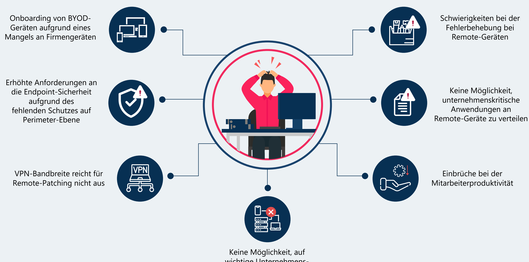
ENDPOINT MANAGEMENT UND SECURITY-HERAUSFORDERUNGEN IN CORONA-ZEITEN

Zum ersten Mal seit Beginn des digitalen Zeitalters ist fast die gesamte Weltbevölkerung zu Remote- bzw. Home-Office-Modellen übergegangen, um die Verbreitung des Corona-Virus einzudämmen. Diese beispiellose Veränderung hat nicht nur neue Sicherheitsrisiken mit sich gebracht, sondern hat sich auch als Herausforderung für das Endpoint Management und den Remote-Zugriff auf kritische Unternehmensressourcen erwiesen.

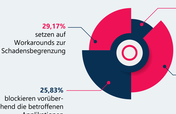
Wir haben Informationssicherheits- und IT-Fachleute befragt, um herauszufinden, wie sich die Corona-Krise auf die IT auswirkt. Wie gehen Unternehmen aktuell mit den Remote-Work-Szenarien um und wie stellen sich Unternehmen auf die kommenden Trends ein, die die neue Normalität möglicherweise mit sich bringt?

TOP-BEDENKEN BEI REMOTE-ARBEITSMODELLEN

47% der Befragten gaben an, dass sie vor neuen Herausforderungen stehen, jetzt, da sie remote arbeiten.



SO REAGIEREN UNTERNEHMEN AUF ZERO-DAY-SCHWACHSTELLEN



Immer mehr Organisationen gehen dazu über, Anwendungen mit Zero-Day-Schwachstellen **vorübergehend zu blockieren**, da ihre Endpoints vermehrt unsicheren Internetverbindungen ausgesetzt sind.

FERNARBEIT FÖRDERT DAS WACHSTUM VON BYOD-MODELLEN UND SELF-SERVICE-PORTALEN

15% der Unternehmen verfügen nicht über genügend Firmen-Laptops, um die Arbeit aus der Ferne zu ermöglichen. Infolgedessen gibt es einen Ansteg bei der Nutzung privater Geräte für die Arbeit.

43% der befragten Organisationen stellen Endanwendern ein Self-Service-Portal zur Verfügung, um lizenzierte Software zu installieren, die sie zur Durchführung ihrer täglichen Arbeit benötigen.

73% der Unternehmen, deren Remote-User für Schwachstellen- und Patch-Scans eine VPN-Verbindung benötigen, klagen über Engpässe und signifikant reduzierte Geschwindigkeit bei der Update-Bereitstellung.

PATCHING WURDE KOMPLIZIERTER

48% der Unternehmen mussten Remote-Benutzern die Flexibilität einräumen, Patch-Bereitstellungen und anschließende Neustarts zu verschieben, um Unterbrechungen der Produktivität zu vermeiden.

Im Durchschnitt erhalten IT-Administratoren jetzt **25** Helpdesk-Tickets pro Tag. **43%** der Befragten gaben an, dass sie – seit die Mitarbeiter remote arbeiten – mehr Tickets erhalten.

STARKER ANSTIEG BEI DER ZAHL DER HELPDESK-TICKETS

Die meisten Admins gaben an, dass sie durchschnittlich **2,5 Stunden** zusätzlich arbeiten, um Helpdesk-Tickets zu lösen und Probleme zu beheben.

46% der Admins verwenden Remote Access Tools zur Fehlerbehebung.

ERHÖHTE SICHERHEITSANFORDERUNGEN FÜR UNTERNEHMENSGERÄTE AUFGRUND MANGELHAFTEN PERIMETER-SCHUTZES

45% der Befragten mussten Einschränkungen durchsetzen, wie z. B. eine Festplatten-Verschlüsselung auf den Firmengeräten der Benutzer.

