

SMARTshield



Integrierte Drucksicherheits-Technologie
Für ColorWave und PlotWave Drucker

Canon

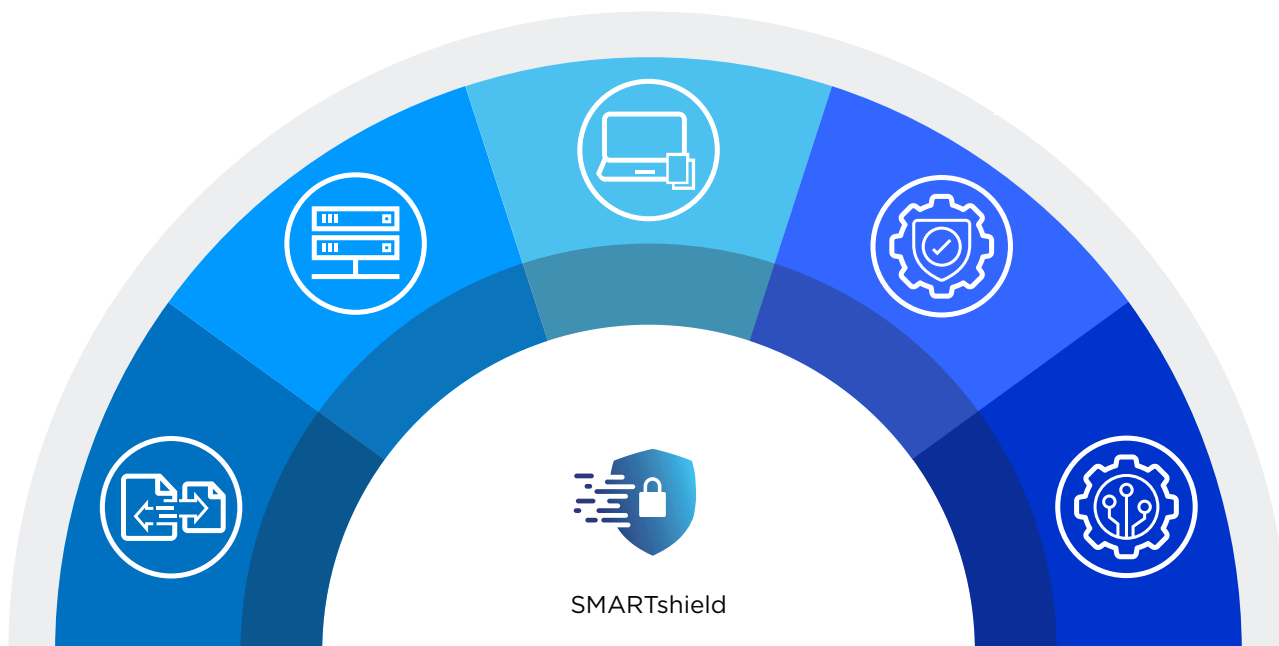
DIE 1. KLASSE DER DRUCKSICHERHEIT

Unsere marktführenden Großformatdrucker gehen auf die Sicherheitsanliegen technischer Dokumentennutzer ein, die mit vertraulichen Kundendaten zu tun haben.

SMARTshield ist eine Suite von Sicherheitsfunktionen, die in die aktuellen PlotWave und ColorWave Systeme integriert sind. Entwickelt wurde sie zum Schutz Ihrer Systeme: heute und in der Zukunft.



ColorWave 3800



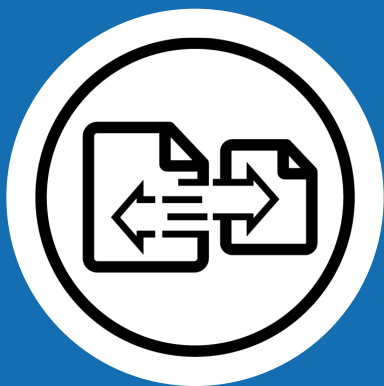
Mehr denn je müssen Unternehmen und Behörden mit Großformatdruckern ihre geschäftskritischen, vertraulichen und sensiblen Informationen innerhalb ihrer Büros und Netzwerke schützen. Dazu zählen sowohl Informationen, die von Einzelarbeitsplätzen und anderen Geräten zum Drucker geschickt werden, als auch Daten, die im Drucker gespeichert sind. Es ist entscheidend, dass Systeme gegen unbefugten Zugriff auf Druckdaten, gedruckte Informationen und die eigene IT-Infrastruktur des Endnutzers via Drucker geschützt sind. Aus diesem Grund brauchen Unternehmen einen sicheren Großformatdrucker, der dem IT-Administrator, den Nutzern und der Führungsebene die Arbeit erleichtert.

