsichtlich Sicherheit und Authentifizierung gibt es drei übliche Faktoren, und jeder hat seine Schwachstellen:

- Gerätebasierte Sicherheit
- Benutzerbasierte Sicherheit
- Multi-Faktor-Authentifizierung

Gerätebasierte Sicherheit

Diese Sicherheitsmethode kann bei verwalteten Firmengeräten verwendet werden oder bei verwalteten Geräten, die nicht mit den Sicherheitsrichtlinien eines Unternehmens konform sind.

Dieses Sicherheitsmodell versagt beim Schutz des Geräts, wenn Anmeldedaten durch Phishing erlangt oder erraten werden. Außerdem ist ein Gerät nicht geschützt und nicht mit den Unternehmensstandards konform, wenn es nicht verwaltet wird, was auf viele Geräte zutrifft.

Benutzerbasierte Sicherheit

Diese Sicherheitsebene kann bei Geräten verwendet werden, die einen Benutzernamen und ein Passwort zum Zugriff benötigen. Geht jedoch ein nicht verwaltetes Gerät, das Zugriff auf Dienste und Ressourcen eines Unternehmens hat, verloren oder wird gestohlen, oder geraten die Anmeldedaten eines Benutzers in die falschen Hände, ist das gesamte Netzwerk einem Risiko ausgesetzt.

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung ist eine Sicherheitsebene, bei der dem Benutzer nur Zugriff auf sein Gerät und Unternehmensressourcen gewährt wird, nachdem er erfolgreich mehrmals auf verschiedenen Wegen überprüft wurde. Beispiele für Anmeldedaten zur persönlichen Identifizierung sind unter anderem:

- Etwas, das Sie wissen (ein Passwort)
- Etwas, das Sie haben (ein Sicherheitstoken)
- Etwas, das ein Teil von Ihnen ist (ein Fingerabdruck)

Da diese Methode einen Benutzernamen oder Passwort und eine zweite physische Authentifizierungsmethode (wie ein RSA-Token) verwendet, wirkt sie wie eine außerordentlich sichere Variante zur Überprüfung des Benutzers. Unternehmen fehlt es jedoch an Tools, um sie in all den vielfältigen Kontexten anzuwenden, in denen Geräte genutzt werden können. Es fehlt ihnen auch an Methoden, um Sicherheit für das breite Spektrum an Anwendungsfällen, Nutzern und Standorten zu bieten, die in diesen Kontexten auftreten.

Letztendlich reichen aber weder eine benutzerbasierte noch eine physische Authentifizierungsmethode allein aus. Unternehmen brauchen beides und noch mehr, ohne dabei die Benutzererfahrung zu beeinträchtigen.

IDENTITÄT IST DER NEUE PERIMETER

Mittlerweile gibt es eine Reihe an Anbietern, die Unternehmen unterstützen, Identitäten und Zugriffsrechte auf Dienste zu verwalten – unter anderem Centrify, Duo Security, Microsoft, Ping Identity, Okta, Sailpoint und Salesforce. Viele dieser Tools funktionieren mit bereits bestehender Infrastruktur zur Authentifizierung wie Active Directory und weiten diese Identitäten auf Cloud-Dienste aus. Hierfür verwenden sie Protokolle wir Oauth, SAML und OpenID.

Identität ist die Schnittmenge aller Benutzergeräte und kann einfache benutzer-, geräte- oder tokenbasierte Sicherheit übertreffen. Identitätsmanagement in Ihren Prozess der Sicherheitsverwaltung mit einzubeziehen ist der Schlüssel für eine sichere Umgebung in einer mobilen Welt des Cloud Computing.

„Verstöße und Angriffe auf die Sicherheit sind heute so ausgereift und verbreitet, dass der Verstand und die Hände des Menschen dies nicht alleine bewältigen können“, sagt Brad Anderson, Corporate Vice President von Microsoft.

> Lesen Sie mehr über EMS unter https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security

Unternehmen brauchen eine Reihe an Fähigkeiten, um die Risiken von Identität, Geräten und Applikationen zu verstehen, und letztendlich eine Garantie, dass nur vertrauenswürdige Benutzer, mit vertrauenswürdigen Geräten und vertrauenswürdigen Applikationen auf Daten zugreifen können.

Mit identitätsbasierter Sicherheit authentifiziert Microsoft die Anmeldedaten von Benutzern mit Azure Active Directory (AD), sobald ein Benutzer auf Microsoft Office 365 zugreift. Laut Anderson geschieht diese Authentifizierung der Identität tagtäglich 15 Milliarden Mal.

