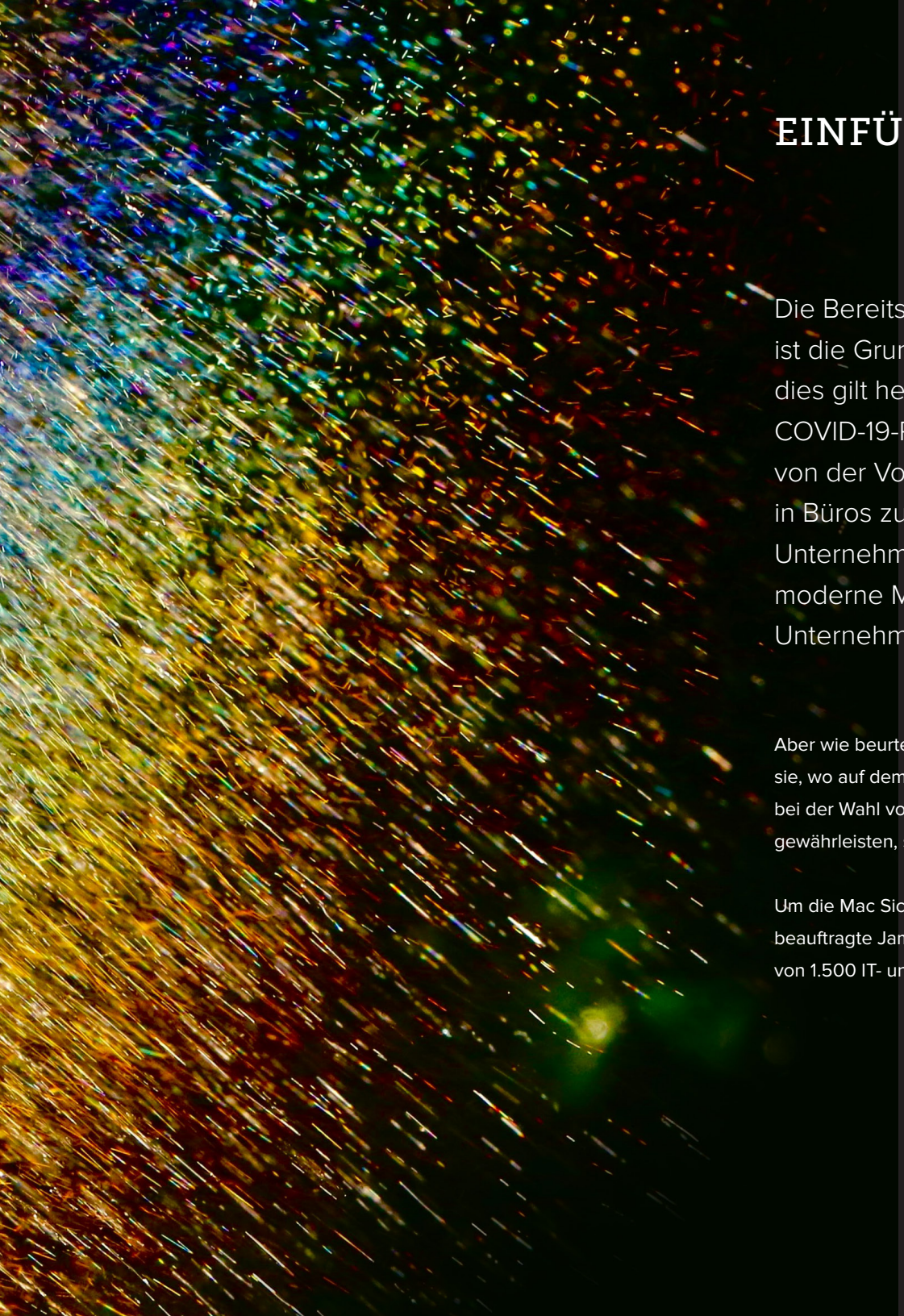
Umfrage: Stand der

MAC SICHERHEIT

jamf



EINFÜHRUNG

Die Bereitstellung von Spitzentechnologie für Mitarbeiter ist die Grundlage für ein florierendes Unternehmen – dies gilt heute mehr als je zuvor. Seit dem Beginn der COVID-19-Pandemie haben wir weltweit die Umstellungen von der Vor-Ort-Bereitstellung von Geräten und Netzwerken in Büros zur Telearbeit erlebt. Diese Veränderung hat die Unternehmenssicherheit in den Vordergrund gerückt, denn moderne Methoden zum Schutz der Mitarbeiter ist für den Unternehmenserfolg von größter Bedeutung.

