Lookout®

WHITEPAPER

# Absicherung Ihrer Daten über die Netzwerkgrenzen hinaus

# WAS BEDEUTET SICHERHEIT ÜBER DIE NETZWERKGRENZEN HINAUS?

In unserer heutigen, vor allem auf Mobilgeräte und die Cloud ausgerichteten Welt müssen Unternehmen drei wichtige Fakten beim Schutz ihrer Ressourcen vor Datenverlust und Angriffen berücksichtigen:

1. Die Netzwerkgrenzen verschwimmen.
2. Die traditionelle Sicherheitsmaßnahmen reichen nicht aus.
3. Geräte sind nicht automatisch vertrauenswürdig.

Da immer mehr Mitarbeiter eine Mischung aus verwalteten und nicht verwalteten Geräten für den Zugriff auf Unternehmensressourcen verwenden, ist eine neue Sicherheitsarchitektur erforderlich:
**„Post-Perimeter Security", also Sicherheit über die Netzwerkgrenzen hinaus.**

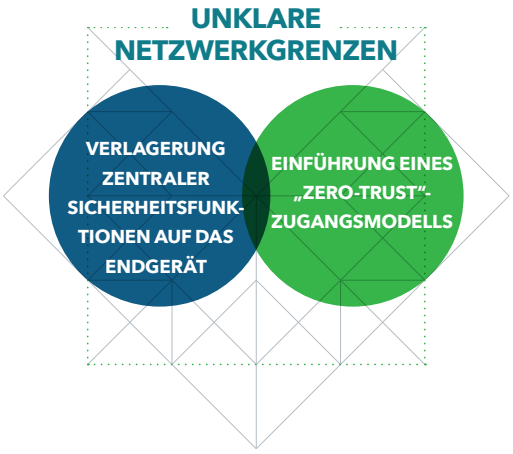
## DAS PROBLEM: Die Netzwerkgrenzen verschwimmen

Die Arbeitsweise vieler Menschen hat sich mittlerweile grundlegend verändert. Kritische Daten werden in die Cloud verlagert und Mitarbeiter können über jedes beliebige Netzwerk darauf zugreifen, egal, wo sie sich gerade befinden. Und so müssen sie sich oft nicht einmal über ein VPN anmelden, um unterwegs ihre geschäftlichen E-Mails abzurufen oder vertrauliche Dokumente zu öffnen bzw. herunterzuladen.

Der bisherige Perimeterschutz, der keinen Einblick mehr in den Datenverkehr der Anwender ermöglicht, lädt außerdem zu Phishing-Attacken und anderen Angriffsformen ein. Hinzu kommt, dass Unternehmensgeräte mittlerweile auch privat genutzt werden. Social-Media- und Messenger-Apps schaffen eine Umgebung, die es Angreifern leicht macht, Mitarbeiter mit Phishing in die Falle zu locken und geschäftliche Zugangsdaten über persönliche Interaktionen auszuspähen.

Mobilität und der nahtlose Datenzugriff sind starke Produktivitätsmotoren für Unternehmen, stellen jedoch auch eine große Herausforderung für Unternehmens-IT dar, die das Netzwerk bisher mit Firewalls und sicheren Web-Gateways schützen.

Tatsächlich aber befinden sich Unternehmensdaten längst nicht mehr nur innerhalb des geschützten Netzwerkbereichs. Vielmehr bewegen sie sich fließend über diese Grenzen hinweg und sind damit besser zugänglich. Angesichts dieses Wandels kommen zwei neue Sicherheitsanforderungen auf:



### Verlagerung zentraler Sicherheitsfunktionen auf das Endgerät

Zunächst einmal gilt es, die eigentlichen Sicherheitsmaßnahmen auf das Endgerät zu verlagern, anstatt die Endgeräte hinter den traditionellen Perimeterschutz zu bringen oder darauf zu vertrauen, dass VPN-Verbindungen den Datenverkehr auf den geschützten Bereich innerhalb des Netzwerks begrenzen. Sie müssen sich überall dort absichern, wo auf Ihre Daten zugegriffen wird – jedoch ohne die Privatsphäre der Anwender zu verletzen.

### Einführung eines „Zero-Trust"-Zugangsmodells

Selbst mit Sicherheitsmechanismen auf dem Endgerät darf ein Unternehmen das Gerät nie automatisch als vertrauenswürdig einstufen, sondern muss es erst prüfen. In dieser neuen Welt ist es unerlässlich, die Integrität aller Geräte kontinuierlich zu prüfen, bevor ihnen Zugang zu Unternehmensdaten gewährt wird – auch hier wieder ohne die Privatsphäre der Anwender zu verletzen.