SMARTshield ist eine vollintegrierte Drucksicherheits-Technologie in all unseren Großformatdruckern. Sie wurde eigens entwickelt, um diese Anforderungen zu erfüllen.

SMARTshield beinhaltet eine Reihe von Sicherheitsvorkehrungen, um Daten und Informationen vor unerwünschten Blicken fernzuhalten.

Mit SMARTshield werden all Ihre Sicherheitsrisiken in jeder Phase des Workflow-Prozesses berücksichtigt.

SMARTshield schützt Sie heute und in der Zukunft.



SICHERE ÜBERMITTLUNG

Datenschutz während der Dateiübermittlung zum Drucker – von jedem Gerät aus.

Dank der ClearConnect-Workflowanwendungen können Benutzer Dateien von ihrem Desktop oder einem beliebigen mobilen Gerät aus senden. Angesichts dieser Flexibilität und Mobilität ist es wichtig, dass wertvolle Daten jederzeit und von allen Geräten aus sicher zum Drucker übertragen werden.



IPsec-Kompatibilität



IPv6- und IPv4-Kompatibilität



HTTPS





SICHERE SPEICHERUNG UND LÖSCHUNG

Schutz vertraulicher Daten, die auf der Festplatte des Druckers gespeichert sind. Es muss verhindert werden, dass vertrauliche Daten einer Firma oder Abteilung, die auf dem Drucker gespeichert sind, gestohlen werden oder unbeabsichtigt in falsche Hände gelangen. SMARTshield verschlüsselt Daten und erlaubt den Zugriff nur nach erfolgreicher Nutzererkennung. So werden all Ihre Daten geschützt. Indem Daten vorschriftsmäßig gelöscht werden, haben Nutzer die Gewissheit, dass unbefugte Kollegen nicht auf vertrauliche Dateien zugreifen können.

- Sichere Dateilöschung
- E-Shredding
- Herausnehmbare Festplatte
- Sicheres Booten
- Datenverschlüsselung
- Festplattenzerstörung zum Vertragsende





BEFUGNISSE

SMARTshield-Benutzerberechtigungschränkt den Zugriff für nicht autorisierte Benutzer auf vertrauliche Dateien ein.

Indem Nutzer sich ausweisen müssen, erhalten Sie eine noch genauere Übersicht von deren Aktivitäten. Auch ist es möglich, die Funktionen und Protokolle, auf die sie zugreifen können, zu beschränken und nutzergerecht die entstanden Kosten zu zuweisen.



- Bedienfeld-Zugriffssperre
- Sicherer Druck über Domain-Zugangsdaten (Active Directory)
- Sicherer Druck über Smartcard (ausschl. Scaneinheit)
- Druckdateien nur über Ihre Smart Inbox verfügbar
- Scannen an Ihren persönlichen Benutzerordner
- Drucken über Ihren persönlichen Benutzerordner
- Deaktivieren von Ports und Schnittstellen
- Drittanbieter-Software wie uniFLOW



SCHUTZ VOR HACKERN

Eine der größten Sicherheits Herausforderungen für Unternehmen ist die Abwehr von Hackern. Angesichts all der wertvollen Druckdaten muss der Zugriff auf den Drucker und die im Controller (oder auf der Festplatte) gespeicherten Daten unbedingt beschränkt werden.

