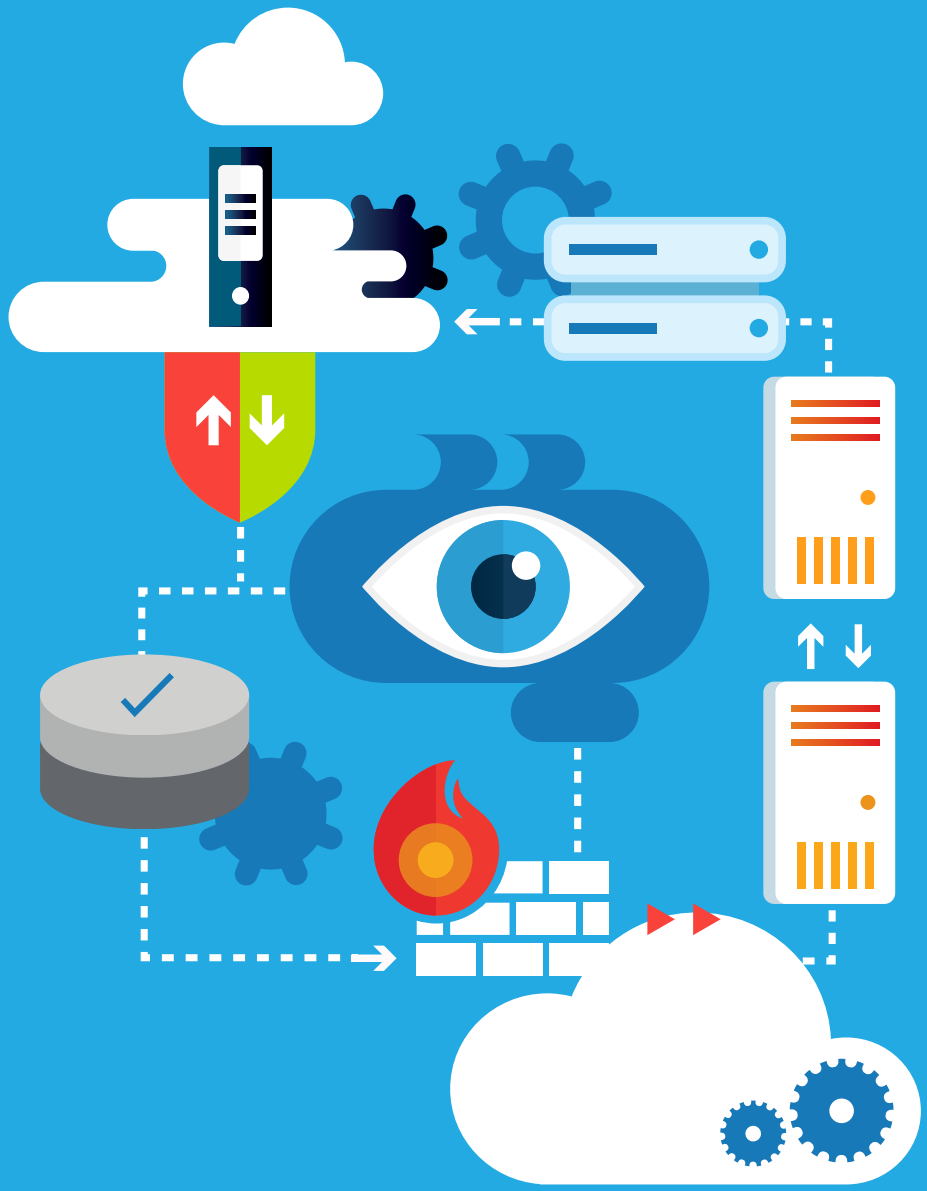
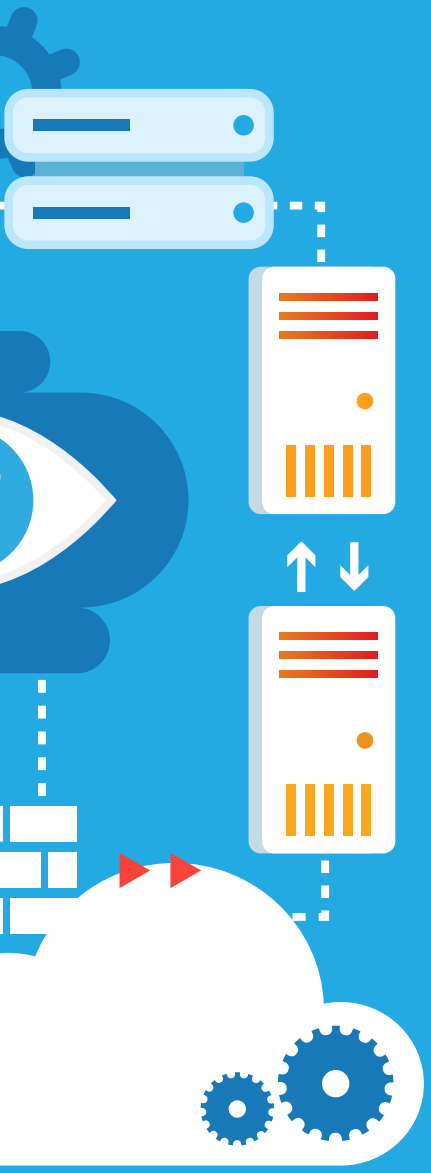
CITRIX®

