

## NEWS RELEASE

### **NETGEAR® führt neuen Security-Service Armor™ ein, um zu Hause WLAN-Netzwerke und verbundene Geräte zu schützen**

*Basierend auf Bitdefender® bietet NETGEAR Armor fortschrittlichen Schutz vor Cyber-Bedrohungen für Heimnetzwerke, mobile Geräte, Internet of Things (IoT) und Smart Home Devices.*

**München/Las Vegas, 10. Januar 2018** – NETGEAR® (NASDAQ: NTGR), weltweit führender Anbieter von Netzwerklösungen und Sicherheits-Systemen für Smart Homes, bringt einen neuen umfassenden Security-Service auf den Markt, der Sicherheit für alle Geräte bietet, die über einen NETGEAR Router verbunden sind. NETGEAR Armor™ powered by Bitdefender®, preisgekrönter Marktführer im Bereich der Netzsicherheit, ist eine fortschrittliche Multilayer-Lösung auf Basis eines Jahresabonnements, die auf NETGEAR Routern und angeschlossenen Geräten läuft, um das Zuhause des Anwenders wie auch dessen Familienmitglieder aktiv vor Cyber-Bedrohungen, wie etwa Viren, Spyware, Spam und Phishing, zu schützen.



POWERED BY  
**Bitdefender®**

NETGEAR Armor wird noch im laufenden Quartal auf dem Nighthawk® AC2300 Smart WiFi Router (R7000P) verfügbar

sein. Im Laufe des Jahres folgt per Firmware-Update der jeweiligen Geräte die Unterstützung für das NETGEAR Orbi™ Mesh WLAN System und die beliebten Nighthawk Performance Router. Das NETGEAR Armor Firmware-Update bietet zentrale Sicherheit für den sofortigen Schutz aller PCs, Macs, Smartphones und Tablets sowie Smart-Home-Geräte vor Cyber-Bedrohungen. Das Software-Paket beinhaltet auch die Bitdefender Total Security Anti-Malware\* für Windows™, macOS®, iOS® und Android™-Geräte – alles in einem einzigen Abonnement. Der neue Security-Service blockiert bereits am Gateway den Zugriff auf Phishing-Websites aus dem Heimnetzwerk heraus, sodass Privatsphäre und Daten der Anwender stets geschützt sind. Die Netzsicherheit hat sich zu einem immer wichtigeren Bereich entwickelt, da zunehmend Smart-Home- und IoT-Geräte in das Heimnetzwerk Einzug halten, die immer eingeschaltet und dauerhaft verbunden sind und neue potenzielle Schwachstellen mit sich bringen. Während PC-Sicherheit seit Langem ein Kernthema im Büro und zu Hause ist, stellt die Vielzahl der heute verfügbaren angeschlossenen Geräte neue, potenzielle Sicherheitsrisiken für den User dar.

„Die Notwendigkeit einer umfassenden Cyber-Sicherheitslösung für zu Hause ist wichtiger denn je“, betont Ciprian Istrate, Vice President Consumer Solutions bei Bitdefender. „Nachdem Bitdefender die erste Cyber-Sicherheitslösung für den Heimgebrauch auf den Markt gebracht hat, die angeschlossene Geräte, die unter das Internet of Things fallen, schützen kann, hebt Bitdefender nun die Cyber-Sicherheit für den Endverbraucher auf die nächste Stufe, indem NETGEAR den Schutz direkt vom Router aus liefert.“

NETGEAR Armor liefert alles, um sein Heimnetzwerk, alle angeschlossenen IoT-Geräte, das Smart Home und Mobile Devices sicher und geschützt zu halten – und das von überall auf der Welt. NETGEAR Armor bietet die folgenden Features:

### **Sicheres Browsen mit URL-Blocking**

Mit NETGEAR Armor schützen User ihr Netzwerk aktiv vor Bedrohungen wie Trojanern, Ransomware, Zero-Day-Attacken, Rootkits und Spyware. Gefälschte Webseiten, die versuchen, Finanzdaten, wie etwa Passwörter oder Kreditkartennummern, zu stehlen, werden ebenso automatisch blockiert, wie bösartige Links in Browsern, E-Mails oder Anwendungen. Armor User können sogar herausfinden, ob ihre Suchergebnisse sicher sind, bevor sie auf einen Link klicken, da sie vor Webseiten gewarnt werden, die Anmeldeinformationen ausspionieren, wenn die Authentifizierung nicht über HTTPS erfolgt.

