

# Xerox:



## ein umfassendes Konzept für Druckersicherheit

Drucker und Multifunktionsgeräte sind heute in der Lage, zentrale Aufgaben im geschäftlichen Alltag zu übernehmen. Angesichts der exponentiellen Zunahme von WLAN-Geräten, cloudgestützter Software und Clouddiensten muss ein Drucker nicht nur für diese Technologien gerüstet, sondern auch gegen die Gefahren gewappnet sein, die von ihnen ausgehen können.



Schutz vor unbefugtem Zugriff



Geräteerkennung



Dokumenten- und  
Datenschutz



Externe Partnerschaften

### SCHUTZ VOR UNBEFUGTEM ZUGRIFF

Die erste und naheliegendste Schwachstelle ist das Gerätedisplay – wer hat physischen Zugriff auf Ihren Drucker und seine Funktionen? Die Sicherheitsoptionen von Xerox beginnen mit der **Benutzerauthentifizierung**, womit gewährleistet wird, dass nur autorisierte Personen Zugriff auf die Geräte haben. Nach der Anmeldung stellt die **rollenbasierte Zugriffssteuerung** sicher, dass jedes Teammitglied nur die Funktionen sieht, die Sie freigegeben haben. Jede Aktion eines jeden Benutzers wird protokolliert, wodurch ein vollständiger **Audittrail** gewährleistet ist.

Danach kümmern wir uns um weniger offensichtliche Schwachstellen – was wird an den Drucker gesendet und wie? Xerox® ConnectKey®-Technologie fängt Angriffe über beschädigte Dateien und Malware ab.<sup>1</sup> Außerdem ist unsere Systemsoftware **digital signiert**, was bedeutet, dass jeder Versuch, infizierte, nicht signierte Versionen zu installieren, automatisch verhindert wird. Druckdateien werden ebenfalls gelöscht, wenn ein Teil nicht als legitim erkannt wird.

### GANZHEITLICHER SCHUTZ FÜR IHREN DRUCKER

Xerox hat diesen technologischen Wandel und die sich ändernden Anforderungen schon vor langer Zeit erkannt und sich darauf eingestellt. Wir bieten umfassende Sicherheitsfunktionen, damit Ihre Drucker und Daten sicher sind. Xerox schützt jeden Teil der Datenkette, einschließlich **Drucken, Kopieren, Scannen, Fax, Dateidownloads** und **Systemsoftware**. Unser mehrschichtiger Ansatz umfasst vier Schlüsselaspekte.



## GERÄTEERKENNUNG

Im unwahrscheinlichen Fall, dass Ihre Daten- und Netzwerkschutzmechanismen überwunden werden, führt die Xerox® ConnectKey® Technologie einen umfassenden Test zur **Firmware-Verifizierung** aus. Dies geschieht entweder beim Systemstart<sup>2</sup> oder durch Aktivierung durch einen autorisierten Benutzer. Hierbei werden Sie gewarnt, wenn schädliche Änderungen an Ihrem Drucker erkannt wurden. Unsere fortschrittlichsten integrierten Lösungen verwenden die **McAfee® Whitelisting-Technologie**,<sup>3</sup> die Geräte kontinuierlich auf potenzielle Malware überwacht und deren Ausführung automatisch verhindert. Die Integration mit **Cisco® Identity Services Engine (ISE)** ermöglicht es, Xerox® Geräte im Netzwerk zu erkennen und als Drucker zu klassifizieren, um die Implementierung von Sicherheitsrichtlinien und Compliance-Anforderungen zu erleichtern.



## EXTERNE PARTNERSCHAFTEN

Xerox arbeitet mit Organisationen zusammen, die Compliance-Tests durchführen, sowie mit branchenführenden Sicherheitsunternehmen, wie **McAfee und Cisco**, um deren umfassende Standards und Expertise mit unseren zu kombinieren.

Unabhängige Dritte – z. B. Zertifizierungsstellen wie **Common Criteria (ISO/ IEC 15408)** und **FIPS 140-2** – messen unsere Leistung auf Basis internationaler Standards und liefern den Beweis, dass wir Top-Compliance-Werte erreichen.

Sie schätzen uns für unseren umfassenden Ansatz in Bezug auf die Druckersicherheit.

<sup>1</sup> Malware wird mithilfe der McAfee® Whitelisting-Technologie abgefangen

<sup>2</sup> Xerox® VersaLink® Drucker

<sup>3</sup> Xerox® AltaLink® MFPs, Xerox® WorkCentre® i-Series MFPs und Xerox® WorkCentre® EC7836/EC7856 MFPs

<sup>4</sup> Gilt nur für Geräte mit Festplattenlaufwerken

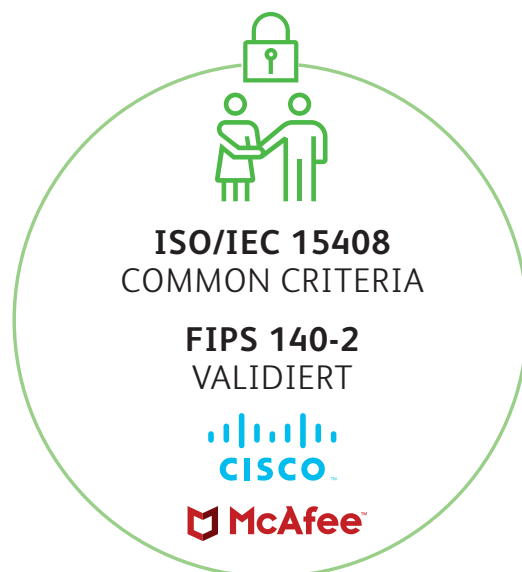


## DOKUMENTEN- UND DATENSCHUTZ

Xerox geht noch weiter. Mit unseren umfassenden Sicherheitslösungen sind auch Ihre gedruckten und gescannten Dokumente vor unbefugter Offenlegung bzw. unbefugten Änderungen geschützt. Die Xerox® ConnectKey-Technologie dient dazu, die absichtliche oder versehentliche Übertragung wichtiger Daten an Personen zu verhindern, die für den Zugriff darauf nicht autorisiert sind.

Wir können die Druckausgabe mit einem **PIN-Code** oder einem **kartenbasierten** Freigabesystem schützen. Wir können verhindern, dass Unbefugte Zugriff auf Scaninformationen erhalten, indem wir **digital signierte, verschlüsselte und kennwortgeschützte** Dateiformate verwenden. Bei ConnectKey-fähigen Druckern können Sie die E-Mail-Felder **An/Kopie/Blindkopie** sperren, um das Scanziel auf **interne Adressen** zu begrenzen.

Xerox schützt außerdem Ihre gespeicherten Informationen mit einer **Verschlüsselung** auf höchstem Niveau. Nicht mehr benötigte Daten, die auf dem Gerät verarbeitet oder gespeichert wurden, können Sie mithilfe von Algorithmen zur **Datenbereinigung** und **Datenlöschung** gemäß der strikten Vorgaben des US-amerikanischen National Institute of Standards and Technology (NIST) und des US-Verteidigungsministeriums löschen.<sup>4</sup>



Weitere Informationen finden Sie unter [www.xerox.com/security](http://www.xerox.com/security)