42% haben Social-Media- und Spiele-Anwendungen blockiert, da sie die Produktivität der Mitarbeiter bei der Arbeit von zuhause aus beeinträchtigen können.

38% verhindern, dass sich Remote-Computer mit nicht vertrauenswürdigen Geräten verbinden.

70% haben Browser-Sicherheitskontrollen auf Endpoint-Ebene eingeführt, um Zugriffe auf bösartige Webinhalte zu verhindern, wenn keine Proxy-Server oder DNS-Filterung vorhanden sind.

Etwas mehr als drei Viertel der Befragten antworteten, dass ihr Unternehmen eine wesentliche Dienstleistung ist,

die trotz Pandemie funktionieren muss, aber **26%** von ihnen arbeiten mit Werkzeugen, die für die Fernarbeit nicht förderlich sind. Angesichts der Veränderungen im Endpoint Management, die durch das Arbeiten im Home Office hervorgerufen werden, ist die Investition in die richtige Technologie in vielerlei Hinsicht wichtiger denn je.

DIE ULTIMATIVE LÖSUNG FÜR AUSGEZEICHNETE FERNARBEIT

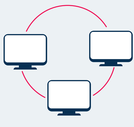
Ganz gleich, ob plötzlicher Wechsel zum Remote-Arbeiten als Reaktion auf die Pandemie oder der Wunsch, mit zukünftigen Trends schrittzuhalten: Die ganzheitlichen Endpoint-Management- und Sicherheitslösungen von ManageEngine sind die richtigen Werkzeuge, um Ihren Mitarbeitern außerhalb Ihrer Unternehmensräume sichere und effiziente Arbeitsbedingungen zu bieten. Unser breites Angebot an robusten Lösungen bietet:

- **Fernüberwachung und Remote-Fehlerbehebung**
- **BYOD und Modern Device Management**
- **Remote-Bereitstellung von Betriebssystemen und Software**
- **Schwachstellen- und Sicherheitskonfiguration-Management**
- **Remote-Patching ohne VPN-Einschränkungen**
- **Zero-Trust-basierte Anwendungs- und Gerätesteuerung**
- **Containerisierung von Unternehmensdaten**
- **Webfilterung und Browser-Sicherheit**
- **Müheloser Zugang zu Unternehmensressourcen**
- **Nahtloses Mitarbeiter-Onboarding**

WIE KÖNNEN UNSERE ENDPOINT-MANAGEMENT- UND SICHERHEITS-LÖSUNGEN EINE UNTERBRECHUNGSFREIE FERNARBEIT ERMÖGLICHEN?

WEBBASIERTE LÖSUNGEN

Alle unsere Lösungen sind webbasiert. Ein Gerät mit Internet-Verbindung ist alles, was Sie brauchen, um Ihre globale hybride IT aus der Vogelperspektive zu betrachten und all Ihre Endpoint-Management- und Security-Aufgaben von überall aus und jederzeit durchzuführen.



REMOTE-CLIENT-AGENTEN

Sind Sie besorgt über Endgeräte, die sich mit dem Netzwerk verbinden? Nutzen Sie unsere agentenbasierte Technologie, um Endpoint-Management- und Security-Aufgaben unterbrechungsfrei in Ihrer verteilten IT-Infrastruktur durchzuführen - ohne auf Ihre VPN-Verbindung angewiesen zu sein.

KATASTROPHEN-MANAGEMENT

Mit der Failover-Server-Option, die übernimmt, falls der primäre Server ausfällt, können Sie die Geschäftskontinuität aufrechterhalten und Ausfallzeiten vermeiden.

ALSO, WORAUF WARTEN SIE NOCH? HIER FINDEN SIE ALLES, UM DIE WESENTLICHEN VORAUSSETZUNGEN FÜR DAS MANAGEMENT UND DIE ABSICHERUNG VON HOME-OFFICE-ARBEITSUMGEBUNGEN ZU SCHAFFEN:

Jetzt zugreifen