Und Sie wollen die Sicherheit, dass Ihr Drucker nicht unterwandert und gegen Ihr Netzwerk genutzt werden kann. SMARTshield begegnet der Hackergefahr an verschiedenen Fronten:

- Deaktivierung ungenutzter Protokolle
- SNMP v3
- IEEE 802.1x Kompatibilität
- McAfee Antivirus (optional)
- McAfee Whitelisting Application-Steuerung (optional)





HEUTE UND IN DER ZUKUNFT SICHER

Sicherheit ist keine statische Situation. Unentwegt suchen Hacker nach neuen Wegen, auf Ihre wertvollen Informationen zuzugreifen. SMARTshield wurde zum Schutz Ihrer Informationen entwickelt: heute und in der Zukunft.

Natürlich haben unsere Sicherheitsfachleute stets die aktuellen Risiken im Blick, damit der Schutz Ihrer Daten und Drucker gewährleistet ist. Zu den jetzigen Funktionen gehören:

- Windows 10 IoT Enterprise LTSC Controllersoftware
- Support bis mindestens 2029 oder darüber hinaus
- Remote Controller-Sicherheitsupdates
- Remote Service



Wir verstehen Ihre Sicherheitsanliegen und haben eine Reihe von Funktionen zusammengestellt, die all Ihre Sicherheitsrisiken auf jeder Stufe des Workflows gezielt überwachen und schützen. Nicht nur heute, sondern auch in der Zukunft.

Canon ist Ihr Partner für eine sichere Druckumgebung.

SMARTSHIELD KOMPATIBEL

SMARTshield ist Teil der folgenden Systeme:

ColorWave 3600



ColorWave 3800



PlotWave 3000 Serie



PlotWave 5000 Serie



PlotWave 7500



SMARTSHIELD IM DETAIL

SICHERE ÜBERMITTLUNG

IPsec-Kompatibilität

IPsec ist ein Protokoll, dass für die Authentifizierung, Vertraulichkeit und Integrität von Daten in der Netzwirkommunikation zwischen dem Controller und anderen Systemen sorgt.

IPv6- und IPv4-Kompatibilität

IPv4 ist eines der zentralen Protokolle der standardbasierten Internetworking-Verfahren im Internet und anderen paketvermittelten Netzwerke. Es verwendet 32-Bit-Adressen. IPv6 ist die aktuellste Version. Es nutzt 128-Bit-Adressen und kann daher viel mehr Systeme ansprechen.

HTTPS

Damit beim Netzwerkverkehr über WebTools Express, Publisher Express und Publisher Select das HTTP-Protokoll nicht abgefangen oder verändert wird, kann das HTTPS-Protokoll statt des HTTP-Verkehrs mit dem Controller genutzt werden. Zusätzlich können vertrauenswürdige Zertifikate einer Zertifizierungsstelle in den Controller integriert werden. So können sog. „Man in the Middle“-Angriffe verhindert werden, bei denen Saboteure, die auf dem Pfad zum Controllerserver sind, vorgeben, der Controller zu sein.

SICHERE SPEICHERUNG UND LÖSCHUNG

Sichere Dateilöschung

Nach einer vom Nutzer festgelegten Zeit werden Druck-, Scan- und Kopieraufträge automatisch aus der Smart Inbox gelöscht. Durch Aktivierung von E-Shredding ist die Dateilöschung sicher.

E-Shredding

E-Shredding ist eine Sicherheitsfunktion, durch die das System alle Druck-, Kopier- und Scandaten nach dem Löschen überschreiben kann. Diese Funktion verhindert die Wiederherstellung von Nutzerdaten (einschl. Dateiinhalten und Dateiattributen), wenn z.B. die Festplatte gestohlen wurde.

Herausnehmbare Festplatte

Mithilfe des optionalen herausnehmbaren Festplatten-Kit können Administratoren die interne Festplatte des Systems nach Arbeitsschluss entfernen und sicher verwahren. Das Laufwerk lässt sich für die Nutzung während der Arbeitszeit einfach wieder einsetzen.

Sicheres Booten

Sicheres Booten gewährleistet, dass das System beim Booten nur vertrauenswürdige Software einsetzt. Wenn der Drucker startet, prüft die Controllersoftware die Signatur jedes Teils der Bootsoftware.