Aber wie beurteilen Organisationen ihren aktuellen Sicherheitsstatus? Woher wissen sie, wo auf dem Sicherheitsspektrum sie sich befinden? Und welche Faktoren spielen bei der Wahl von Hardware und Software eine Rolle, um nicht nur die Sicherheit zu gewährleisten, sondern auch eine positive Endbenutzererfahrung?

Um die Mac Sicherheit in Unternehmen zu bewerten und weitere Fragen zu beantworten, beauftragte Jamf das Marktforschungsunternehmen Vanson Bourne mit der Befragung von 1.500 IT- und InfoSec (Informationssicherheit) Experten in Nordamerika und Europa.

ZUSAMMENFASSUNG

Die Ergebnisse zeigen, dass die Mac Nutzung zunimmt, selbst in Unternehmen, die überwiegend andere Laptops als Macs verwenden. Zu den wichtigsten Faktoren zählen die Vorliebe seitens IT und InfoSec, die Wahrnehmung, dass diese Geräte standardmäßig sicherer sind als Geräte anderer Marken, und die Überzeugung, dass es im Vergleich zu anderen Hardwaretypen einfacher ist, die vollständige Sicherheit eines Mac aufrechtzuerhalten.

Aber kein Betriebssystem und keine Hardware ist perfekt. Unabhängig von der Hardware priorisieren Unternehmen künftige Sicherheitsausgaben in mehreren Schlüsselbereichen, wie z. B. Vorbeugung von Datenverlust, Antivirensoftware sowie Instrumente für den Endgeräteschutz und für Interventionen.

Dieser Anstieg der Sicherheitsausgaben spiegelt die COVID-19-Pandemie wider, die für viele Mitarbeiter den Wechsel von der Arbeit im Büro zur Telearbeit bedeutete. Aus diesem Grund war der Fortbestand der Sicherheit der Endgeräte – unabhängig davon, wo sie eingesetzt oder welche Ressourcen damit abgerufen wurden – eine absolute Notwendigkeit.

In diesem Bericht werden die aktuelle Gerätenutzung sowie Ansätze, Herausforderungen und zukünftige Zustände der Endgerätesicherheit bewertet, um ein vollständiges Unternehmensbild zu erstellen.

TEILNEHMERSTATISTIK

Um eine globale Perspektive zu erhalten, haben wir IT- und InfoSec-Mitarbeiter aus kleinen Unternehmen bis großen Konzernen in Nordamerika und Europa befragt. Die Hälfte der 1500 Befragten benutzte hauptsächlich Mac Geräte, die andere Hälfte Geräte anderer Marken.

