

## Fünf Wege, um die virtuelle Netzwerksicherheit zu erhöhen

### 1. Föderierte Identitäten (Federated ID)

Um eine Authentifizierung auf Anwenderebene gewährleisten zu können, sind „Single-Sign-on“-Funktionen (SSO) erforderlich. Mithilfe von SSO können Unternehmen ihr Sicherheitsmanagement optimieren und eine starke Authentifizierung innerhalb der Cloud sicherstellen.

### 2. Unterbrechungsfreie Konnektivität

Ist ein Großteil der kritischen Unternehmensdaten in der Cloud gespeichert, kann ein Netzwerkausfall den gesamten Geschäftsbetrieb gefährden. Der Zugriff auf Cloud-Dienste muss daher jederzeit gewährleistet sein, auch während einer Wartung.

### 3. Multi-Layer-Kontrolle

Anstatt Firewalls der ersten Generation als Perimeterschutz in der Cloud zu implementieren, empfiehlt sich der Einsatz virtueller Firewall-Appliances der nächsten Generation. Diese bieten erweiterte Firewall- und IPS-Funktionen für eine umfassende Analyse des Datenverkehrs (Deep Traffic Inspection).

### 4. Zentrales Management

Menschliche Fehler stellen immer noch die größte Sicherheitsbedrohung dar, sowohl in physikalischen als auch in virtuellen Umgebungen. Es empfiehlt sich eine zentrale Management-Konsole zur Verwaltung, Überwachung und Konfiguration von allen physikalischen und virtuellen Geräten sowie Drittanbieter-Produkten.

### 5. Virtueller Desktop-Schutz

Immer mehr Unternehmen setzen auf Desktop-Virtualisierung, um von dem Kostenvorteil und der einfachen Administration zu profitieren. Um sie ausreichend zu schützen, sollten Unternehmen sie von anderen Netzwerkbereichen isolieren und Deep Inspection auf Netzwerkebene implementieren.