Entwickeln Sie eine Strategie für die Netzwerk- und Anwendungssicherheit

So schützen Sie Ihre gesamte digitale Umgebung.





Inhalte

Raffinierte Schadsoftware wie WannaCry und NetPetya hat in der letzten Zeit in den Nachrichten für viel Wirbel gesorgt – und das aus gutem Grund. Cyberangriffe haben sich weiterentwickelt, sind hartnäckig und werden immer häufiger.

Angriffe auf Anwendungen sind jedoch nicht die einzigen Bedrohungen, auf die Sie achten sollten.
Bedrohungen jeder Art können sich schnell verbreiten. Vom Netzwerk bis zu den Anwendungen schaden diese Angriffe Organisationen auf jeder Ebene ihrer Infrastruktur. In der Vergangenheit reichte es, ein neues Produkt ans Netzwerk anzuschließen, das das Problem löst. Dieser Ansatz hinterlässt jedoch Sicherheitslücken. Nur eine umfassende End-to-End-Lösung kann Ihre Daten vollständig schützen – unabhängig davon, wo diese gespeichert werden.

Das richtige Maß zwischen Sicherheit und Benutzerfreundlichkeit

Benutzer möchten selbst entscheiden können, welche Anwendungen und Endgeräte sie verwenden. Sie möchten zudem von überall und zu jeder Zeit arbeiten können. Dies führt jedoch zu übermäßiger Komplexität, Sicherheitsrisiken und einem überbordenden System, das für die IT schwierig zu managen ist. Mit der richtigen Lösung müssen Organisationen keiner der beiden Seiten Vorrang geben – sie können sowohl die Anforderungen von Benutzern als auch die der IT erfüllen.

Egal wo sich Ihre Daten befinden, Ihre Organisation kann Mitarbeitern ihre bevorzugten Tools bereitstellen. Gleichzeitig verfügt die IT über die notwendige Visibilität und Kontrolle, um Ihr gesamtes Ökosystem über eine zentrale Konsole zu überwachen.

← Seite 3 | Seite 5 →

Zurück zum Inhaltsverzeichnis

Bedrohungen passen sich Sicherheitsmaßnahmen an und überlisten sie

Cyberangriffe entwickeln sich stetig weiter, um Sicherheitsmaßnahmen zu umgehen.
Sie sind nun in der Lage, in jeden Winkel Ihrer IT-Infrastruktur zu gelangen.
Hier ist ein Überblick darüber, wie sich Angriffe verändern.