Über 90 % der Welt verwendet Active Directory als verlässliche Quelle für lokale Identitäten von Unternehmen. Für viele von ihnen ist Azure AD die verlässliche Quelle für Unternehmensidentitäten in der Cloud. Alles bei Microsoft ist auf Azure AD in Microsofts Cloud aufgebaut.

EINE LÖSUNG FÜR DIE SICHERHEITSLÜCKE

Während der 2017 Jamf Nation User Conference präsentierte Anderson eine neue Lösung für die Lücke in unserer modernen Sicherheitsarchitektur.

„Jamf Pro verwendet die Funktionalität von „Microsoft Workplace Join“ innerhalb von Azure Active Directory, um bei Jamf registrierte Mac Geräte mit allen anderen betriebseigenen und privaten Geräten im Unternehmen zu verbinden. Sobald Workplace Join abgeschlossen ist, kann Intune damit auf dieselbe Art arbeiten wie mit Geräten, die bei Intune registriert sind.“ Weiterhin sagt er: „So können Unternehmen für einen Zugriff auf ihre Unternehmensressourcen sorgen, der nicht nur auf den Anmeldedaten der Benutzer basiert, sondern auch auf der Konformität des Mac. Das nennen wir Conditional Access.

Jamf Pro, der Standard für Apple Gerätemanagement, kann Richtlinien auf Geräten durchsetzen. So können sie mit EMS Conditional Access auf Office 365 zugreifen. Von Jamf verwaltete Mac Computer können jetzt Workplace Joined in Microsofts Cloud erhalten, wenn sie die entsprechenden Konformitätsrichtlinien des Geräts von Intune erfüllen. Diese können auf die Bedürfnisse eines Unternehmens maßgeschneidert werden. Sobald die Daten des Computers in der Cloud sind, können, Microsoft Intune und Enterprise Mobility + Security (EMS) sich vollständig in Jamf integrieren, um diese Geräte zu verwalten.

Wenn ein nicht verwalteter Mac auf E-Mails oder andere Cloud-Dienste zugreifen will, kann die IT einen vom Benutzer initiierten Registrierungsvorgang von Jamf Pro aktivieren und sicherstellen, dass unsichere oder nicht verwaltete Geräte erst verwaltet werden müssen, bevor sie Zugriff erhalten.

Mac Richtlinien wie Passwortanforderungen können mit Intune definiert werden und ermöglichen es der IT, sie auf allen Systemen anzuwenden. Die Zusammenarbeit von Jamf und Microsoft erweitert die Möglichkeiten der mobilen Geräteverwaltung von Apple (MDM = Mobile Device Management) beim Zugriff auf lokale Tools auf einzigartige Art und Weise. Beispielsweise kann ein Administrator ein Konfigurationsprofil erstellen, das die Nutzung von starken Passwörtern prüft und umsetzt. Dies schließt die Lücke zwischen Unternehmensrichtlinien und was mit traditionellen MDM-Optionen auf dem Mac standardmäßig verfügbar ist.

Wenn Microsoft Anmeldedaten von Benutzern und Jamf Gerätedaten prüft, läuft in Echtzeit eine Analyse des Benutzerrisikos, des Geräterisikos (ist es mit den Unternehmensrichtlinien konform oder nicht) und des Applikationsrisikos (welche App verwendet wird), um zu bestimmen, ob Zugriff auf die Cloud-Ressourcen gewährt oder der Zugriff blockiert werden soll.

Dort, wo die Multi-Faktor-Authentifizierung nicht greift, da sie sich hauptsächlich an den Benutzer richtet, prüft diese neue Methode außerdem, wie der Benutzer mit Informationen umgeht. Sie stellt sicher, dass die geprüfte Identität ein vertrauenswürdiger Benutzer auf einem konformen Gerät ist.

Die Multi-Faktor-Authentifizierung wird für Unternehmen jetzt um die Konformitätsprüfung erweitert: 1. Benutzername und Passwort, 2. Code und Token, und 3. Gerätekonformität.

Jetzt können Unternehmen dynamisch und je nach Kontext den richtigen Zugriff gewähren, basierend auf Benutzer, Gerät und dem Kontext des Anwendungsfalls. So haben sie anpassungsfähige und flexible Grenzen, die Mitarbeiter mit mehreren Geräten und Arbeitsorten heute benötigen.

PROXY-FREIER CONDITIONAL ACCESS

EMS Conditional Access ist entscheidend, um diesen Sicherheitsansatz umzusetzen, und ermöglicht es, jedes Risiko in Bezug auf Identität, Gerät und Applikation automatisch zu prüfen.

So hat die IT die Kontrolle darüber, unter welchen Bedingungen Benutzer auf Ihre Ressourcen zugreifen können.