### **Schwachstellenanalyse**

NETGEAR Armor durchsucht das eigene Netzwerk blitzschnell nach angeschlossenen Geräten, die bezüglich unbefugtem Zugriff, Datendiebstahl oder böswilliger Angriffe gefährdet sind. Die Stärke des Passworts, die Firmware-Version und alle Schwachstellen, die Hackern Zugriff auf das Heimnetzwerk ermöglichen könnten, werden geprüft. Es geht spielend einfach, einen ausführlichen Bericht zu erstellen, der auch Tipps zur Behebung bestimmter Schwachstellen enthält, oder einfach den Status der Geräte zu überprüfen und mögliche Probleme zu adressieren.

### **Intelligente Vermeidung von Netzwerk-Eindringlingen**

NETGEAR Armor verhindert, dass Hacker auf Smart-Home-Geräte, wie z. B. internetfähige Thermostate, Kühlschränke, Baby-Monitoring-Systeme und Sicherheitskameras, zugreifen können. Armor Anwender werden sofort benachrichtigt, wenn neue Geräte in ihr Netzwerk eingebunden werden, sodass sie Zugriffsanfragen für Geräte, die unbekannt sind, sofort ablehnen können. Für

maximalen Komfort können User ihre Netzsicherheit von jedem beliebigen Ort aus unter <http://armor.netgear.com> verwalten.

### **End-point Protection mit Bitdefender Total Security**

NETGEAR Armor beinhaltet Bitdefender Total Security Anti-Malware für Android, iOS, Windows-PCs und Macs, egal ob zu Hause oder unterwegs. NETGEAR Armor überwacht mithilfe intelligenter, verhaltensorientierter Erkennung alle aktiven Anwendungen und sobald der Dienst verdächtige Aktivitäten entdeckt, werden sofort Schutzmaßnahmen ergriffen, da er so konzipiert ist, innerhalb von drei Sekunden auch auf die neuesten bekannten Bedrohungen zu reagieren. Wenn der Armor Nutzer den optionalen Autopilot™ aktiviert, können alle Entscheidungen zur Cyber-Sicherheit ohne Pop-ups oder Dialogfelder getroffen werden, um nicht von Arbeit oder Spiel abzulenken.

„Seit mehr als 20 Jahren ist NETGEAR in der Branche als führender Anbieter von WLAN-Systemen bekannt und hat kontinuierlich innovative Technologien für Heim- und Büronetzwerke auf den Markt gebracht. Jetzt, mit der Einführung von NETGEAR Armor, machen wir das Netzwerk intelligenter und sicherer für die neue Welt des IoT und permanent verbundener Geräte“, sagt David Henry, Senior Vice President Connected Home bei NETGEAR. „Dieser Schritt ist von entscheidender Bedeutung für unsere Kunden, deren Privathaushalte mittlerweile über viele vernetzte Geräte verfügen, darunter Smart Home und IoT-Geräte, von denen jedes ein potenzielles Sicherheitsrisiko darstellen kann. Nach dem kürzlich erfolgten Start der Circle® mit Disney® Kindersicherung ist NETGEAR Armor das nächste Produkt in einer Reihe von Dienstleistungen, die wir einführen, um die Erfahrung unserer Kunden mit ihrem Netzwerk weiter zu verbessern.“

### **Weitere Features**

- Schutz des Netzwerks vor bösartigen Verschlüsselungsprogrammen, die für die Entschlüsselung oder Freigabe persönlicher Daten ein Lösegeld verlangen.
- Verwaltung und Konfiguration jedes Geräts, das eine Verbindung zum Netzwerk herstellt oder versucht, eine Verbindung zum Netzwerk herzustellen.
- Sofortige Benachrichtigungen, wenn sich neue Geräte mit dem Netzwerk verbinden.
- Prüfung der Sicherheit von WLAN-Netzwerk und -Router per Remote-Zugriff von Computern und Smartphones.
- Sicherung von Passwörtern, Kreditkarteninformationen und anderen sensiblen Daten in einem Cyber-Tresor mit einfachem Zugriff.