Häufige Arten von Angriffen auf das Netzwerk:
In der Vergangenheit waren Netzwerke das Hauptziel von Angriffen. Zu den besten Schutzmaßnahmen gehörten Firewalls, Patches und gut geschulte Mitarbeiter. Dies waren zwar keine großartigen Optionen, aber solange sich die Daten hinter der Firewall befanden, konnten Organisationen üblicherweise die Kontrolle behalten. Dies ging jedoch nur solange gut, bis Angreifer höhere Protokollebenen ins Visier nahmen und Ziele außerhalb des Rechenzentrums angriffen.

Angriffe auf das Netzwerk

- Brute-Force-Angriffe
- Würmer
- DNS
- Port-Scans
- Andere

Häufige Arten von Angriffen auf Anwendungen:
Da sich Daten immer häufiger außerhalb des Rechenzentrums befinden – in Clouds, Online-Ressourcen, auf Endgeräten und in Anwendungen –, wird es immer schwieriger, sie abzusichern. Fortschrittliche Schadsoftware fing an, Daten in höheren Protokollschichten zu folgen und sich außerhalb der Reichweite von Firewalls zu verbreiten – in Cloud-, Internet- und Anwendungsebenen.

Angriffe auf Online-Ressourcen und Anwendungen

- Browser
- URL-Manipulationsangriffe
- SQL Injection
- Angreifer, die sich als andere Personen ausgeben
- Pufferüberlaufangriffe
- DDoS (Distributed Denial of Service)

← Seite 4 | Seite 6 →

Zurück zum Inhaltsverzeichnis

Traditionelle Maßnahmen reichen nicht länger aus

Um der neuen Bedrohungen Herr zu werden, haben viele Organisationen für jedes Sicherheitsproblem eine spezielle Lösung implementiert: eine für den Schutz von Endgeräten, eine weitere für Anwendungen und noch eine für das Netzwerk. Diese dezentralen Systeme funktionieren jedoch nicht, da sie:

- **die Komplexität steigern.** Wenn Daten vom Rechenzentrum in die Cloud migriert oder gar auf Endgeräten, also außerhalb der Firewall, gespeichert werden, müssen IT-Teams verschiedene Systeme verwenden, um sie alle zu managen und abzusichern.

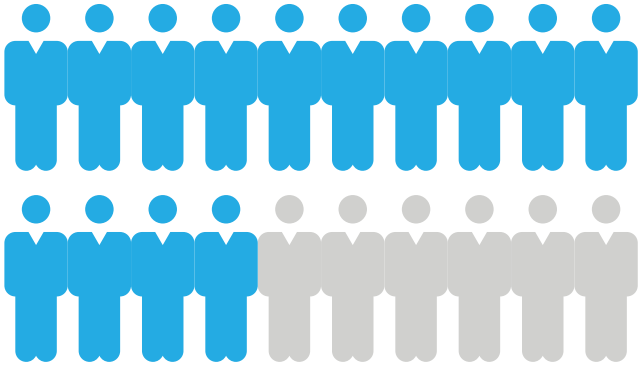
- **Sicherheitslücken hinterlassen.** Die verschiedenen Systeme wurden nicht für einen durchgängigen Schutz entwickelt und hinterlassen Sicherheitslücken, durch die Malware hindurchschlüpfen kann.

- **nicht miteinander kommunizieren.** Isolierte Einzellösungen können keine Anomalien oder Modifikationen erkennen und deshalb nicht proaktiv verhindern, dass Bedrohungen in das Netzwerk eindringen.

- **unbekannte Angriffe nicht identifizieren können:** Ein großes Problem für die vielen dezentralen Sicherheitssysteme sind Bedrohungen, die sie nicht sehen können, auch bekannt als Zero-Day-Angriffe. Diese können über einen längeren Zeitraum hinweg unerkannt bleiben, sodass Hacker viel Zeit haben, um Zugriff auf vertrauliche Daten zu erhalten.