Datenverschlüsselung

Die Festplattenverschlüsselung des POWERSync Controllers verschlüsselt alle Dateien, die sich auf dem gesamten Laufwerk befinden (einschl. Betriebssystem und allen Daten; verwendete Raumverschlüsselung). Der Verschlüsselungsmechanismus basiert auf einem Trusted Platform Module (TPM) und Microsoft BitLocker-Mechanismus gemäß FIPS 140-2-Zertifizierung. Das AES 256-Verschlüsselungsverfahren wird eingesetzt.

Festplattenzerstörung zum Vertragsende

Auf Kundenwunsch kann das interne Festplattenlaufwerk des POWERSync Controllers entfernt und zerstört werden. So ist sichergestellt, dass keine Kundendaten auf dem Drucker verbleiben, wenn dieser zurückgenommen wird.

BEFUGNISSE

Bedienfeld-Zugriffssperre

Durch Aktivierung der Zugangssteuerung kann auf das ClearConnect Bedienfeld erst nach Entsperrung über die Domain-Zugangsdaten oder Smartcard zugegriffen werden.

Sicherer Druck über Domain-Zugangsdaten (Active Directory)

„Sensible“ Druckaufträge werden erst gedruckt, wenn sich der Auftraggeber am Bedienfeld des Systems korrekt ausweist und die Drucke freigibt.

Sicherer Druck über Smartcard (ausschl. Scaneinheit)

„Sensible“ Druckaufträge werden erst gedruckt, wenn sich der Auftraggeber am Bedienfeld des Systems per Wischen und Einführen der Smartcard ausweist und die Drucke freigibt.

Druckdateien nur über Ihre Smart Inbox verfügbar

Wenn man 'Direktdruck' in WebTools Express deaktiviert, ruht die Druckdatei in Ihrer Smart Inbox, bis sie über das ClearConnect Bedienteld oder WebTools Express aktiviert wird. Diese Funktion verhindert, dass Ausdrücke versehentlich von Kollegen mitgenommen werden.

Scannen an Ihren persönlichen Benutzerordner

Die Funktion 'Scannen an Ihren persönlichen Benutzerordner' ist verfügbar durch Authentifizierung per Nutzernamen und Kennwort. Nach Authentifizierung auf dem Bedienfeld des Druckers kann der Nutzer eine Datei zu seinem Hauptverzeichnis im Netzwerk scannen, wie er es für seinen Account auf MS Windows Active Directory eingerichtet hat.

Drucken über Ihren persönlichen Benutzerordner

Die Funktion 'Drucken über Ihren persönlichen Benutzerordner' ist verfügbar durch Authentifizierung per Nutzernamen und Kennwort. Nach Authentifizierung auf dem Bedienfeld des Druckers kann der Nutzer über sein Hauptverzeichnis im Netzwerk drucken, wie er es für seinen Account auf MS Windows Active Directory eingerichtet hat.

Deaktivieren von Ports und Schnittstellen

Damit Unbefugte keinen Zugriff auf den POWERSync Controller haben, können alle ungenutzten Ports und Schnittstellen deaktiviert werden

Drittanbieter-Software wie uniFLOW

Die PlotWave und ColorWave Drucker können per Clear Connect Benutzeroberfläche in die uniFLOW Umgebungen des Kunden integriert werden. Dadurch erhalten Nutzer zusätzliche Funktionen, mit denen sie die Druck- und Kopierkosten senken, die Dokumentensicherheit erhöhen und die Mitarbeiterproduktivität steigern können.



SCHUTZ VOR HACKERN

Deaktivierung ungenutzter Protokolle

Netzwerkadministratoren können bestimmte Protokolle so konfigurieren, dass sie zugänglich sind. Auf diese Weise wird eine ungewollte Systemkommunikation und der Systemzugang über spezifische Transportprotokolle wirksam blockiert.

SNMP V3

Die sichere Version von SNMP sorgt für Authentifizierung und Integrität zwischen der Network Management Station (NMS) und den verwalteten Druckern.