Viele Anbieter von Enterprise Mobility Management (EMM) bieten Lösungen, die den Conditional Access mit einem Proxy-Server unterstützen, um externe Geräte beim Zugriff auf Ressourcen zu authentifizieren, die innerhalb der Netzwerkgrenzen eines Unternehmens liegen. Ein Proxy-Server ist ein Server, der als Mittler für Anfragen von Benutzern agiert, die von anderen Servern aus auf Ressourcen zugreifen wollen. Dies betrifft sowohl den eingehenden Datenverkehr in einem Netzwerk als auch den ausgehenden. Bei der einzigartigen Zusammenarbeit von Jamf und Microsoft sind Proxies nicht nötig. Alles wird direkt in Azure Active Directory integriert, das als einzige verlässliche Quelle dient. Die Konformität eines Geräts kann als Voraussetzung dienen, um Zugriff auf verschiedene Dienste zu erlangen. Es gibt hierbei also keinen Mittler wie einen Proxy-Server, der eine Netzwerkkonfiguration erfordert, um zu entscheiden, wer Zugriff erlangt, oder der als zusätzliches Teil der Infrastruktur des Netzwerks gewartet werden muss. Dies bietet eine bessere, direkt in Azure Active Directory und Intune integrierte Authentifizierung und schließt eine weitere Sicherheitslücke.

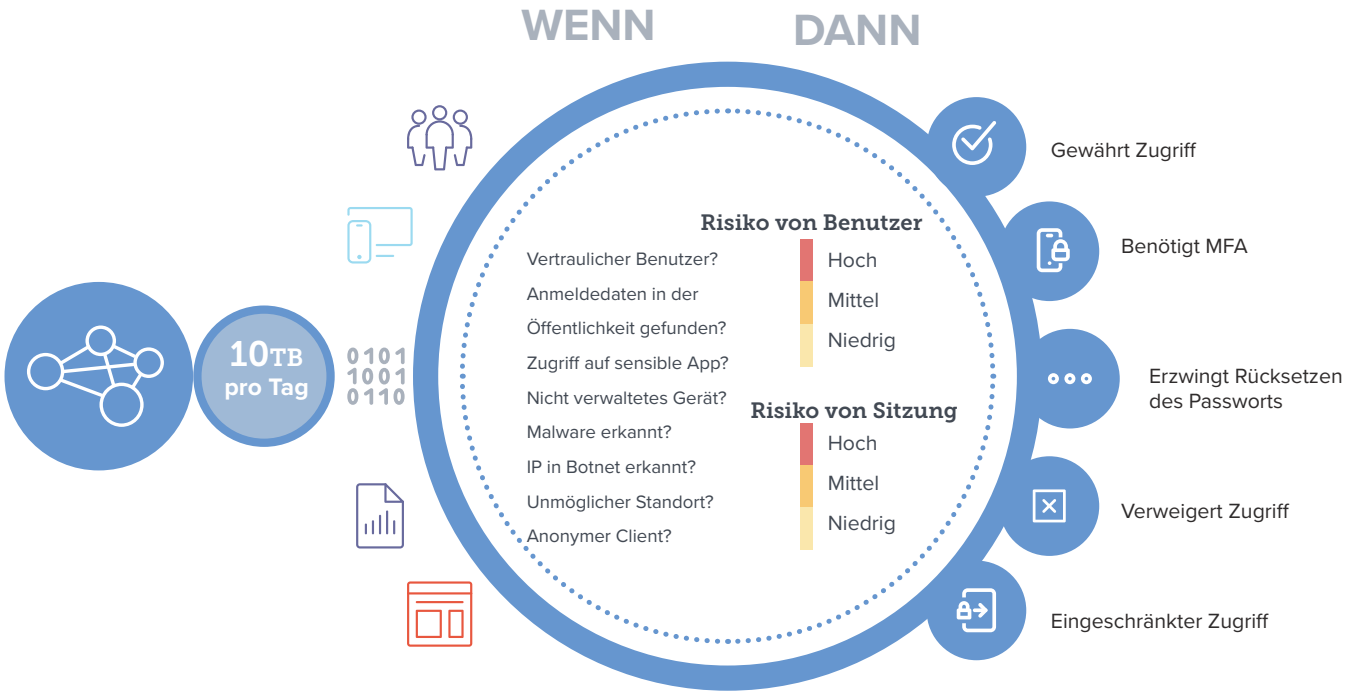
Unternehmen haben die schnelle Einführung von Mac Geräten akzeptiert und anerkannt. Daher brauchen sie auch für diese eine Lösung, die über Perimeter-basierte Sicherheit hinausgeht, genau wie bei anderen Geräten. Man könnte ganz allgemein sagen, dass man zuerst dem Gerät vertrauen können muss, bevor man dem Benutzer vertraut, der sich damit authentifiziert.