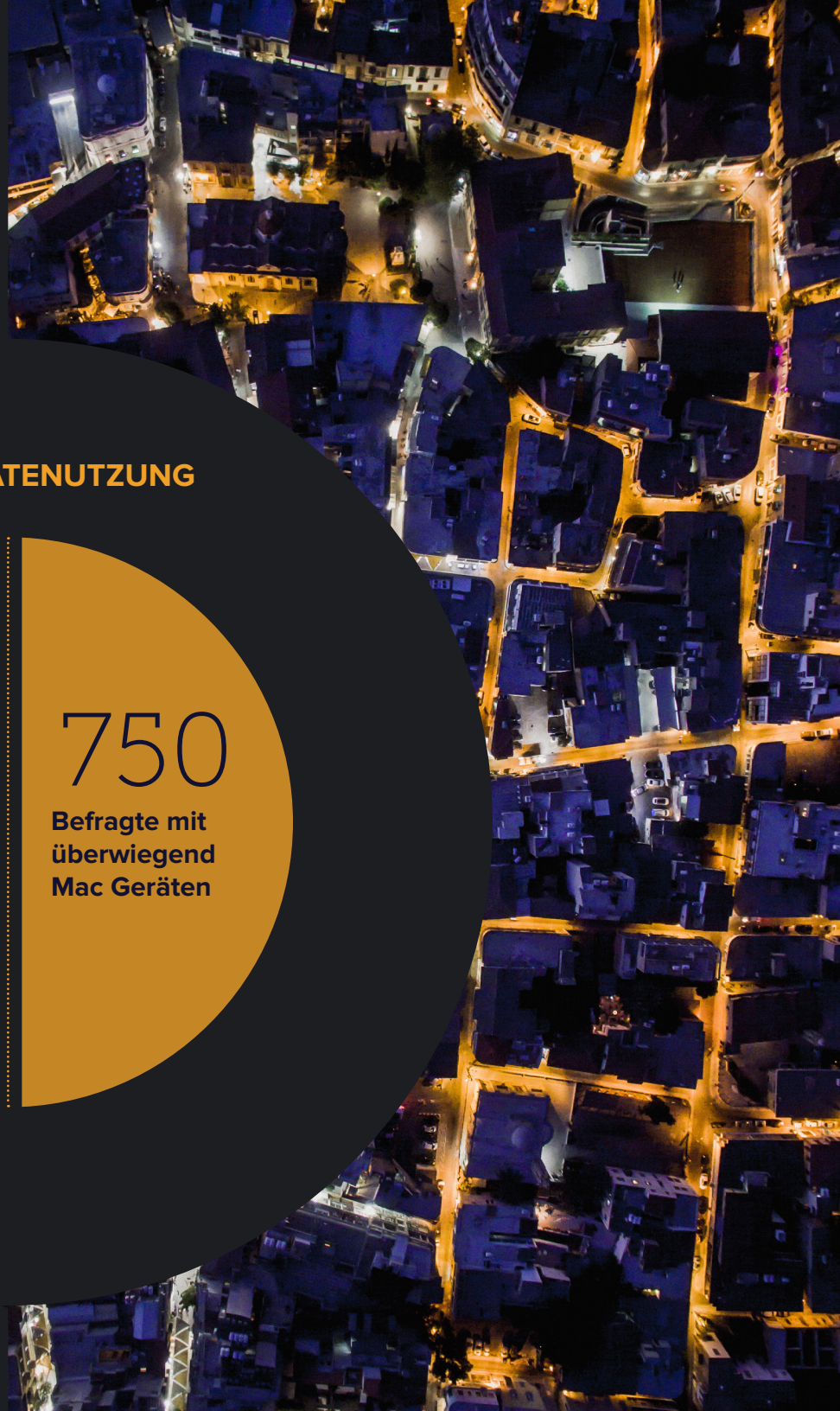
NACH ORGANISATIONSGRÖSSE

Anzahl der Mitarbeiter	Befragte
100-199	150
200-499	252
500-999	**327**
1.000-2.999	**358**
3.000-4.999	261
5.000 oder mehr	152

NACH GERÄTENUTZUNG

750
Befragte überwiegend mit Benutzern anderer Geräte als Mac

750
Befragte mit überwiegend Mac Geräten



MAC NUTZUNG NIMMT ZU

Es gibt klare Hinweise darauf, dass alle IT- und InfoSec-Befragten, unabhängig davon, welche Geräte überwiegend in ihren Unternehmen verwendet werden, für die nächsten 12 Monate einen Anstieg der verwendeten Mac Geräte erwarten.

74 % der Befragten, die hauptsächlich in Mac Umgebungen arbeiten, geben an, dass sie die Anzahl der Geräte in ihrer Organisation erhöhen werden