- **interne Bedrohungen nicht bekämpfen.** Die meisten Sicherheitslösungen sind darauf ausgelegt, Angriffe von außen zu bekämpfen. Sie gehen jedoch nicht auf undichte Stellen im Inneren ein. Einzellösungen wurden nicht entwickelt, um ungewöhnliches Verhalten zu erkennen und notwendige Maßnahmen einzuleiten. Folglich können sie nicht verhindern, dass vertrauliche Informationen das Netzwerk verlassen.

- **den Zugriff nicht anhand der Anforderungen von Nutzern aufteilen können:** Das Verhalten von Anwendern auf verschiedenen Endgeräten (besonders BYOD-Geräten) zu managen, ist viel schwieriger, wenn Sie über verschiedene Einzellösungen verfügen. Dadurch werden Ihre häufig schon überlasteten IT-Teams nur noch weiter belastet.



↑ Über 70 %

aller Manager gaben an, dass die große Menge an BYOD-Geräten und Anwendungen, die Mitarbeiter ins Unternehmen bringen, die Hauptursache für Cyberangriffe ist.[1]

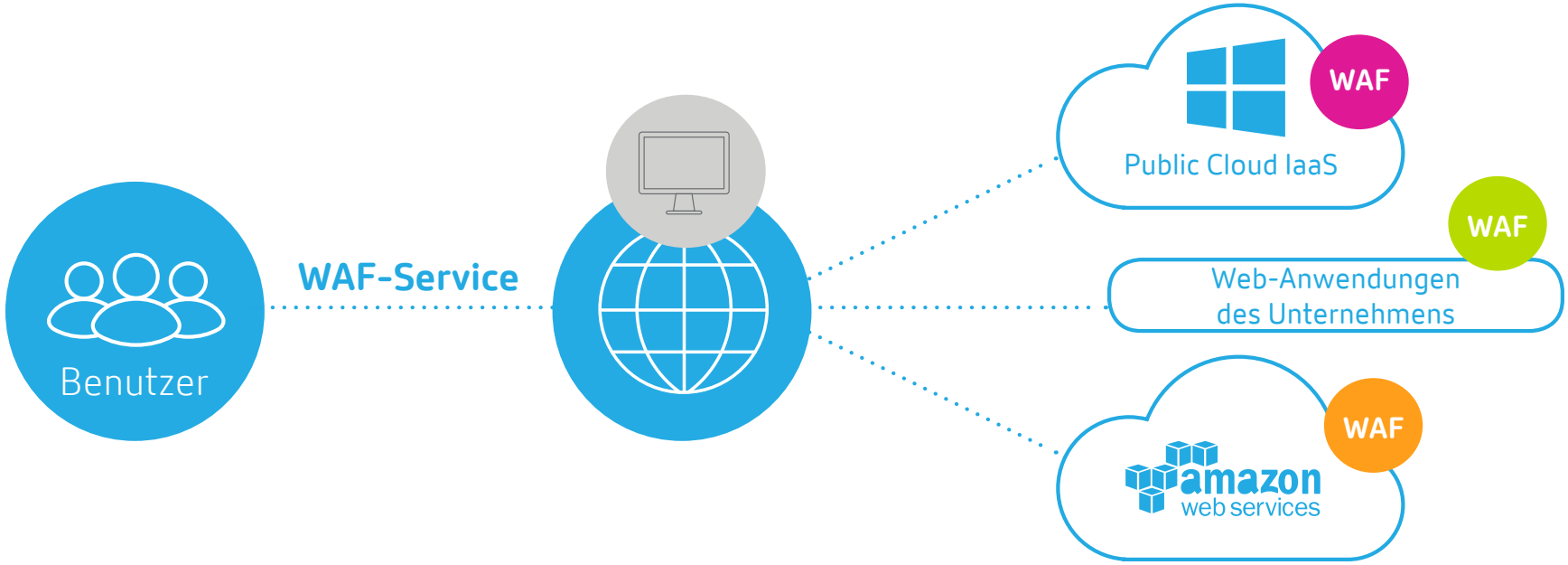
← Seite 5 | Seite 7 →

Zurück zum Inhaltsverzeichnis

Warum ein neuer Sicherheitsansatz unerlässlich ist

Durch die Verbreitung von Cloud-Services ist es nicht unwahrscheinlich, dass Ihre Organisation neuen Bedrohungsarten gegenübersteht. Und Sie benötigen eine Plattform, die Ihre Daten überall absichern kann – egal, ob sie sich im Netzwerk, im Internet oder in der Anwendungsebene befinden.