IEEE 802.1X-Systemauthentifizierung

Zwecks Bereitstellung eines portbasierten Authentifizierungsmechanismus (gemäß Standard IEEE802.1X) darf ein System von einer Zentralbehörde authentifiziert werden, um im Netzwerk mit den anderen Systemen zu kommunizieren.

McAfee Antivirus (optional)

Optionale Möglichkeit, McAfee Antivirus-Software auf dem POWERSync Controller als zusätzlichen Schutz gegen Viren zu installieren.

McAfee Whitelisting Application-Steuerung (optional)

Optionale Sicherheitsfunktion, aktiviert über eine Lizenz. Bei Aktivierung erstellt sie eine detaillierte Liste aller Dateien auf dem Controller und verhindert unzulässige Änderungen durch Malware, Viren oder unbefugte Nutzer. Anhand der Liste überprüft sie die Integrität der Dateien und blockiert Manipulationsversuche und unbefugte Änderungen.

HEUTE UND IN DER ZUKUNFT SICHER

Windows 10 IoT Enterprise LTSC Controllersoftware

Der POWERSync Controller im Drucker verwendet Windows 10 IoT Enterprise LTSC.

Support bis 2029 oder darüber hinaus

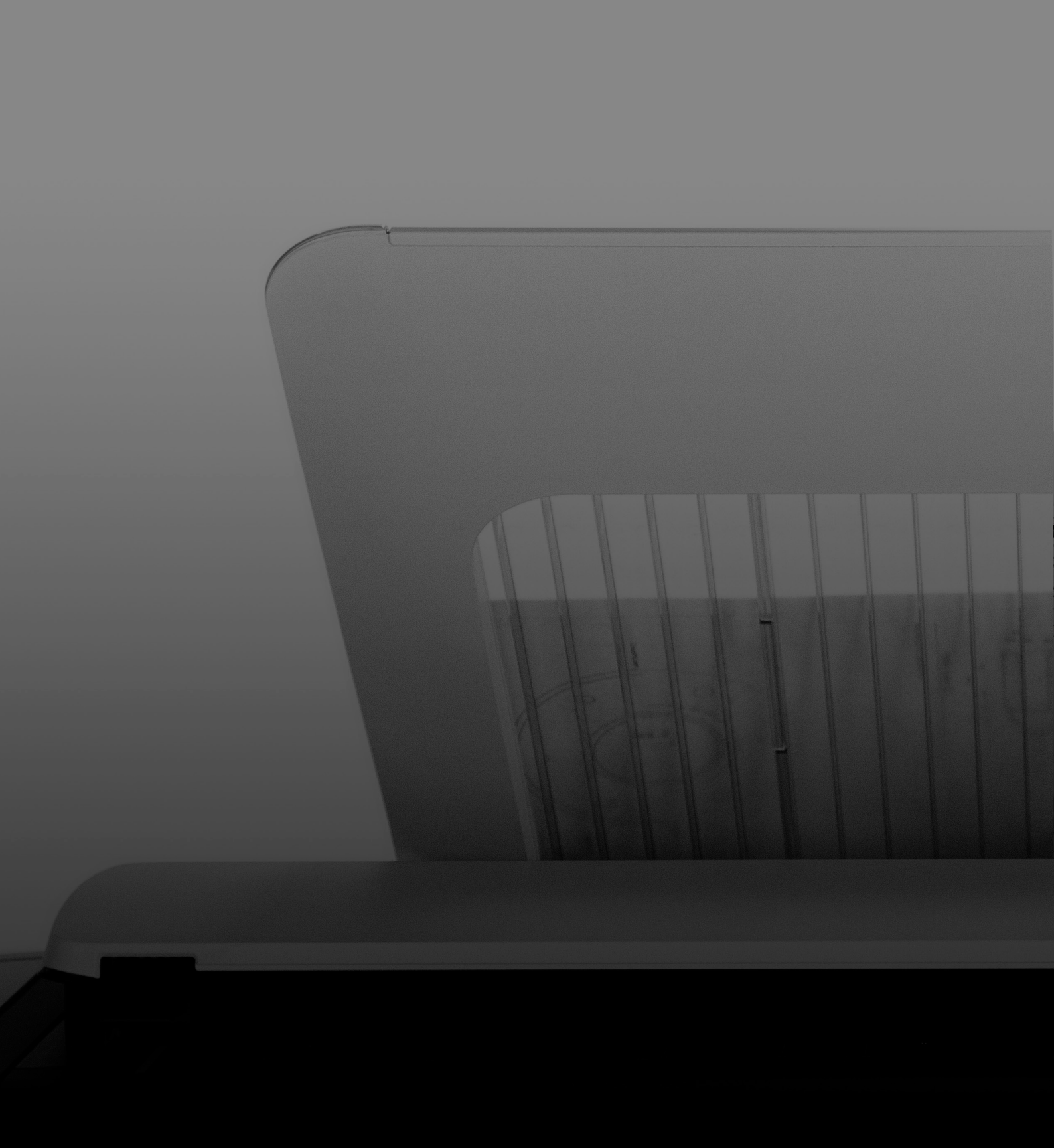
Microsoft garantiert den Support von Windows 10 IoT Enterprise LTSC bis 2029 oder darüber hinaus. Innerhalb dieses Zeitraums werden Sicherheitsupdates bereitgestellt.