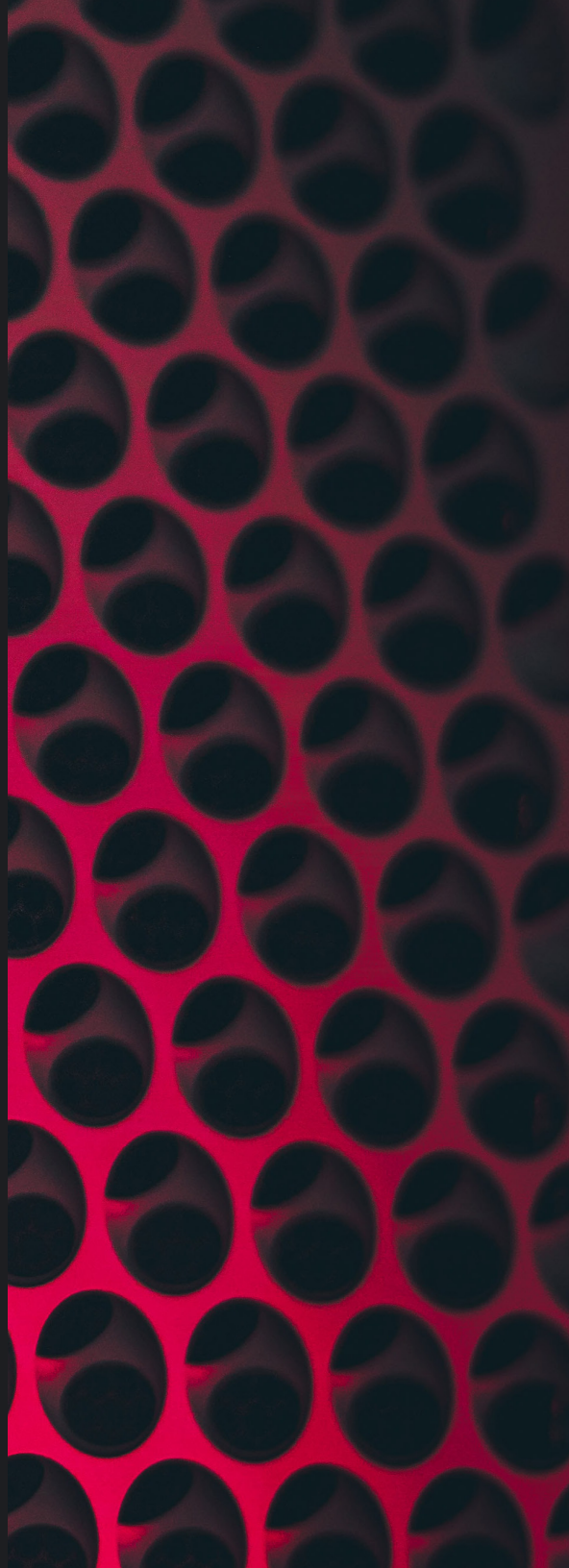
65 % der Befragten, die hauptsächlich in Umgebungen anderer Marken als Mac arbeiten, geben an, dass sie eine Steigerung der Anzahl an Mac Geräten in Betracht ziehen werden

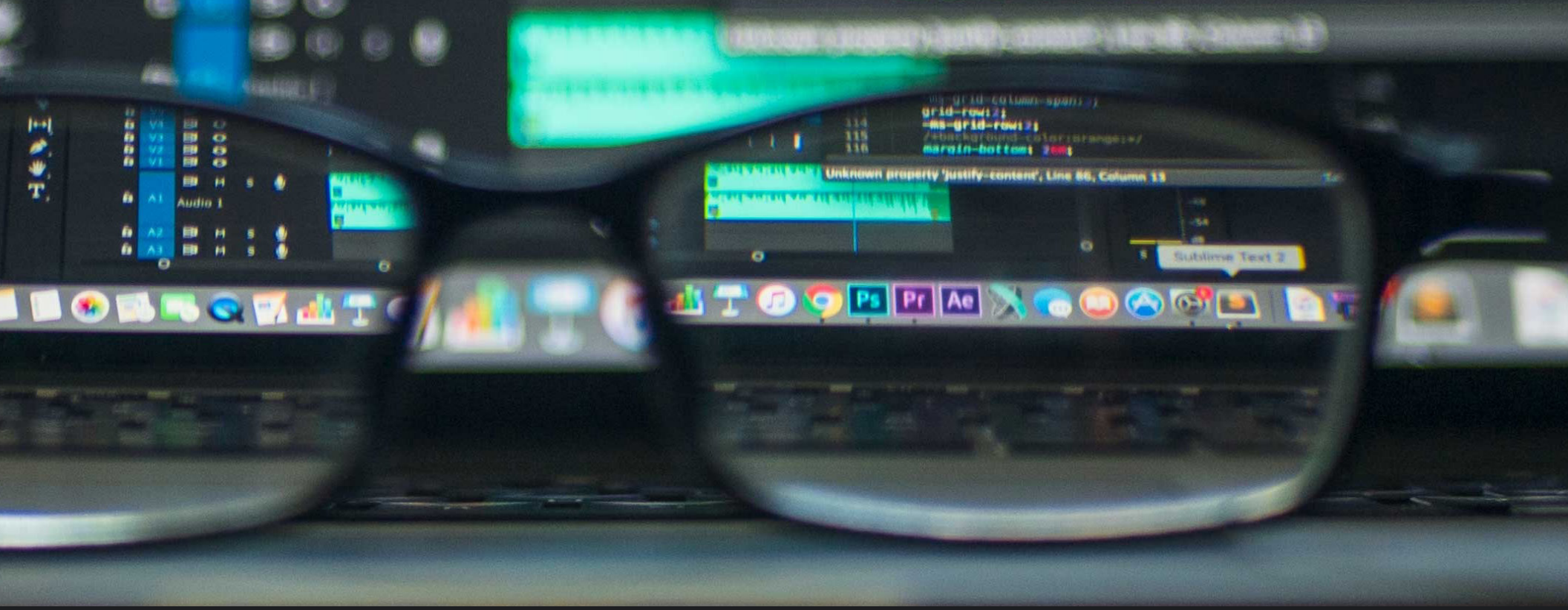
Warum bevorzugen IT- und InfoSec-Profis Mac?