Mithilfe eines durchgängigen Ansatzes, der eine vollständig integrierte Web Application Firewall (WAF) bietet, können Sie Bedrohungen über alle Clouds, Netzwerke, Endgeräte und Anwender hinweg managen. Zudem wird in jeder Umgebung ein einheitlicher Benutzerkomfort für Anwender und IT-Teams gewährleistet.



← Seite 6 | Seite 8 →

Zurück zum Inhaltsverzeichnis

74 %

der Unternehmen stimmen zu, dass ein neues IT-Sicherheits-Framework notwendig ist, um das Sicherheitsniveau zu verbessern und das Risiko zu senken.[1]

← Seite 7 | Seite 9 →

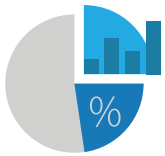
Zurück zum Inhaltsverzeichnis

Ein idealer Sicherheitsansatz ist ganzheitlich

Mit einer konsolidierten, kontextorientierten und sicheren Methode stellen Sie verfügbare und zuverlässige Systeme zur Verfügung und sorgen gleichzeitig dafür, dass Daten durch folgende Maßnahmen umfassend geschützt sind:

Vollständige Visibilität

Sie benötigen einen vollständigen Einblick in den Datenverkehr und die Transaktionen innerhalb Ihrer Umgebung, um Bedrohungen und ungewöhnliche Aktivitäten erkennen zu können. Dazu gehören beispielsweise eine Anmeldung zu einer für diesen Nutzer unüblichen Zeit und an einem unüblichen Standort.



Verwertbare Informationen aus Analysen

Mithilfe fortschrittlicher Telemetriefunktionen können Sie Daten aus jeder Quelle sammeln (Endgeräte-, Server- und Anwendungsprotokolle, Zählerdaten, E-Mails, SIEM-Produkte von Drittanbietern usw.). Sie können anschließend Anomalien innerhalb Ihres Netzwerks, Ihrer Clouds, Anwendungen, Web-Traffic sowie von Anwendern überwachen, analysieren und identifizieren. Dadurch kann die IT Probleme proaktiv bekämpfen, bevor Ihr System infiziert wird.

Vereinfachter Zugriff

Ganz gleich, ob ein BYOD-Gerät, ein dedizierter Desktop oder ein gemeinsam genutztes Endgerät verwendet werden, SSO (Single Sign-On) vereinfacht den Zugriff für Anwender. Gleichzeitig verringert sich der Aufwand für IT-Teams, da diese sich weniger um Passwortprobleme von Mitarbeitern oder abgelaufene Zugriffsprivilegien kümmern müssen.

Management, Aktualisierung, Konfiguration und Durchsetzung von Richtlinien

Stellen Sie sicher, dass Ihre Organisation das Zugriffsniveau granular konfigurieren kann, sodass nur autorisierte Personen vertrauliche Daten einsehen können.

Globale Installation von Updates und Patches

Patches und Updates auf den zahlreichen verwendeten Endgeräten zu installieren ist nahezu unmöglich. Das Management von Systemen über eine zentrale Konsole bedeutet, dass Teams Patches und Updates innerhalb von Minuten statt Stunden installieren können.

Schutz vor gezielten Angriffen auf die Anwendungsebene

Implementieren Sie Regeln zum Schutz der Web Application Firewall (WAF) von Servern, um häufige Angriffsarten wie Cross-Site Scripting (XSS) und SQL Injections zu unterbinden.

End-to-End-Verschlüsselung

Verwalten Sie Datenverkehr und Zertifikate, um das Rechenzentrum abzuhärten und innerhalb von Hybrid- und Multi-Cloud-Umgebungen zu schützen.