## DIE NEUE SICHERHEITSARCHITEKTUR: Sicherheit über die Netzwerkgrenzen hinaus

In der Praxis bedeutet das, dass eine neue Sicherheitsarchitektur eingeführt werden muss; ein Konzept, das wir als „Post-Perimeter Security" (Sicherheit über die Netzwerkgrenzen hinaus) bezeichnen.[1] Es besteht im Grunde aus drei miteinander verbundenen Kernkomponenten:

- Endgeräteschutz
- Zugriff auf Cloud-Dienste
- Identitäts- und Zugriffsmanagement

Die Analyse des Geräterisikos mithilfe einer Sicherheitslösung zum Schutz der Endgeräte ein entscheidender Aspekt der Sicherheitsarchitektur in einer Welt verschwimmender Netzwerkgrenzen. Dieser Schutz bietet Visibilität im Bezug auf Bedrohungen oder Risiken auf dem Gerät selbst. Nur so lässt sich feststellen, ob das Gerät eines Mitarbeiters sicher genug ist, um auf Unternehmensressourcen zugreiffen zu dürfen. Durch diesen Schutzmechanismus können Richtlinien auf Basis der spezifischen Risikotoleranz eines Unternehmens durchgesetzt werden – in Echtzeit.

Ein weiterer Aspekt dieser Architektur ist die Absicherung des Zugriffs auf die Unternehmens-Cloud als auch auf das Internet ohne sich auf den üblichen Netzwerkschutz zu verlassen. Hierfür müssen einige dieser zentralen Sicherheitsfunktionen auf das Endgerät verlagert werden, darunter die Überwachung von manipulierten Links und Webseiten. Damit einhergehend muss auch verhindert werden, dass Mitarbeiter gefährliche Inhalte öffnen.

Diese beiden Aspekte gehen Hand in Hand mit einer Identitätslösung –z. B. von einem „Single-Sign-on"–Anbieter, der Mitarbeitern entweder erlaubt, sich anzumelden und auf Unternehmensressourcen zuzugreifen, oder ihnen erst gar nicht die Möglichkeit zur Authentifizierung bietet. Nach erfolgter Anmeldung wird das Risiko des Endgeräts kontinuierlich überprüft und sobald ein neues Risiko erkannt wird, verwehrt. In bestimmten Szenarien kann der Zugriff über ein Enterprise-Mobility-Management-Tool (EMM, z. B. bei verwalteten Geräten) oder ein Mobile-Application-Management-Tool (MAM, z. B. bei verwalteten Anwendungen) gesteuert werden

## WARUM SETZEN IMMER MEHR UNTERNEHMEN AUF „POST-PERIMETER-SECURITY"?

Unternehmensdaten werden zunehmend in der Cloud gehostet, auf die immer häufiger über Geräte zugegriffen wird, die sich in Netzwerken außerhalb der Kontrolle der IT-Abteilung befinden. Dies können Mobilfunknetze (WWAN) oder öffentliches WLAN sein. Firmendaten werden längst nicht mehr einfach nur zwischen einem Server und einem Endgerät in einem von der IT verwalteten Netzwerk übertragen. Stattdessen gelangt ein Großteil der Unternehmensdaten nicht einmal mehr physisch in die Firmensysteme. Heutzutage müssen Daten über Netzwerkgrenzen hinaus auf jedem Gerät zugänglich sein.

> **„Gartner schätzt, dass 80 % aller Arbeitsaufgaben bis 2020 über Mobilgeräte erledigt werden."**
>
> – Gartner, „Prepare for Unified Endpoint Management to Displace MDM and CMT", Juni 2018

### Cloudbasierte Produktivitätstools werden immer häufiger genutzt.

Mittlerweile werden viele zentrale Produktivitätsanwendungen für Büroaufgaben als Softwaredienst (Software as a Service, SaaS) bereitgestellt, unterstützt durch eine Identitäts- und Zugriffsmanagementlösung. SaaS-Anwendungen sind nicht länger an ein spezifisches Gerät gebunden, sondern an eine Nutzeridentität. Das bedeutet, dass Anwender jederzeit und überall von jedem beliebigen Gerät auf diese Anwendungen zugreifen können, egal ob Laptop oder Mobilgerät. Dies hat den Nachteil, dass Unternehmen nicht länger traditionelle Sicherheitsmaßnahmen anwenden können, um den Zugriff auf die Unternehmensdaten und den Datenverkehr zu überwachen.