77 % der Unternehmen – ob mit oder ohne Mac Umgebung – glauben, dass Mac Geräte standardmäßig sicherer sind als andere Geräte

79 % der Befragten, die hauptsächlich in Mac Umgebungen arbeiten, geben an, dass der wahrgenommene gute Ruf in Bezug auf Sicherheit ihre Entscheidung für den Kauf von Mac Geräten positiv beeinflusst

57 % der Befragten, die hauptsächlich in Umgebungen mit anderen Geräten arbeiten, geben an, dass der wahrgenommene gute Ruf in Bezug auf Sicherheit ihre Entscheidung für den Kauf von Mac Geräten positiv beeinflusst





MAC NUTZUNG NIMMT ZU

Unter IT- und InfoSec-Experten herrschte Einigkeit darüber, dass die Überwachung und Sichtbarkeit von Endgeräten auf Mac einfacher ist, aber auch darüber, dass sich die Sicherheit von Mac Geräten leichter bewahren lässt.

Wenn alle Sicherheitstools aktiviert sind, können **71 % der Befragten**, deren Unternehmen sowohl Mac als auch andere Geräte verwenden, eine bessere Endbenutzer-Zufriedenheit mit Mac Geräten verzeichnen.

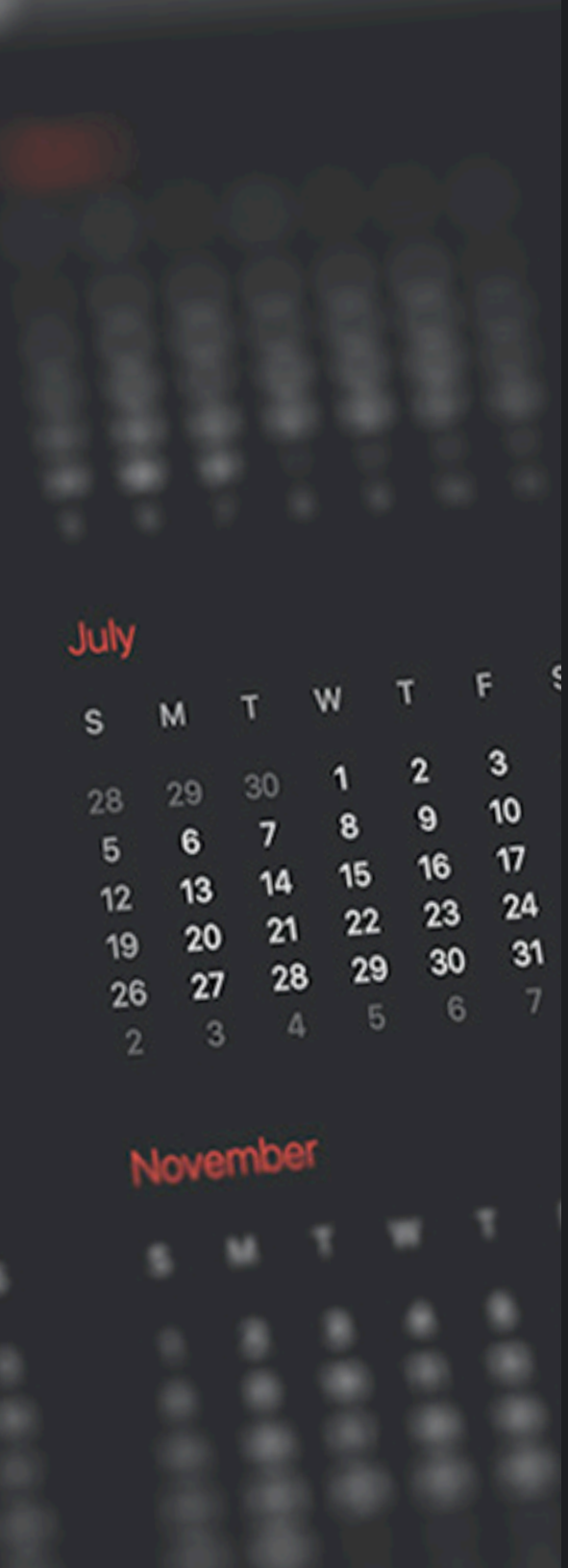
Der wahrgenommene Ruf und die Zufriedenheit der Endbenutzer führen dazu, dass **84 % der Befragten**, deren Unternehmen sowohl Mac Geräte als auch Geräte anderer Marken verwenden, angeben, dass sie sich für Mac entscheiden würden, wenn alle Endbenutzer ihres Unternehmens denselben Gerätetyp verwenden müssten.