← Seite 8 | Seite 10 →

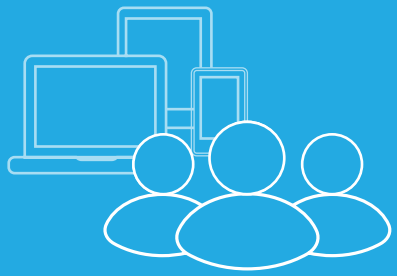
Zurück zum Inhaltsverzeichnis

Umfassender Schutz mit einem sicheren digitalen Arbeitsplatz

Konsolidiert

Die IT kann Ihre gesamte IT-Infrastruktur mithilfe einer zentralen Oberfläche konfigurieren, überwachen und verwalten, um so für einheitlichen Benutzerkomfort sorgen.

Sicher



Bei der anwenderorientierten Sicherheit steht der Anwender im Mittelpunkt. Alle Informationen zum Anwender und seinen Verhaltensweisen werden für kontextbasierten Zugriff, Sicherheitskontrollen und vorausschauende Analysen gebündelt und für vollständige Visibilität im Netzwerk und in der Anwenderumgebung genutzt.

Kontextorientiert

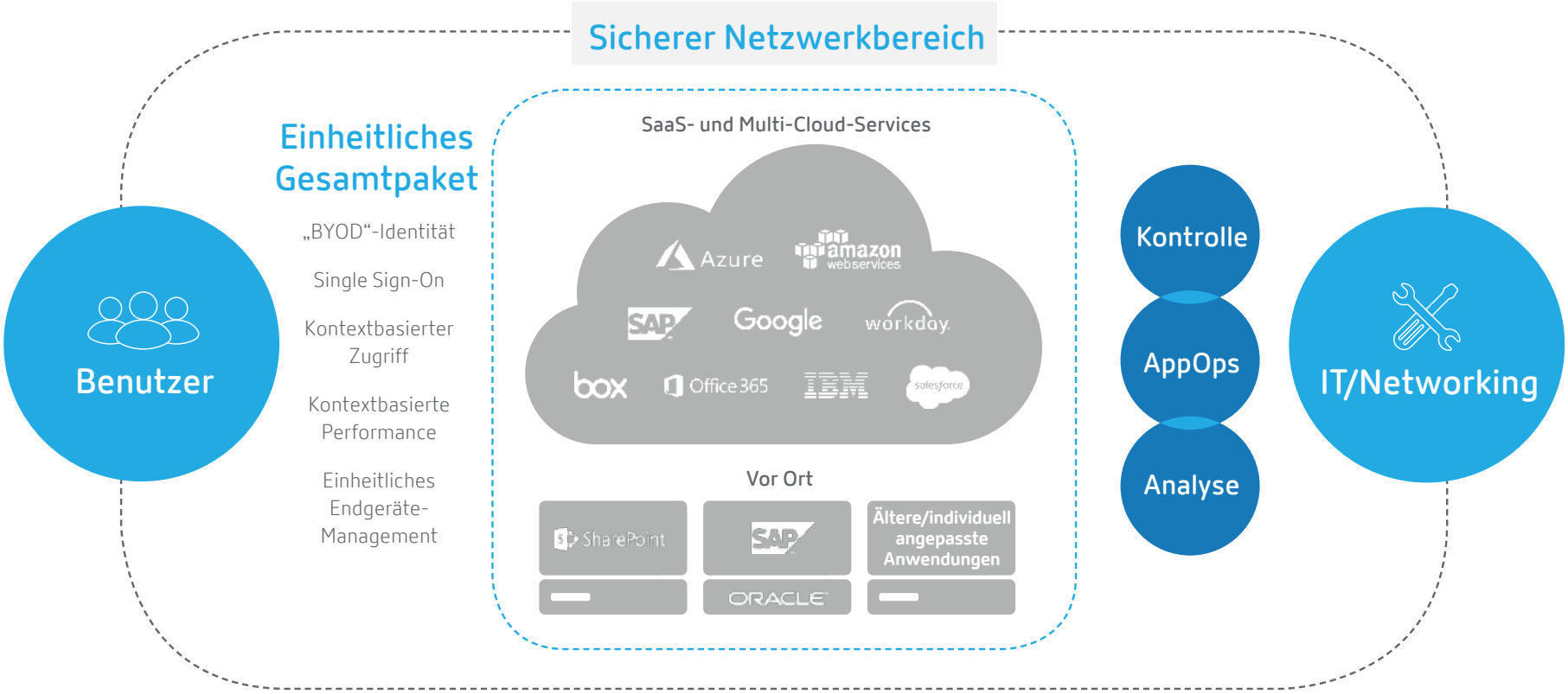
Digitale Arbeitsplätze nutzen maschinelles Lernen, um sich an die Arbeitsstile jedes einzelnen Mitarbeiters und an entsprechende Abweichungen anzupassen, damit Mitarbeiter ihre Aufgaben sicher und von überall aus erledigen können.