## VOLLUMFÄNGLICHE VERWALTUNG UND KONTROLLE NOTWENDIG

In einer Welt ohne Netzwerkgrenzen haben Mitarbeiter mehr Kontrolle darüber, welche Tools sie für ihre Arbeit verwenden. Oft nutzen sie deshalb lieber ihre eigenen und privaten Tools, statt Unternehmensanwendungen und -diensten, die ihnen von der IT bereitgestellt wurden. Hier besteht die Herausforderung für die IT darin, den Zugriff auf Unternehmensdaten abzusichern, ohne den Anwender einzuschränken. Hinzu kommt noch die zunehmende Verbreitung von BYOD-Richtlinien (Bring Your Own Device) in Unternehmen, die es der IT meist besonders schwer macht, die als Arbeitsmittel genutzten Privatgeräte zu überwachen. Neben der Verwaltung von Geräten und Anwendungen (z. B. über eine Mobilgerätemanagement- oder Mobile-Application-Management-Lösung, kurz MAM), kommt es heute auch darauf an, den Zugriff auf Unternehmensdaten per Identitätsprüfung und SaaS-Anwendungskontrollen zu schützen.

### „Post-Perimeter Security" basiert auf bestehenden Strategien

Die automatische Freigabe auf Daten, sobald sich ein Anwender oder Endgerät am Firmennetzwerk anmeldet, funktioniert in einer auf Mobilgeräte und die Cloud ausgerichteten Welt nicht mehr. Deshalb entwickelte der Forrester Research-Analyst Jon Kindervag 2009 das Sicherheitsframework Zero Trust[2]. Ziel von „Zero Trust" ist es, sämtliche Endgeräte, die auf Unternehmensdaten zugreifen möchten, als nicht vertrauenswürdig einzustufen. Stattdessen wird sämtlicher Datenverkehr protokolliert und überprüft, um sicherzustellen, dass die Anwender sich richtig verhalten.

2011 entwickelte Google ein Modell für Unternehmenssicherheit, genannt BeyondCorp[3]. BeyondCorp war ursprünglich eine Google-interne Initiative, die es jedem Mitarbeiter ermöglichte, auch aus nicht vertrauenswürdigen Netzwerken ohne die Verwendung eines VPN zu arbeiten. Die Zugangsvoraussetzungen sind in Vertrauensstufen organisiert, von denen jede sensibler ist als die vorherige. BeyondCorp betrachtet Mobilgeräte als primäre Plattformen, die dieselben Zugriffsrechte benötigen, um Aufgaben ausführen zu können.