71 %

der Befragten geben an, dass Mac eine bessere Zufriedenheit der Endbenutzer bietet

84 %

der Befragten würden Mac für ihre gesamte Belegschaft wählen



HERAUSFORDERUNGEN BEIM OS UPDATE

Trotz der positiven Sicherheitswahrnehmung für Mac, erfahren Unternehmen immer noch Herausforderungen und Bedenken hinsichtlich der Sicherheit von Betriebssystemen und hinsichtlich ihrer gesamten Geräteflotte.

Mac Benutzer berrichten im Durchschnitt weniger Zeit für die Ausführung von Betriebssystem-Sicherheitspatches als ihre Kollegen, die keine Mac Geräte verwenden. Trotz des Geschwindigkeitsunterschieds bei Mac Upgrades verbleiben von der Patch-Veröffentlichung bis zur Bereitstellung durchschnittlich vier Tage.

Mac Benutzer führen Betriebssystem-Sicherheitspatches durchschnittlich

30 % **SCHNELLER** als Benutzer von anderen Geräten aus

4 Tage
DURCHSCHNITTLICH

dauert es um Betriebssystem-Sicherheitspatches auf dem Mac auszuführen

Für wichtige Betriebssystemversionen ist die Diskrepanz zwischen Mac Geräten und anderen Geräten sogar noch größer.

Mac Benutzer installieren wichtige Betriebssystemversionen fast

2,5-mal **SCHNELLER** als Benutzer von anderen Geräten

5 Tage
DURCHSCHNITTLICH

dauert es für Mac Benutzer zur Ausführung wichtiger Betriebssystemversionen

HERAUSFORDERUNGEN BEIM OS-UPDATE

Die Zeit, die für die Einführung des neuesten Hauptbetriebssystems benötigt wird, lässt Geräte für Schwachstellen offen. Insbesondere große Organisationen haben damit zu kämpfen. **Warum?**

TOP 5 GRÜNDE

Kompatibilitätstests

Kompatibilität von Sicherheitsinstrumenten

Kompatibilität interner Anwendungen

Compliance-Anforderungen

Drittanbieter-Kompatibilität

Verzögerungen beim Upgrade auf das neueste Hauptbetriebssystem verstärken die Sicherheitsbedenken für Unternehmen, da bekannte Sicherheitslücken für Angreifer zugänglich bleiben. Weltweit sind Unternehmen einer Vielzahl von Bedrohungen für Endbenutzergeräte ausgesetzt. Unternehmen stehen unter dem ständigen Druck, sich vor potenziell schädlichen Cybersicherheitsangriffen zu schützen. Insbesondere in Remote-Arbeitsumgebungen müssen sich Unternehmen vor häufigen Angriffen auf ihre Geräte, Benutzer und Daten schützen.

