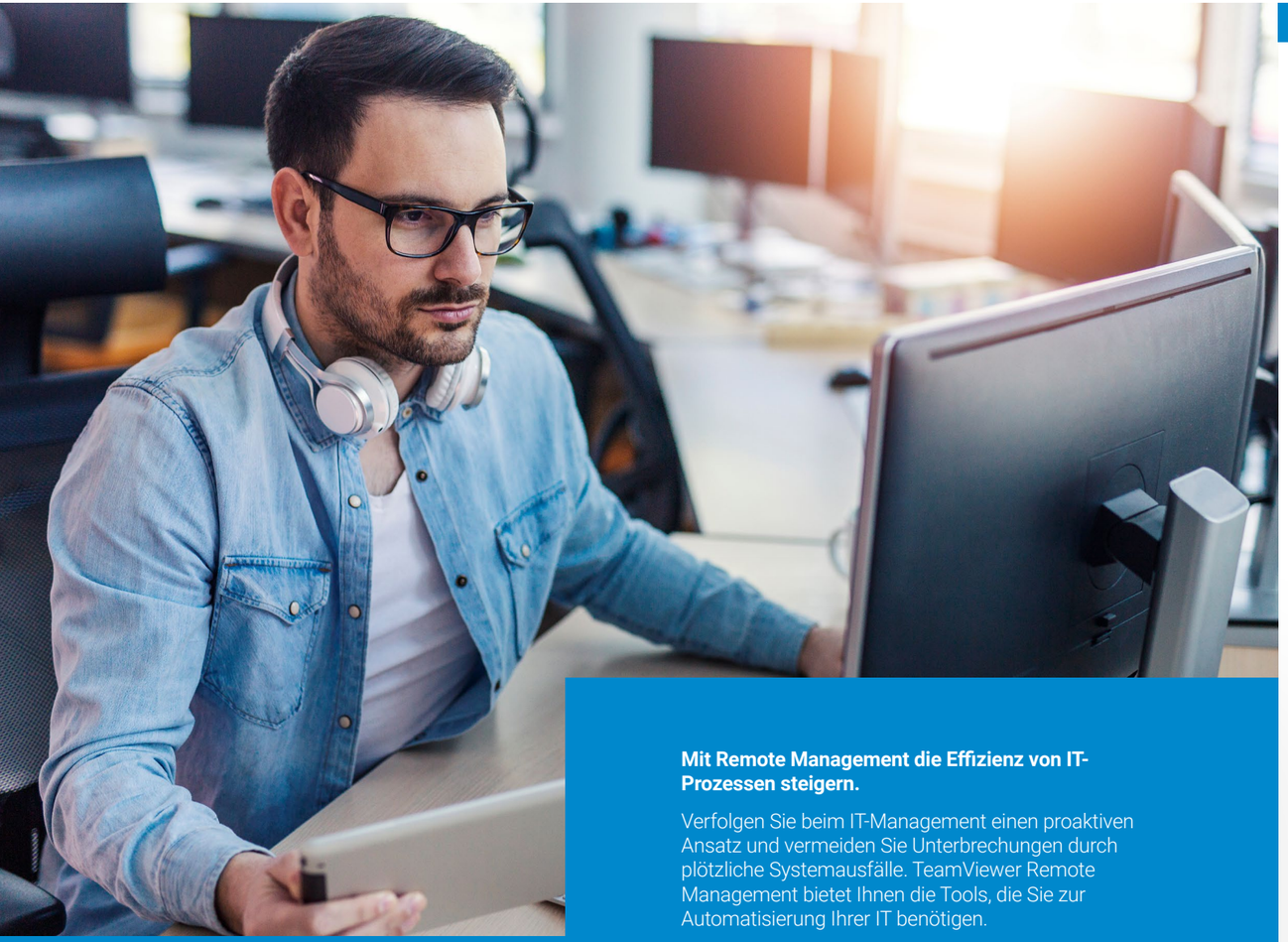
TeamViewer
Remote Management

Ihre professionelle IT-Management-Plattform

Proaktives IT-Management mit TeamViewer Remote Management

Übernehmen Sie die Kontrolle über Ihre IT-Infrastruktur



Mit Remote Management die Effizienz von IT-Prozessen steigern.

Verfolgen Sie beim IT-Management einen proaktiven Ansatz und vermeiden Sie Unterbrechungen durch plötzliche Systemausfälle. TeamViewer Remote Management bietet Ihnen die Tools, die Sie zur Automatisierung Ihrer IT benötigen.

Nahtlose Integration in die TeamViewer Plattform.