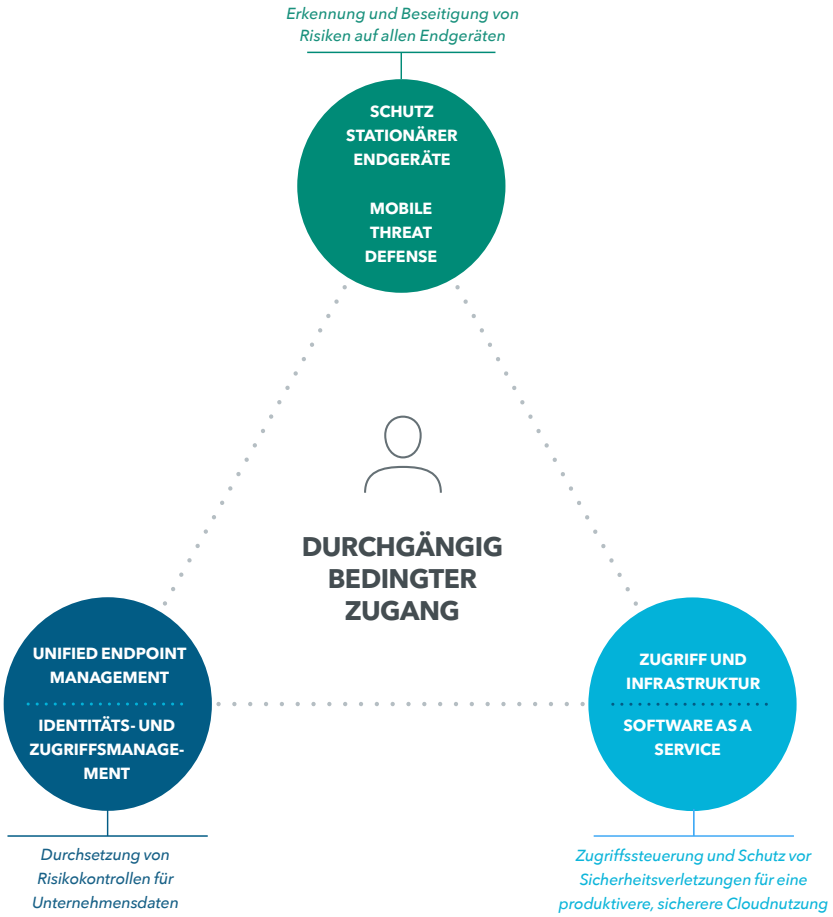
2017 erweiterte Gartner das Zero-Trust-Modell und BeyondCorp mit seinem Framework CARTA (Continuous Adaptive Risk and Trust Assessment), das Risiken und die Vertrauenswürdigkeit kontinuierlich überprüft. Gartner zufolge sind einmalige Sicherheitsüberprüfungen (z. B. bei der Anmeldung), die zur Freigabe oder Verweigerung des Zugriffs führen, unzureichend für umfassenden Schutz und machen das Unternehmen anfällig für Zero-Day-Exploits und gezielte Angriffe sowie interne Bedrohungen und den Diebstahl von Zugangsdaten.[4]. Der Kern des CARTA-Frameworks besteht darin, dass das Vertrauen (und Risiko) digitaler Geschäftsentitäten und ihrer Handlungen dynamisch und kontinuierlich überprüft werden muss, während Interaktionen stattfinden und zusätzlicher Kontext gewonnen wird.

.„Post-Perimeter Security" gründet auf diesen zentralen Säulen moderner Sicherheit in einer mobilgeräte- und cloudorientierten Welt und bietet eine Architektur, mit der Unternehmen den Zugriff auf Firmenressourcen kontinuierlich und dynamisch beschränken können. So lassen sich Anwender gezielt schützen, die oft das erste Einfallstor für Cyberangriffe sind.

## SO WIRD „POST-PERIMETER-SECURITY" REALITÄT

Da sich immer mehr Apps, Geräte und Netzwerke außerhalb der Reichweite von perimeterbasierten Sicherheitsmechanismen befinden, werden Konzepte wie Zero Trust, BeyondCorp und CARTA für viele IT-Abteilungen zum obersten Ziel. Ziel bei der Verwirklichung des „Post-Perimeter Security"-Ansatzes ist es, bereits vorhandene Dienste zu erweitern und zu integrieren.

## Was ist für Sicherheit über die Netzwerkgrenzen hinaus notwendig?




## Schutz für alle Endgeräte

Beim Endgeräteschutz kommt es darauf an, Anwenderhandlungen und Geräten grundsätzlich nicht zu vertrauen und daher ihr Risiko kontinuierlich zu ermitteln. Ein solcher Schutz muss sich sowohl auf Desktops als auch mobile Endgeräte erstrecken, da der Zugriff auf Unternehmensanwendungen über all diese Geräte gleichermaßen erfolgt. Außerdem muss sich der Endgeräteschutz um Dienste wie Identitäts- und Zugriffsmanagement-Lösungen und/oder die cloudbasierten Anwendungen selbst erweitern lassen, um bei Risiken eingreifen zu können. In bestimmten Fällen sind dazu Integrationen mit Kontrollmechanismen von EMM-Tools (Enterprise Mobility Management) erforderlich.

## Sicherheit und Produktivität in der Cloud

Mit der zunehmenden Verbreitung von Clouddiensten und der entsprechenden Infrastruktur wird der sichere Zugriff auf gehostete Anwendungen und Daten zur obersten Priorität. Sicherheitslösungen für die Cloud bieten einen unabhängigen Zugriff und Schutz vor Sicherheitsverletzungen für die gehosteten Daten und Dienste. Darüber hinaus müssen Anbieter von Clouddiensten Identitäts- und Zugriffsmanagement sowie Endgeräteschutz integrieren, um die potenziellen Risiken abzudecken, die von Zugriffsanfragen ausgehen. Zum Schutz der Anwender vor bösartigen Webseiten, müssen auch auf dem Endgerät die entsprechenden Sicherheitsvorkehrungen getroffen werden.