TOP 5 CYBERSICHERHEITSANLIEGEN

Malware

Datenverlust

Phishing/Spear-Phishing

Nicht autorisierte Software

Ransomware

SICHERHEITSHERAUSFORDERUNGEN

Wenn es darum geht, einen potenziellen Sicherheitsvorfall einzudämmen, erweisen sich viele Bedenken – **durchschnittlich 37 % in Nordamerika und Europa** – als falsch positive Bedenken. Dies führt zu kostspieligem Zeit- und Ressourcenaufwand für die Untersuchung nicht vorhandener Bedrohungen. Wenn Zeit für die Überprüfung von Fehlalarmen aufgewendet wird, bleibt weniger Zeit, um tatsächliche Bedrohungen zu identifizieren.

FAST DIE HÄLFTE der IT- und InfoSec-Teams nennen unbekannte Bedrohungen als ihre größte Herausforderung bei der Eindämmung (47 %) und Behebung (45 %) eines potenziellen Sicherheitsvorfalls. Weitere wichtige Herausforderungen bei der Behebung sind:

MANGEL AN

- Zeit
- Personal
- Tools
- Geld

Obwohl Mac als das Gerät mit der besten standardmäßigen Sicherheit angesehen wird, steigt mit zunehmender Akzeptanz im Unternehmen auch Beachtung von Cyberangriffen und Bedrohungen. Um dem entgegenzuwirken, sind Präzision und die richtige Zuweisung von Tools und Ressourcen unerlässlich.

ZUKUNFT DER SICHERHEIT

Das Ziel von modernen Unternehmen: nachhaltige Investitionen in Sicherheit.

96 % der Unternehmen planen, mehr für die Sicherheit von Endgeräten auszugeben, insbesondere:

1. Data Loss Prevention (Vorbeugung von Datenverlust, DLP)
2. Anti-Virus/Next Generation Anti-Virus (AV/NGAV)
3. Endpoint Detection and Response (EDR)
4. Security Information and Event Management (SIEM)
5. Cloud Access Security Brokers (CASB)

Mit diesen größeren Investitionen in Sicherheit wollen IT- und Sicherheitsteams ihre Geräteflotte stärken und die Vorbeugung, Erkennung, Intervention und Behebung von Sicherheitsvorfällen verbessern. Dies ist unbedingt erforderlich, da eine verteilte Belegschaft die IT- und InfoSec-Teams nur stärker belastet, insbesondere angesichts der Tatsache, dass die Zahl der Telemitarbeiter infolge von COVID-19 um 38 % gestiegen ist.

SCHLUSSFOLGERUNG

COVID-19 hat dafür gesorgt, dass mehr Arbeitnehmer als je zuvor im Homeoffice arbeiten. Technologieerfahrung ist heute ein wesentlicher Faktor für die Mitarbeitererfahrung. Unternehmen müssen sich darauf konzentrieren, Mitarbeitern die bestmögliche Endbenutzererfahrung und den bestmöglichen Schutz zu bieten.

Während sich Unternehmen an die Telearbeit anpassen, ist es wichtiger denn je, die Sicherheit von Endgeräten zu gewährleisten und Ressourcen entsprechend zuzuweisen, um Bedrohungen am besten zu stoppen.

JAMF APPLE ENTERPRISE MANAGEMENT

Jamf ist die einzig umfassende Apple Enterprise Management-Lösung, die den gesamten Lebenszyklus von Apple im Unternehmen automatisiert, einschließlich Gerätebereitstellung, -verwaltung und -sicherheit, ohne die Endbenutzererfahrung zu beeinträchtigen, wobei es nicht erforderlich ist, dass die IT das Gerät berührt. Teil des Portfolios ist Jamf Protect – ein exklusiv für Mac entwickelter Schutz für Endgeräte – die den Sicherheitsstandard von Mac erweitert und Sie in die Lage versetzt, Bedrohungen zu erkennen, zu verhindern und Sicherheitsvorfälle zu beheben. Mit der Unterstützung von Apple Betriebssystemversionen am selben Tag werden Jamf Lösungen niemals der Grund sein, warum Sie Updates verzögern und Geräte Angriffen aussetzen.

Aus diesem Grund vertrauen sicherheitsorientierte Organisationen wie 10 der 10 größten US-Banken (laut bankrate.com) und 24 der 25 wertvollsten Marken der Welt (laut Forbes) darauf, dass Jamf ihre Apple Umgebung verwaltet.

Die kostenlose Testversion zeigt Ihnen, was Jamf zu bieten hat.

TESTVERSION ANFORDERN

Oder wenden Sie sich für eine Testversion an Ihren bevorzugten autorisierten Apple-Händler.