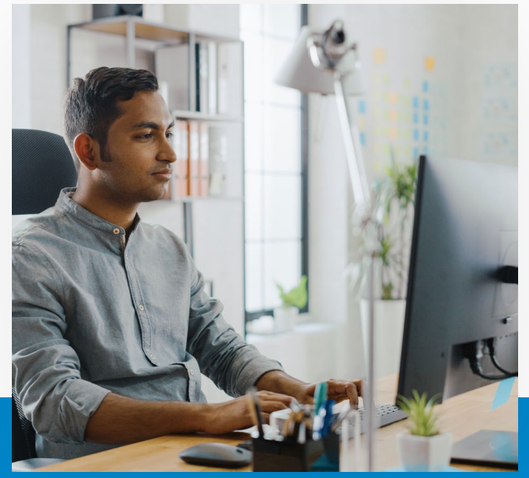
TeamViewer Remote Management ist vollständig in Ihre TeamViewer Management Console integriert und informiert Sie über vorhandene und potenzielle Risiken bezüglich Ihrer IT-Infrastruktur. Somit haben Sie die Möglichkeit, remote einzugreifen und Problemen vorzubeugen, bevor diese auftreten.

Monitoring und Schutz Ihrer IT über die TeamViewer Management Console.

Holen Sie sich die richtigen Tools für Ihr IT-Management

Device und Network Monitoring

Überwachen Sie kritische Aspekte Ihrer IT-Infrastruktur.



TeamViewer Monitoring erkennt Probleme mit Ihrer IT-Infrastruktur frühzeitig und warnt Sie umgehend.

Definieren Sie individuelle Überwachungsrichtlinien, nach denen Sie über den Festplattenzustand, die CPU-Auslastung, den Online-Status von Computern, die Tonerfüllstände von Druckern und vieles mehr informiert werden.

Handeln Sie proaktiv und vermeiden Sie mit TeamViewer Monitoring zeitaufwändige, kostspielige Systemausfälle und Datenverluste.

Schnellere Reaktionszeit

Definieren Sie zulässige Schwellwerte und lassen Sie sich benachrichtigen, wenn diese erreicht werden.

Deutlich weniger Ausfälle

Reduzieren Sie ungeplante Ausfallzeiten, indem Sie vorbeugende Wartungsarbeiten rechtzeitig ausführen.

Geringere Kosten

Durch die proaktive Wartung Ihrer Systeme können Sie die Häufigkeit teurer Ausfälle reduzieren und potenziellem Datenverlust vorbeugen.

Remote-Task-Manager

Verbessern Sie Ihren Support – bieten Sie Ihren Kunden ein schnelles und nahtloses Benutzererlebnis.

Mit dem integrierten Remote-Task-Manager können Sie alle laufenden Prozesse und Dienste auf Ihren Geräten über ein zentrales Dashboard anzeigen lassen und verwalten.

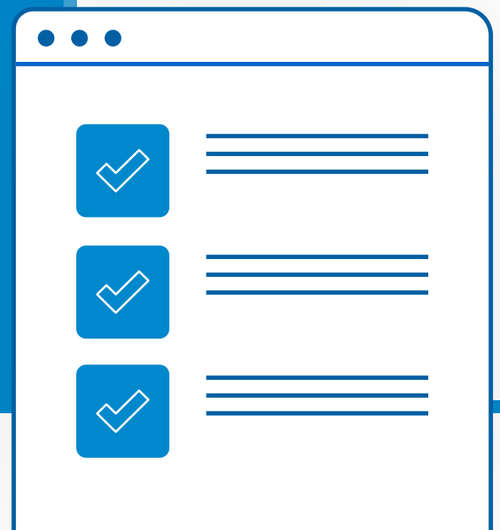
Ohne zuvor eine Remote-Verbindung zum jeweiligen Gerät aufbauen zu müssen, können Sie Prozesse und Dienste ferngesteuert starten und stoppen.

Remote Scripting

Automatisieren Sie komplexe Aufgaben auf Ihren Geräten.

Stellen Sie Skripte sofort oder geplant bereit.

Skripte können ausgeführt werden, wenn bestimmte Ereignisse erkannt oder Schwellwerte erreicht werden.



Probleme frühzeitig erkennen und sofort reagieren

TeamViewer Monitoring überwacht kritische Aspekte Ihrer Windows-, macOS-, Linux- und Netzwerkgeräte – wie Drucker und Router – sodass Sie bei Bedarf schnell und effizient handeln können.

Online-Status

Erhalten Sie regelbasierte Benachrichtigungen, wenn Geräte offline gehen.

CPU-Auslastung

Legen Sie einen Schwellwert fest, um Benachrichtigungen zu erhalten, wenn dieser für längere Zeit überschritten wird.

Systemupdate

Erhalten Sie Benachrichtigungen zu allen verfügbaren Updates und prüfen Sie, ob die Benutzer automatische Windows-Updates deaktiviert haben.

Prozesse

Erhalten Sie Benachrichtigungen, wenn vordefinierte Prozesse gestartet und/oder beendet werden.

Festplattenzustand

Erhalten Sie Benachrichtigungen, sobald eines Ihrer Geräte einen S.M.A.R.T.-Fehler meldet, sodass Sie schnell reagieren und Datenverlust vorbeugen können.

Festplattenspeicher

Erhalten Sie Benachrichtigungen, sobald der Speicherplatz auf Geräten einen festgelegten Grenzwert unterschreitet.