Microsoft und Jamf haben zusammen eine zweckorientierte Lösung erschaffen, die sich vollständig in die grundlegenden Technologien von Azure Active Directory und Intune integriert. So bleibt die ursprüngliche Benutzererfahrung intakt und die Stärken von Jamf und Intune werden genutzt, um dem Kunden eine Lösung anzubieten, die weit über das hinausgeht, was jedes Unternehmen selbst anbieten kann.

PARTNERSCHAFT VON MICROSOFT UND JAMF

Die EMS-Partnerschaft von Jamf und Microsoft bietet eine automatisierte Compliance Management Lösung für Mac Computer, die auf Apps zugreifen, die mit einer Azure AD Authentifizierung eingerichtet wurden. Diese Zusammenarbeit verwendet Conditional Access, damit nur vertrauenswürdige Benutzer auf konformen Geräten mit genehmigten Apps auf Firmendaten zugreifen können.

Jamf und Microsoft verhindern gemeinsam, dass ein unautorisierter Benutzer mit einem Gerät auf bestimmte vom Unternehmen bereitgestellte Ressourcen zugreifen kann. Hierbei kann es sich um ein privates Gerät handeln, ein nicht verwaltetes Gerät oder ein von der Firma verwaltetes Gerät,



EMS Conditional Access

das nicht mit den Sicherheitsrichtlinien übereinstimmt und so das Risiko nicht erwünschter Zugriffe auf Firmendaten erhöht. Dies wird erreicht, indem die Geräte der Benutzer, mit denen sie auf Microsoft Office 365 und andere Applikationen zugreifen wollen, von Azure AD geprüft werden.

Was diesen Vorgang von anderen Anbietern mit Conditional Access unterscheidet, ist dass die Geräte keinen Proxy durchlaufen müssen. Die Vermeidung des Proxys bietet Unternehmen einen effizienteren Weg, um ihre Geräte zu schützen.

Und was ist mit der Benutzererfahrung? Sie ist eindeutig und unkompliziert. Ist ein Gerät nicht konform und ein Benutzer versucht, sich zu authentifizieren und Zugriff zu erlangen, erhält er eine Nachricht auf sein Gerät, die besagt, dass er bestimmte Voraussetzungen nicht erfüllt. Der Benutzer kann die Nachricht dann anklicken und die einzelnen Schritte durchgehen, um das Konformitätsproblem zu lösen.

Die Nachricht informiert den Benutzer darüber, was gerade passiert und warum das Gerät nicht konform ist. Liegt das Problem beim Passwort, so kann der Benutzer einfach auf „Problem lösen“ klicken und das Passwort aktualisieren. Entspricht es dann den Richtlinien, erhält er Zugriff.

Die Informationen, die Jamf an Microsoft weiterleitet, sorgen für eine höhere und intelligentere Sicherheit, was zu einer besseren Management Lösung führt, die wiederum eine bessere Benutzererfahrung bietet.

IN DEN WORTEN VON ANDERSON: „EINE LÖSUNG, DIE BENUTZER BEGEISTERT UND DER DIE IT VERTRAUT.“

Um eine zeitgemäße, zuverlässige und sichere Benutzererfahrung anzubieten, müssen sich die Arbeitsabläufe an Arbeitszeiten und -orte der Menschen anpassen – und an die Tools, die sie verwenden. Die IT muss ihre Schutzprotokolle auf eine natürliche Art integrieren und Richtlinien erstellen, damit Benutzer, die sie nicht erfüllen, nahtlos wieder konform werden können, ohne dabei ein Risiko für Firmendaten darzustellen.

Jamf und Microsoft geben der IT zusammen die Möglichkeit, dieses Ziel mit identitätsbasierter Sicherheit zu erreichen. So öffnet sich die Welt für die Benutzer, und das, ohne Proxies zu verwenden.

Seit Jahrzehnten errichten Unternehmen als erste Verteidigungslinie „Mauern“ und bestimmen Perimeter für die Netzwerke ihrer Firma. Die interne Sicherheit kam dabei manchmal etwas zu kurz. Der Umgang mit Daten und die Welt haben sich verändert und diese zeitgemäßen Lösungen widmen sich diesen Veränderungen.

Erfahren Sie, wie Sie Ihre Sicherheitsroutinen weiterentwickeln können, damit die IT alle nötigen Tools hat und die Benutzer auf dem Gerät ihrer Wahl geschützt und produktiv bleiben.

Bessere Sicherheit beginnt hier

jamf

www.jamf.com

Um mehr darüber zu erfahren, wie sie Jamf Pro für die Verwaltung Ihrer Macs oder iOS nutzen können, besuchen Sie **jamf.com/de/produkte/jamf-pro**