- Banking und Online-Shopping mit Safepay™, einem einzigartigen, dedizierten Browser, der Transaktionen absichert.
- Kontinuierliche und automatische Sicherheitsupdates.

NETGEAR Armor schützt Heimnetzwerke, ohne Geschwindigkeit, Leistung oder Privatsphäre des Netzwerks zu beeinträchtigen. Der Dienst scannt das Netzwerk und identifiziert jedes Gerät, das mit ihm verbunden ist. Der Scan geht schnell und ist ressourcenschonend, da er meist in der Cloud stattfindet, um Leistung und Effizienz zu maximieren. Router und Personal Devices werden nur selten für stromhungrige oder prozessorintensive Aufgaben herangezogen. Und NETGEAR Armor scannt und speichert niemals den tatsächlichen Inhalt von Dokumenten oder Dateien.

### **Preise und Verfügbarkeit**

NETGEAR Armor powered by Bitdefender wird zunächst per Firmware-Upgrade auf dem Nighthawk AC2300 Smart WiFi Router (R7000P) verfügbar sein und in den kommenden Monaten ebenfalls über Firmware-Updates auch für das NETGEAR Orbi Mesh WLAN System und die komplette Produktpalette der Nighthawk Router angeboten. Nach 90 Tagen kostenloser Testphase geht NETGEAR Armor automatisch in ein Jahresabonnement über. Der Preis hierfür wird in Kürze bekannt gegeben.

*\*Die Bitdefender Fair Use Policy ist auf maximal 20 Lizenzen beschränkt.*

### **Über Netgear Inc.**

NETGEAR (NASDAQ: NTGR) ist weltweit führender Anbieter innovativer Netzwerklösungen für kleine und mittelständische Unternehmen, Privatanwender und Service Provider. Das Portfolio umfasst verschiedenste Technologien in den Bereichen Wireless (WiFi und LTE), Ethernet und Powerline und zeichnet sich durch seine Zuverlässigkeit und Einfachheit aus. Die Produktfamilien beinhalten sowohl drahtgebundene als auch drahtlose Geräte für Networking, Breitbandzugang und Netzwerkkonnektivität. Die Produkte sind in vielfachen Konfigurationen verfügbar und erfüllen die unterschiedlichsten Anforderungen der Anwender. NETGEAR Produkte sind weltweit in ungefähr 31.000 Einzelhandelsstandorten und bei über 28.000 Value-Added Resellern (VARs) sowie Kabel-, Mobil- und Wireline-Service-Providern verfügbar. VARs können sich über das Partner Solution Programm qualifizieren. Hauptsitz des Unternehmens ist San Jose (Kalifornien) mit

zusätzlichen Standorten in nahezu 25 Ländern. Die Niederlassungen in der DACH-Region befinden sich in München, Wien und Baar. Weitere Informationen zu NETGEAR sind unter <http://www.netgear.de> oder telefonisch (+49 89 45242-9000) erhältlich.

Informationen zu NETGEAR in Deutschland: [www.netgear.de](http://www.netgear.de)

Newsroom für NETGEAR Business-Lösungen: <http://www.netgear-newsroom.de>

NETGEAR auf LinkedIn: <https://www.linkedin.com/company/netgear-business-deutschland>

NETGEAR auf Twitter: <https://twitter.com/NetgearBusiness>

**Weitergehende Informationen:**

Weitergehende Informationen sowie hochauflösendes Bildmaterial finden Sie [hier](#).

**Pressekontakt:**

**IsarGold GmbH**

Simone Kohler

Müllerstr. 39

80469 München

Tel. +49 89 4141715-15

[netgear@isar.gold](mailto:netgear@isar.gold)