Windows-Dienste

Erhalten Sie Benachrichtigungen, wenn bestimmte Windows-Dienste beendet werden oder nach einer gewissen Anzahl von Versuchen.

Ereignisprotokolle

Lassen Sie sich benachrichtigen, wenn bestimmte Ereignisse in den Protokollen Ihrer Geräte erkannt werden.

Firewall

Eine deaktivierte Firewall stellt ein erhebliches Risiko für Ihre IT-Sicherheit dar. Wenn die Firewall deaktiviert ist, erhalten Sie sofort eine Benachrichtigung.

Status der Antivirensoftware

TeamVeiwer Monitoring informiert Sie, sobald die Antivirensoftware als inaktiv oder veraltet erkannt wird.

Datenverkehr

Legen Sie minimale und maximale Schwellenwerte für den am Netzwerkadapter eingehenden und ausgehenden Datenverkehr fest und erhalten Sie Benachrichtigungen, wenn er nicht innerhalb dieser Grenzen liegt.

Speichernutzung

Vermeiden Sie Probleme die aufgrund von zu hoher Speicherauslastung entstehen können.

Weitere Informationen über

Remote Device Monitoring

Network Monitoring

Asset Management

Behalten Sie den Überblick über die in Ihrer Organisation eingesetzte Hard- und Software.

TeamViewer Asset Management bietet den vollen Überblick über die eingesetzten Hardware- und Software-Assets in Ihrem Unternehmen.

Mit nur wenigen Klicks erhalten Sie wichtige Informationen zu Ihrem Inventar in einem zentralen Dashboard – mit nahtloser Integration in TeamViewer.

Inventar-Tracking

Von der Anzahl der verwendeten Tastaturen bis hin zur Übersicht der genauen Softwareversionen: Mit TeamViewer Asset Management verlieren Sie nie den Überblick über Ihr IT-Inventar.

Hardware

Erfassen Sie in Sekundenschnelle Ihre im Einsatz befindliche Hardware in einem detaillierten Inventarbericht.

- Typ
- Name
- Details
- Hersteller

Software

Überprüfen Sie, ob Benutzer unerwünschte Software installiert haben und ob Ihre Lizenzen die tatsächliche Software-Nutzung abdecken.

