



## Sophos Next Generation Firewall XG auch über Microsoft Azure erhältlich

**Wiesbaden, 2. November 2016** – Der Spezialist für Netzwerk und Endpoint Security Sophos baut seine Unterstützung für IaaS-Plattformen aus und bietet seine Next Generation XG Firewall auch in der Microsoft Azure-Plattform an. Kunden und Nutzer der Microsoft Azure-Plattform haben einen direkten und schnellen Zugriff auf alle Sicherheitsfunktionen der Sophos XG Firewall, zahlen jedoch nur für die Sicherheitskomponenten und -Features, die sie tatsächlich nutzen. Die Sophos XG Firewall ist bei Microsoft Azure ab Ende 2016 verfügbar, eine Vorschau ist bereits heute eingerichtet.

### Schnelle und einfache Konfiguration

Basierend auf der Sophos [UTM](#) und der Next Generation Firewall, liefert die Sophos XG Firewall einen umfassenden Schutz der nächsten Generation, der die Managementkosten reduziert und die Cloud-basierte Verwaltung deutlich erleichtert. Innerhalb des Microsoft Azure Ecosystems können Kunden mit Hilfe des Azure Resource Managers die XG Firewall als eine vorkonfigurierte virtuelle Maschine je nach Bedarf nahtlos einsetzen und anpassen. Sie generiert und speichert detaillierte Out-of-the-Box-Berichte, die genaue Auskunft über das Nutzerverhalten geben. Im „User Threat Quotient“-Bericht werden Ausgangswerte festgelegt, um ungewöhnliches Nutzerverhalten zu erkennen.

### Mehr Sicherheit durch integrierte Synchronized Security

Wichtiger Bestandteil der Sophos XG Firewall ist die Cloud-basierte Sophos Synchronized Security inklusive der Heartbeat-Technologie, einem technologischen Kommunikations-Tool zwischen Endpoints und der Firewall. Sophos Synchronized Security ist zentraler Bestandteil der Sophos Next Generation Firewall und bietet erweiterten Schutz durch eine direkte Kommunikation zwischen Firewall und Endpoint Security. Die Lösungen teilen ihr Wissen und bieten so ein wesentlich schnelleres Erkennen von Attacken, eine automatische Isolation infizierter Geräte und so eine schnellere Behebung des Problems. Sophos Heartbeat ist dabei das technologische Kommunikationsnetz zwischen Endpoints und der Firewall. Heartbeat übermittelt verdächtiges Verhalten einzelner Geräte oder bösartige Attacken in Echtzeit. Sophos Heartbeat leitet eine sofortige Aktion ein, die einen Malware-Ausbruch oder Datendiebstahl unterbindet.

„Organisationen verlagern ihre Aktivitäten zunehmend in die Cloud und die Sicherheit steht häufig nicht an erster Stelle. Das möchten wir ändern und bieten eine Infrastruktur, die gleich von Beginn an schützt. Benutzerdefinierte Vorlagen, flexible Lizenzoptionen und Support für den Azure Resource Manager und klassische Deployment-Modelle gehören dazu“, erläutert Joe Levy, Chief Technology Officer bei Sophos. „Sicherheit muss stark und leistungsfähig sein. Dazu ist es besonders wichtig, dass sie sich möglichst einfach in die IT-Infrastruktur der Organisationen integriert.“

### Kernfunktionen der Sophos XG Firewall

- **Security Heartbeat.** Diese einzigartige Technologie verbindet Firewall und Endpoint, um Informationen zu teilen und den Schutz vor Bedrohungen deutlich erhöhen.
- **Network Security Control Center.** Eine innovative Schnittstelle, die umgehend Netzwerk- und Bedrohungsinformationen liefert, damit eine Reaktion auf Angriffe schnell erfolgen kann.

- **Einheitliches Policy-Modell.** Eine vereinfachte Richtlinienverwaltung mit vorkonfigurierten Templates für Business-Anwendungen, um die Konfiguration deutlich zu vereinfachen.
- **Benutzer- und App-Risikoanalyse.** Eine App-Risk-Score-Funktion hilft, Risiko-Benutzer und -Anwendungen zu identifizieren und potenzielle Sicherheits-Hotspots auszumachen.
- **Benutzer Threat Quotient.** Verwalten von Benutzer-Policies, die sich auf das Verhalten des Individuums sowie auf den Zustand seines Computers oder seines mobilen Geräts stützt.
- **Sophos Firewall Manager.** Zentrale Verwaltung mehrerer Firewalls, die für Sophos-Partner und Managed Service Provider kostenlos ist.
- **Zentrales Cloud Management.** Mit dem neuen Sophos Cloud Firewall Manager können Sophos Partner und MSPs mehrere Sophos XG Firewall-Installationen zentral aus der Cloud verwalten.

### **Flexible Preisgestaltung**

Das Lizenzmodell ermöglicht das „Pay As You Go“ direkt in Microsoft Azure oder die Option von „Bring Your Own License“ (BYOL). Bei der BYOL-Option können Kunden die Lizenz bei einem Sophos Partner erwerben und in Microsoft Azure verwenden. Dazu gehören auch Support und Preisvorteile, die der gewählte Partner anbietet. Die Verfügbarkeit von BYOL kann von Land zu Land variieren. Informationen sind beim lokalen Sophos Partner erhältlich.

### **Über Sophos**

Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter [www.sophos.de](http://www.sophos.de).

### **Pressekontakt:**

Sophos

Jörg Schindler, PR Manager CEEMEA

[joerg.schindler@sophos.com](mailto:joerg.schindler@sophos.com), +49-721-25516-263

TC Communications

Arno Lücht, +49-8081-954619

Thilo Christ, +49-8081-954617

Christiane Capps, +49-174-3335550

Ulrike Masztalerz, +49-30-55248198

[sophos@tc-communications.de](mailto:sophos@tc-communications.de)