Remote Controller-Sicherheitsupdates

Über WebTools Express kann der Systemadministrator per Remotezugriff Sicherheitsupdates hochladen und installieren. Dies ermöglicht ein schnelles Handeln und eine hohe Verfügbarkeit, weil kein Servicetechniker persönlich am Drucker erscheinen muss.

Remote Service

Der Remote Service von Canon gewährleistet die maximale Verfügbarkeit Ihrer Canon Systeme. Als controllerintegrierte Anwendung bietet Ihnen der Remote Service Supportdienste wie Remote Diagnose, Remote Zählerstandserfassung und Remote Unterstützung. Dadurch steigt die Systemverfügbarkeit, der Verwaltungsaufwand sinkt, und Probleme und Störungen werden frühzeitig behoben – Sie können entspannter arbeiten.



© 2020 Canon Production Printing Bestellnummer 2000144

Canon ist ein eingetragenes Warenzeichen von Canon Inc. Arizona ist ein Warenzeichen oder eingetragenes Warenzeichen von Canon Production Printing Netherlands B.V. Alle anderen Warenzeichen sind Eigentum ihrer jeweiligen Besitzer und werden hiermit anerkannt.

Diese Publikation darf nicht – auch nicht in Teilen – egal in welcher Form oder mit welchen Mitteln, weder elektronisch noch manuell oder in sonst einer Weise kopiert, verändert, reproduziert oder übermittelt werden, wenn keine schriftliche Einverständniserklärung von Canon Production Printing vorliegt. Illustrationen und technische Angaben müssen nicht unbedingt mit den Standardversionen der Produkte und Dienstleistungen auf allen Märkten übereinstimmen. Der Inhalt dieser Publikation darf weder als Garantie oder Gewährleistung in Bezug auf bestimmte Eigenschaften oder Spezifikationen noch in Bezug auf technische Leistungen oder als für bestimmte Anwendungen geeignet ausgelegt werden. Der Inhalt dieser Veröffentlichung kann sich von Zeit zu Zeit ohne vorherige Ankündigung ändern. Canon Production Printing kann nicht für irgendwelche unmittelbaren Schäden, Neben- oder Folgeschäden irgendeiner Art oder Verluste oder Kosten haftbar gemacht werden, die aus der Verwendung des Inhalts dieser Veröffentlichung entstehen.

Canon

Canon Deutschland GmbH
Europark Fichtenhain A10
D-47807 Krefeld
Canon Helpdesk
Tel.: +49 2151 3450
Fax: +49 2151 345 102
canon.de

Canon Austria GmbH
Oberlaaer Straße 233
A-1100 Wien
Canon Helpdesk
Tel. (01) 360 277 4567
canon.at

Canon (Schweiz) AG
Richtstrasse 9
CH-8304 Wallisellen
Tel. +41 (0)22 567 58 58
canon.ch
German edition