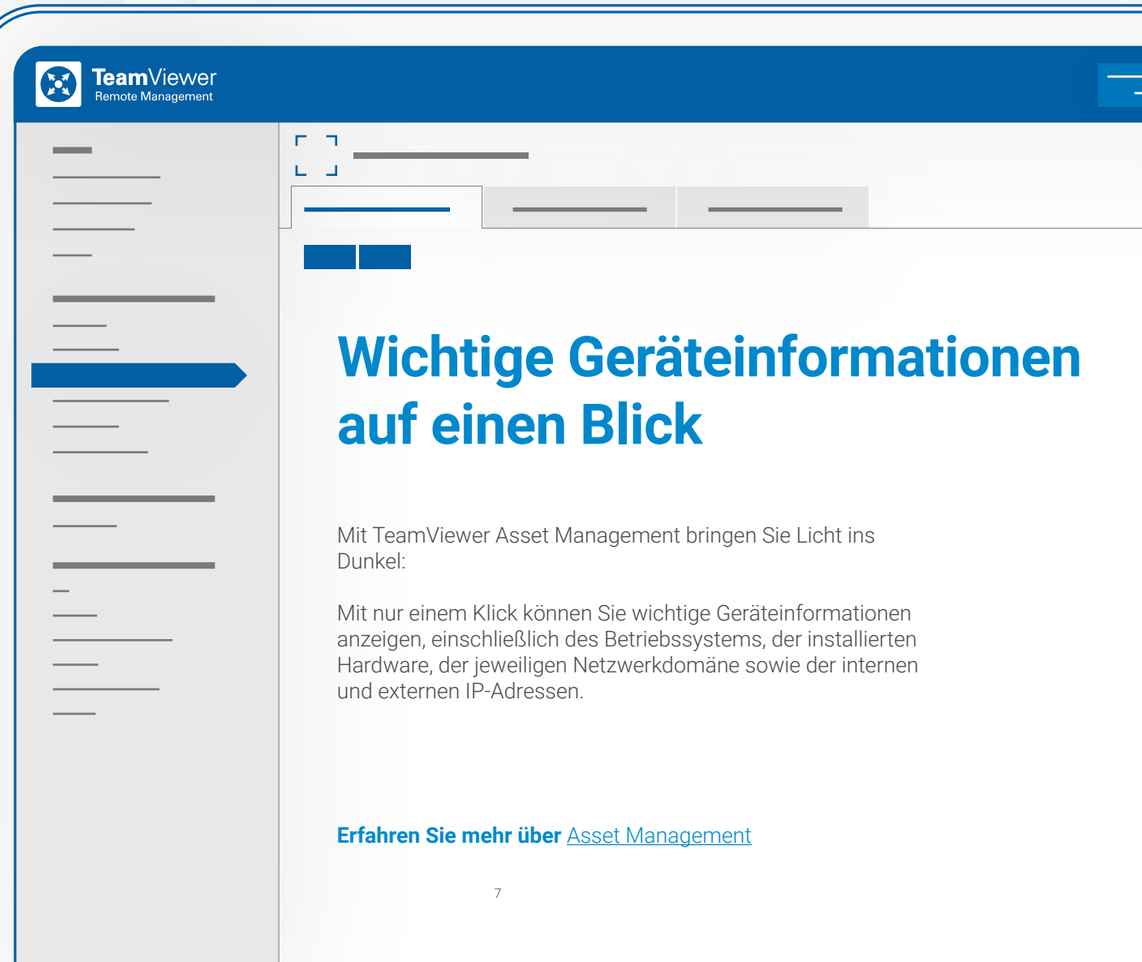
- Version
- Änderungsdatum

Erstellen Sie umfassende Berichte zu allen Konfigurationen Ihrer Geräte.

Inventarbericht

Mit TeamViewer Asset Management erstellen Sie umfassende Berichte zu Ihrer Hard- und Software. In Sekundenschnelle erhalten Sie einen vollständigen Inventarbericht oder eine individuelle Übersicht, die sich auf bestimmte Daten konzentriert.

Exportieren Sie die Informationen für andere Anwendungen in eine CSV-Datei.



Wichtige Geräteinformationen auf einen Blick

Mit TeamViewer Asset Management bringen Sie Licht ins Dunkel:

Mit nur einem Klick können Sie wichtige Geräteinformationen anzeigen, einschließlich des Betriebssystems, der installierten Hardware, der jeweiligen Netzwerkdomäne sowie der internen und externen IP-Adressen.

Erfahren Sie mehr über Asset Management

Patch Management

Schützen Sie Ihre Geräte mit aktuellen, automatischen Patches für Windows- und Drittanbieter-Software.

Viele Sicherheitsvorfälle lassen sich auf eine unzureichende Patch-Strategie zurückführen. Sparen Sie Zeit durch Automatisierung und halten Sie Ihre Betriebssysteme und Anwendungen auf dem neuesten Stand.

Ein nicht gepatchtes Gerät kann zur Gefahr für Ihre gesamte IT-Infrastruktur werden. Das Patch Management von TeamViewer Remote Management (in der Lizenz für TeamViewer Monitoring und Asset Management enthalten) erkennt automatisch potenzielle Schwachstellen in Betriebssystemen und Anwendungen von Drittanbietern. Patches werden automatisch aus der weltweit führenden Patch-Datenbank bereitgestellt.

Mehr Datensicherheit

Halten Sie Ihre Geräte auf dem neuesten Stand und geschützt, um das Risiko von Datenpannen aufgrund von Malware oder Ransomware zu verringern, die Unternehmen jedes Jahr Millionen Euro kosten.

Mehr Produktivität

Durch automatisiertes Patchen wird der laufende Betrieb nicht gestört und alles bleibt stets up to date.

Effizientere IT

Nutzen Sie Zeit, die Sie normalerweise für das manuelle Patchen aufwenden würden, für andere wichtige Projekte.

Erhöhte Compliance

Gewährleisten Sie den Schutz Ihrer Daten und die Einhaltung anderer Anforderungen.

Bedarfsgerechtes Patchen

Mit TeamViewer Patch Management patchen Sie alle Ihre Geräte flexibel und behalten stets den Durchblick.

Patchen von Windows

Stellen Sie Windows-Updates zentral bereit.

Benutzerfreundliches Dashboard

Erfahren Sie unmittelbar den Patch-Status jedes Geräts.

Patchen von Drittanbieter-Software

Patchen Sie anfällige Anwendungen mit Hilfe der Patch-Datenbank.

Automatisierung

Identifizieren notwendige Patches automatisch und planen Sie deren Bereitstellung.

Vollständige Integration

Stellen Sie Patches über die Ihnen bereits bekannte TeamViewer Management Console bereit.

Benutzerdefinierte Richtlinien

Definieren Sie individuelle Richtlinien entsprechend den Anforderungen Ihrer Benutzer.

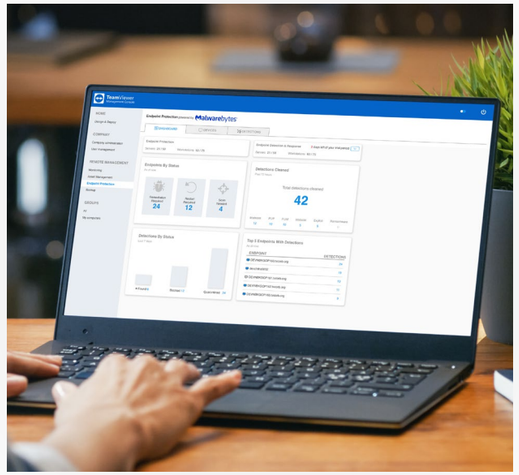
So einfach kann Patchen sein

1. Überprüfen Sie in einem zentralen Dashboard, welche Patches verfügbar sind, welche Priorität sie haben und von welchen Geräten sie benötigt werden.
2. Definieren Sie individuelle Richtlinien und legen Sie fest, dass Patches automatisch zu einem für Sie und Ihre Benutzer passenden Zeitpunkt bereitgestellt werden.
3. Dank der vollständigen Integration des Patch Managements in TeamViewer können Sie über Remote Access in Echtzeit auf Geräte zugreifen und diese warten.
4. Erledigen Sie all diese Aufgaben von einem beliebigen Ort aus.