← Seite 9 | Seite 11 →

Zurück zum Inhaltsverzeichnis

Bereitstellung der passenden Erfahrung für jeden Benutzer zur richtigen Zeit

Es ist umständlich, ein immer komplexer werdendes Netzwerk sowie zahlreiche Anwendungen auf verschiedenen Clouds managen müssen. Außerdem erhöht dies das Sicherheitsrisiko. Mit Citrix Workspace kann die IT die Kontrolle übernehmen und Sicherheitsbedrohungen in den dezentralen Hybrid- und Multi-Cloud-Umgebungen von heute proaktiv managen. Verschiedene Einzellösungen, die sich nicht ineinander integrieren lassen, ermöglichen keinen durchgängigen Schutz. Citrix ist der einzige Anbieter, der Ihnen einen umfassenden Schutz für Anwendungen und Netzwerke auf mehreren Ebenen bietet. Diese Lösung lässt sich in Citrix Analytics integrieren, das ihnen ein zentrales Dashboard zur Verfügung stellt, über das Sie Sicherheitsrisiken überwachen, managen und beheben können.



← Seite 10 | Seite 12 →

Zurück zum Inhaltsverzeichnis

Zusätzliche geschäftliche Vorteile unseres Sicherheitsansatzes

Sichere Zusammenarbeit für den Schutz von geistigem Eigentum:
Die Lösung von Citrix wurde von Grund auf neu entwickelt, um Unternehmen in höchstem Maße zu schützen. Anwender können Dokumente einfach, sicher und professionell miteinander teilen und gemeinsam daran arbeiten. Alle Metadaten und Inhalte sind hierbei durch das in der Branche übliche AES-256-Verschlüsselungsverfahren geschützt.

Governance, Risiko und Compliance (GRC):
Indem wir GRC in unserem Sicherheitsansatz berücksichtigen und diese Faktoren durch umfassende Analysefunktionen unterstützen, sind wir in der Lage, unseren Ansatz weitaus stärker zu synchronisieren, um alle Ihre Anforderungen an Sicherheit und Compliance zu erfüllen.

← Seite 11 | Seite 13 →

Zurück zum Inhaltsverzeichnis

> Unser Management wollte ein flexibles und effizientes Arbeiten ermöglichen, aber wir mussten sicherstellen, dass die Lösung zuverlässig ist. Mit Citrix Workspace waren wir optimal abgesichert, was für ein Unternehmen wie Stater besonders wichtig ist, da wir mit äußerst vertraulichen Finanzdaten arbeiten.
>
> – Frank Veldink, ICT Infrastructure Architect bei Stater

← Seite 12 | Seite 14 →

Zurück zum Inhaltsverzeichnis

Erfahren Sie auf **citrix.de/secure**, wie ein integrierter, intelligenter Sicherheitsansatz Ihnen dabei helfen kann, den Zugriff, die Kontrolle und die Sicherheit, die Sie benötigen, zu erhalten.

Quellen:
*„The Need for a New IT Security Architecture“, Ponemon Institute, gesponsert von Citrix, 2017

Zurück zum Inhaltsverzeichnis