## Identitäts- und Zugriffsmanagement

Die Identität gilt heute als die neue „Netzwerkgrenze" und als Basis für den Zugriff auf Unternehmensdaten. Plattformen für die Identitätsprüfung rationalisieren den Zugriff mittels Funktionen wie Einmalanmeldung (SSO), was es Anwendern erleichtert, verschiedene Anwendungen und Dienste gleichzeitig zu nutzen. Zwar offerieren die Anbieter von Identitäts- und Zugriffsmanagement-Lösungen bereits wichtige Sicherheitsfunktionen wie die Multifaktor-Authentifizierung, um den Zugriff auf Daten vor Ort und in der Cloud zu schützen, jedoch müssen sie auch den entsprechenden Endgeräteschutz integrieren, um das Risiko nicht vertrauenswürdiger Geräte kontinuierlich prüfen zu können. Die Kombination aus Identitätsprüfung und Endgeräteschutz ermöglicht Unternehmen eine fortlaufende Einschätzung der Vertrauenswürdigkeit von Anwendern und Geräten.

## DIE „POST-PERIMETER ALLIANCE“

Die „Post-Perimeter Security Alliance“ (Allianz für Sicherheit über die Netzwerkgrenzen hinaus) vereint führende Enterprise-Anbieter, die eine gemeinsame Vision haben: Sicherheit und Produktivität für eine moderne, cloud- und datenschutzorientierte Welt. Heute ist es besonders schwierig, mit nur einer einzigen Lösung umfassenden Schutz über die Netzwerkgrenzen hinaus zu erreichen. Vielmehr sind integrierte Sicherheitsfunktionen notwendig, die Endgeräte, die Cloud und Identitäten umspannen. Und genau mit dieser Kombination sorgt unsere Allianz für Produktivitätssteigerungen und den Schutz des Zugriffs auf Unternehmensdaten. Die von der „Post-Perimeter Security Alliance“ gebotenen Lösungen ermöglichen die kontinuierliche Prüfung des Risikos für Unternehmensdaten sowie geeignete Gegenmaßnahmen.

Zu den Mitgliedern der „Post-Perimeter Security Alliance“ zählen Anbieter von Lösungen zur Erkennung mobiler Bedrohungen, für den Endgeräteschutz, das Identitäts- und Zugriffsmanagement sowie von Enterprise-Mobility-Management- und cloudbasierten Produktivitätslösungen. Da es sich um die Marktführer auf ihrem jeweiligen Gebiet handelt, ist es sehr wahrscheinlich, dass eine oder mehrere Lösungen dieser Anbieter bereits Bestandteil der Infrastruktur von Unternehmen ist. Ob bewusst oder unbewusst, viele Firmen sind bereits auf bestem Weg zu einer Strategie für Sicherheit über die Netzwerkgrenzen hinaus.

**Klicken Sie hier um mehr darüber zu erfahren, wie Sie Sicherheit über die Netzwerkgrenzen hinaus in lhr Unternehmen integrieren können.**

> **„Eine branchenübergreifende Initiative wie die Post-Perimeter Security Alliance ist heute besonders sinnvoll und kann Unternehmen helfen, die eine Architektur für Sicherheit über die Netzwerkgrenzen hinaus implementieren möchten, jedoch nicht wissen, wie die einzelnen Puzzleteile zusammenpassen.“**
>
> – Phil Hochmuth, Program Director, Enterprise Mobility bei IDC

[1] Gibt es Vertrauen in Zero-Trust-Modellen? Mit Post Perimeter Security in einer neuen mobilen Arbeitswelt (1. November 2018)
Quelle: https://www.lookout.com/de/info/lookout-post-perimeter-lp

[2] Getting Started with Zero Trust: Never trust, always verify
Quelle: https://drive.google.com/file/d/1y_bexOdulUAr8M9wZxTqAGv21T3Vchor/view?ts=5c361c31

[3] Barclay Osborn, Justin McWilliams, Betsy Beyer und Max Saltonstall. (Frühling 2016) „BeyondCorp, Design to Deployment at Google“
Quelle: https://storage.googleapis.com/pub-tools-public-publication-data/pdf/44860.pdf

[4] Gartner, „Seven Imperatives to Adopt a CARTA Strategic Approach“ (10. April 2018)
Quelle [Abonnement erforderlich]: https://www.gartner.com/doc/3871363/seven-imperatives-adopt-carta-strategic