Erfahren Sie mehr über Patch Management

Endpoint Protection

Erweiterte Cyberabwehr von Malwarebytes mit vollständiger TeamViewer Integration.



Viren, Trojaner, Ransomware oder Zero-Day-Exploits proaktiv erkennen und Bedrohungen ausschalten.

Endpoint Protection muss heutzutage ganzheitlich angegangen werden und agil genug sein, um auch fortschrittliche Angriffe zu stoppen. Eine ständige Anpassung an die sich rasant ändernde Bedrohungslage ist unverzichtbar.

Malwarebytes Endpoint Protection bietet Cloud-basierten Malware-Schutz und Malware-Beseitigung mit vorausschauender Erkennung von Bedrohungen. So bleiben Unternehmen jeder Größe stets geschützt, selbst vor Zero-Day-Exploits. Inklusive End-to-End-Schutz. Einfach zu skalieren und zu verwalten.

Proaktive Lösungen gegen Cyberbedrohungen

Schutz vor Zero-Day-Exploits

Verhindern Sie Zero-Day-Malware-Angriffe dank der zuverlässigen Erkennung von Anomalien.

In einem Durchgang

Beseitigen Sie die Infektion und alle Artefakte gründlich und dauerhaft – in einem Durchgang.

Proaktives verhaltensbasiertes Blockieren

Identifizieren Sie Bedrohungen durch verhaltensbasierte Analysen in nahezu Echtzeit und blockieren Sie diese automatisch.

Intelligente Erkennung von Cybergefahren

Verhaltensüberwachung und maschinelles Lernen sorgen für zuverlässige Erkennung von Cybergefahren mit weniger Fehlalarmen auf allen Ebenen: Web, Speicher, Anwendungen und Dateien.

Zentrales Scannen und Beseitigen

Automatisieren Sie das Scannen und Beseitigen von Malware: in einer einzelnen Abteilung oder auf Tausenden von Geräten gleichzeitig – alles zentral über die Management Console.

Intelligenter Schutz

Schnelle Einblicke

TeamViewer Endpoint Protection analysiert Cyberbedrohungen automatisch und bewertet potenzielle Auswirkungen. Dies spart CISOs Zeit und warnt das Management sofort vor möglichen Risiken. Probleme lassen sich so schnell korrigieren und deren Eskalation verhindern.

Leichte Skalierbarkeit

Unsere Cloud-basierte Lösung lässt sich mit der schnellen Remote-Bereitstellung über TeamViewer auf jede Unternehmensgröße skalieren und den individuellen Anforderungen der einzelnen Abteilungen anpassen. Damit erkennen Sie komplexe Bedrohungen effizient, konsistent und schnell.

Einfach und ohne Scripts

Bekämpfen Sie Malware mit wenigen Klicks. Automatisieren Sie Prozesse und nutzen Sie umfassende Funktionen ohne Scripts bemühen zu müssen.

Wie Sie Brute-Force-Angriffe stoppen

1

Mit einem automatisierten Tool führt ein Angreifer wiederholte Anmeldeversuche durch.

2

Malwarebytes Endpoint Detection and Response (EDR) erkennt Brute-Force-Angriffe als verdächtige Aktivitäten.

3

Die gefährdeten Endpunkte werden dann vom Rest des Netzwerks isoliert, um die potenzielle Verbreitung schädlicher Aktivitäten zu verhindern.

4

EDR untersucht und behebt das Problem, während Sie weiterhin über TeamViewer Remote Access auf das Gerät zugreifen können, ohne Ihr Netzwerk zu gefährden.

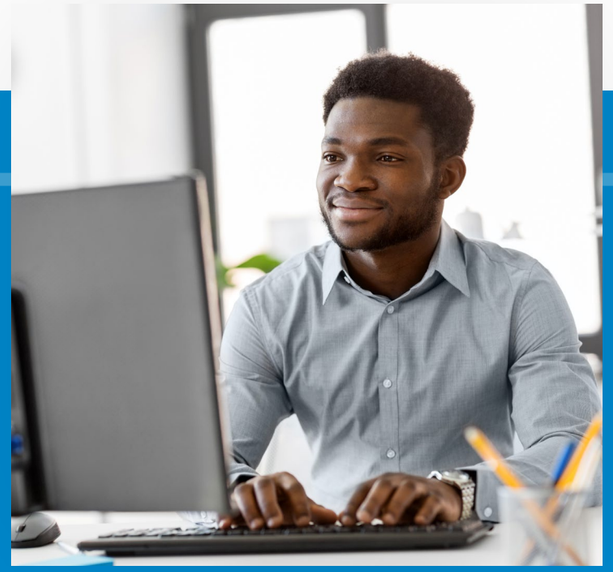
Erfahren Sie mehr über die Malwarebytes Endpoint Protection

Backup

Greifen Sie jederzeit und von überall auf Ihre gesicherten Daten zu.

TeamViewer Backup ist nahtlos in TeamViewer integriert und bietet zuverlässigen Schutz Ihrer Daten.

Nach der schnellen Remote-Bereitstellung werden Ihre bzw. die Daten Ihrer Kunden sicher in der Cloud gespeichert und sind jederzeit verfügbar.



Geräte-Backup

Sichern Sie automatisch auf Geräten gespeicherte Daten in der Cloud.

Die Cloud

Speichern Sie Ihre Daten sicher in der Cloud und haben Sie jederzeit Zugriff darauf.

Remote-Bereitstellung

Bringen Sie TeamViewer Backup in weniger als einer Minute mit nur wenigen Klicks zum Laufen.

Remote-Wiederherstellung

Stellen Sie Ihre Daten von überall aus und zu jeder Zeit auf Ihren lokalen oder verteilten Geräten wieder her.

Unbegrenzte Anzahl von Geräten

Ihr TeamViewer Backup-Speicher wird automatisch auf all Ihre Geräte aufgeteilt.

Skalierbarkeit

Kaufen Sie jederzeit Speicherplatz hinzu.

Individuelle Backup-Richtlinien

Egal, ob Sie ein einzelnes Gerät verwalten, ganze Abteilungen oder verschiedene Kunden: Erstellen Sie einen Backup-Plan, der genau auf die individuellen Erfordernisse zugeschnitten ist.

Dateiauswahl und Dateiausschluss

Bestimmen Sie, welche Dateien Sie in Ihre Backups einbinden wollen und welche nicht.

Backup-Zyklus und Zeitplan

Legen Sie fest, in welchem Zyklus oder zu welchen Zeiten Ihr Backup automatisch stattfinden soll.

Bandbreitenbegrenzung

Begrenzen Sie zeitweise die Durchsatzrate, mit der Daten an die Backup-Server gesendet werden.

Backup mit höchsten Sicherheitsstandards

Die Aufrechterhaltung höchster Sicherheitsstandards hat für uns oberste Priorität.

- Clientseitige, **AES-256-Verschlüsselung** vor der Datenübertragung
- SSL-verschlüsselte Datenübertragung
- Datenspeicherung auf **AES-256-verschlüsselten Amazon-AWS-S3-Servern**
- Standorte der Rechenzentren:
  - EMEA: Frankfurt, Paris, London, Dublin, Stockholm
  - AMERIKA: Virginia (US), Montreal (KANADA)
  - APAC: Sydney, Tokio, Mumbai, Seoul, Singapur
- **ISO/IEC-27001:2005-Zertifizierung** für Managementsysteme zur Informationssicherheit
- Redundante Datenspeicherung

Erfahren Sie mehr über TeamViewer Backup

Web Monitoring

Stellen Sie sicher, dass Ihre Website optimal läuft.

Eine reibungslos funktionierende Website ist für jedes Unternehmen heute Pflicht. Sie ist maßgebend für ein gutes Image und erster Anlaufpunkt für Ihre Kunden.

Websites müssen regelmäßig getestet werden, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Regelmäßige manuelle Tests können jedoch kostspielig und schwer umsetzbar sein. Mit TeamViewer Web Monitoring werden Verfügbarkeit und Geschwindigkeit Ihrer Website automatisch in benutzerdefinierten Intervallen an Standorten auf der ganzen Welt überprüft. Wenn Probleme auftreten, werden Sie benachrichtigt, damit diese behoben werden können, bevor es zu einem Ausfall kommt.

Umsatzeinbußen vermeiden

Bieten Sie jedem Besucher, Kunden und Interessenten das bestmögliche Website-Erlebnis.

Erkennen Sie Angriffe schneller

Erhalten Sie eine Benachrichtigung, wenn die Verfügbarkeit Ihrer Website aufgrund eines Angriffs gefährdet ist.

Verbessern der Leistung Ihrer Website

Erkennen Sie Engpässe und suboptimale Implementierungen.

In Suchergebnissen nach oben rücken

Vermeiden Sie Leistungseinbußen bei Websites und erhöhen Sie Ihr SEO-Ranking und Ihre Website-Präsenz auf Suchmaschinen-Ergebnisseiten (SERP).

Web Monitoring ganz einfach

Mit TeamViewer Web Monitoring halten Sie Ihre Website schnell und stabil, überall auf der Welt.

Uptime Monitoring

Es gibt verschiedene Gründe, warum Websites nicht verfügbar sind, z. B.:

- Serverüberlastung
- Hackerangriffe
- Probleme im Rechenzentrum
- Probleme mit der Website-Programmierung
- Probleme mit dem Internet-Service-Provider

Uptime Monitoring benachrichtigt Sie darüber, wann und wo Ihre Website nicht verfügbar ist, damit Sie sie so schnell wie möglich wieder zum Laufen bringen können.

Erfahren Sie mehr über Web Monitoring

Page Load Monitoring

40 Prozent der Verbraucher verlassen Websites, wenn das Laden länger als drei Sekunden dauert. Jede Sekunde zählt, um potenzielle Kunden nicht zu verlieren.

Mit Page Load Monitoring erhalten Sie Benachrichtigungen, wenn Ihre Website einen Ladezeitschwellenwert überschreitet, der kontinuierlich von über 30 Standorten weltweit überwacht wird.

Erkennen Sie die einzelnen Elemente und Engpässe, die Ihre Website verlangsamen.

Transaction Monitoring

Mithilfe der automatisierten Transaktionsüberwachung können Sie Umsatzverluste aufgrund fehlgeschlagener Webshop-Verkäufe, Kundenanmeldungen oder anderer Transaktionen vermeiden. Wie? Durch komplette Transparenz darüber:

1. Ob Transaktionen problemfrei abgewickelt werden
2. Wo Ausfälle oder Verzögerungen auftreten
3. Wie kosteneffizient die Leistung Ihrer Website ist
4. Ob Komponenten von Drittanbietern funktionieren

Wir **schützen Ihre Daten** zuverlässig

Der Schutz Ihrer Daten und Privatsphäre sind uns äußerst wichtig. Ende-zu-Ende-Verschlüsselung und Zwei-Faktor-Authentifizierung sind nur einige Maßnahmen, die wir dafür ergreifen. Doch wir tun noch mehr, um Ihre Arbeit mit TeamViewer so sicher wie möglich zu machen.

TeamViewer: **rundum sicher**

Die TeamViewer ID

Die TeamViewer ID ist eine einzigartige numerische ID, die jedem Gerät bei der Installation zugewiesen wird. Wie bei einer Telefonnummer wählen Sie die ID an und erfragen anschließend das Passwort, um den Verbindungsaufbau zu authentifizieren.

Das TeamViewer Passwort

Dieses sechsstellige, zufallsgenerierte Kennwort wird im Fernsteuerungs-Tab Ihrer TeamViewer Anwendung angezeigt und ist für spontane Supportsitzungen gedacht. Es wird nach jedem Start von TeamViewer neu generiert – oder öfter, je nach Einstellung.

Secure Remote Password Protocol (SRP)

Für die Autorisierung und Passwort-Verschlüsselung wird das Secure Remote Password Protocol (SRP) verwendet: Das Passwort wird nie direkt gesendet und ausschließlich auf dem lokalen Rechner gespeichert.

Verschlüsselung

TeamViewer Verbindungen laufen über gesicherte Datenkanäle, die mit einem RSA-4096-Public/Private-Key-Exchange aufgebaut und mit 256-Bit-AES verschlüsselt sind.

Conditional Access*

Steuern Sie die Nutzung und die Zugriffsrechte von TeamViewer in Ihrem gesamten Unternehmen über die Management Console.

Zertifizierte Sicherheit

Alle von TeamViewer verwendeten Rechenzentren sind nach ISO/IEC 27001 zertifiziert, der internationalen Norm für Informationssicherheitsmanagement. Mit der ISO 9001:2015 demonstriert TeamViewer zudem ein ganzheitliches Qualitätsmanagement.

Schutz vor Brute-Force-Attacken

Zur Abwehr von Brute-Force-Angriffen erhöht TeamViewer exponentiell die Wartezeit zwischen Verbindungsversuchen. Die Wartezeit wird erst nach der erfolgreichen Kennworteingabe zurückgesetzt.

Zwei-Faktor-Authentifizierung

Zusätzlich zu Ihrem Kennwort ist ein Sicherheitscode erforderlich, um sich an Ihrem TeamViewer Konto anzumelden. Der Code wird von einer App generiert.

*Verfügbar mit TeamViewer Tensor. Gemäß den allgemeinen Geschäftsbedingungen.

Protokolle und Datensicherheit

So kommen TeamViewer Verbindungen zustande

TeamViewer wählt die optimale Art der Verbindung: Nach dem Handshake über unsere Masterserver findet in 70 % der Fälle eine Direktverbindung über das User Datagram Protocol (UDP) oder das Transmission Control Protocol (TCP) statt, selbst hinter Standardgateways, Network-Address-Translation-Routern (NAT) und Firewalls. Die restlichen Verbindungen werden über unser hochredundantes Router-Netzwerk via TCP- oder HTTP-Tunneling geleitet. Sie müssen keinerlei Ports öffnen.

Verschlüsselung und Authentifizierung

TeamViewer Verbindungen laufen über gesicherte Datenkanäle: RSA-4096-Public/Private-Key-Exchange und 256-Bit-AES-Verschlüsselung. Diese Technik wird in vergleichbarer Form auch bei HTTPS/SSL eingesetzt. Da der Private Key niemals den Client verlässt, ist durch dieses Verfahren technisch sichergestellt, dass zwischengeschaltete Computer im Internet Daten nicht dechiffrieren können. Das gilt auch für unsere eigenen Router: Nicht einmal TeamViewer als Betreiber des zentralen Rechenzentrums kann den Datenverkehr lesen.

Datenschutz und Compliance

Vertrauenswürdige Geräte (Trusted Devices)

Die Funktion „Vertrauenswürdige Geräte" bietet zusätzlichen Schutz für Ihr TeamViewer Konto: Sie müssen Geräte, von denen Sie sich zu erstem Mal einloggen, bei der Anmeldung autorisieren und werden per E-Mail benachrichtigt.

Integritätsprüfung (Data Integrity)

Wir prüfen automatisch, ob Ihr TeamViewer Konto ungewöhnliches Verhalten zeigt: zum Beispiel Zugriff von einem verdächtigen Standort aus, was darauf hindeuten könnte, dass das Konto kompromittiert wurde. In diesem Fall erhalten Sie von uns eine E-Mail zur Erstellung eines neuen Passworts.

Allow- und Blocklist

Falls Sie bestimmte Kontakte daran hindern möchten, eine Verbindung zu Ihrem Computer aufzubauen, empfiehlt sich das Einrichten einer Blocklist. Richten Sie eine Allowlist ein, um ausschließlich bestimmten Konten oder IDs Zugriff zu erlauben.

ISO/IEC 27001

Alle von TeamViewer genutzten Rechenzentren sind zertifiziert nach ISO/IEC 27001, der internationalen Norm für Informationssicherheits-Managementsysteme und Sicherheitsverfahren.

ISO 9001:2015

Mit der Zertifizierung nach ISO 9001:2015 demonstriert TeamViewer ein ganzheitliches Qualitätsmanagement, absolute Kundenorientierung und kontinuierliche Verbesserung.

Datenschutzgrundverordnung (DSGVO)

TeamViewer ist ein weltweit agierendes Unternehmen, für das der Schutz personenbezogener Daten von Kunden und Mitarbeitern höchste Priorität hat. Weitere Informationen zum Datenschutz und zur DSGVO finden Sie auf der Seite „TeamViewer und die DSGVO" in unserer Trust Center.

HIPAA-, HITECH- und SOC2-zertifiziert

TeamViewer besitzt die HIPAA-, HITECH- und SOC2-Zertifizierung von A-LIGN, einem US-amerikanischen Sicherheits- und Compliance-Anbieter. Während HIPAA und HITECH für Organisationen des Gesundheitswesens von entscheidender Bedeutung sind, um die Vertraulichkeit und Sicherheit sensibler Daten und geschützter Gesundheitsinformationen (PHI) zu gewährleisten, ist SOC2 ein wesentlicher Berichtsrahmen für Dienstleisterorganisationen, um eine Methode zur Berichterstattung über nicht finanzielle interne Kontrollen einzurichten, damit deren Kunden ein besseres Verständnis für die Durchsetzung der fünf Trusted Service Principles (TSP) erhalten.

TeamViewer
Remote Management

Noch Fragen?

Weitere Informationen erhalten Sie unter **+49 7161 60692 50**
oder im Internet unter teamviewer.com/support.

TeamViewer Germany GmbH
Bahnhofsplatz 2
73033 Göppingen
Deutschland

Über TeamViewer

Als globales Technologieunternehmen und führender Anbieter einer Konnektivitätsplattform ermöglicht es TeamViewer, aus der Ferne auf Geräte aller Art zuzugreifen, sie zu steuern, zu verwalten, zu überwachen und zu reparieren. Ergänzend zur hohen Zahl an Privatnutzern, für die die Software kostenlos angeboten wird, hat TeamViewer mehr als 600.000 zahlende Kunden und unterstützt Unternehmen jeglicher Größe und aus allen Branchen dabei, geschäftskritische Prozesse durch die nahtlose Vernetzung von Geräten zu digitalisieren: zum Beispiel in den Bereichen Remote Connectivity, Augmented Reality, Internet of Things und Digital Customer Engagement. Seit der Gründung im Jahr 2005 wurde die Software von TeamViewer global auf mehr als 2,5 Milliarden Geräten installiert. Das Unternehmen hat seinen Hauptsitz in Göppingen, Deutschland, und beschäftigt weltweit mehr als 1.400 Mitarbeiter. Die TeamViewer AG (TMV) ist als MDAX-Unternehmen an der Frankfurter Börse notiert.

Wir sind nur einen Klick entfernt

www.teamviewer.com

Copyright © 2021 TeamViewer Germany GmbH. Alle Rechte vorbehalten.

TVRM-B-DE-EMEA-072021-1