DEVELOP

Dynamic balance

www.develop.eu

Security without sacrifice

copybox
DOCUMENT SYSTEMS

GO FOR INDUSTRY-LEADING STANDARDS

It is important to be aware of the fact that today no enterprise is immune to security risks – security breaches happen everywhere, all the time! However, prudent company owners plan ahead and take the necessary precautions before the attack. By partnering with DEVELOP, the pioneer and industry leader in this field, you are taking advantage of the comprehensive range of security features available for our ineo MFPs and printers.

Conscientious managers understand that the MFPs and printers installed throughout their company can constitute the most serious of security gaps. If left unattended in the output tray, confidential information might get into the wrong hands and easily leave the company, for example via scan-to-email or fax transmission. As a security-conscious company owner or manager, you will want to ensure that your network is protected and that unauthorized access to information on the company's intranet is blocked.

At DEVELOP, we support your efforts to protect against security risks by allocating extensive engineering resources to the advanced development of security-related features for our ineo MFPs and printers. Providing our customers with the latest technology required for today's security-conscious environments, we create industry-leading standards. And thus offer you the level of comprehensive protection that our customers from all industries and public authorities rightfully expect.

ISO 15408 certification

DEVELOP devices are certified almost without exception in accordance with the Common Criteria ISO 15408 framework. These are the only internationally recognized standards for IT security testing for digital office products. Printers, copiers and software compliant with Common Criteria certification have all passed a strict security evaluation and are able to satisfy and deliver the kind of security levels that a prudent business operation seeks.

Whether you are concerned about network intrusion, data theft or compliance with regulations; or your focus is on limiting access to devices or functionalities, the innovative technology in our ineo MFPs and printers includes professional solutions for the detection and prevention of security breaches. Our ineo devices can help you keep your data where they belong, thanks to:

Access control

In both public and corporate domains, MFPs are still frequently ignored as posing possible security risks. While some dangers are perhaps identified, they are often simply neglected, especially concerning confidential documents and information. Preventive measures must include controlled access to devices as well as a viable security policy that does not diminish the systems' user-friendliness. The DEVELOP range of security features has various solutions for this.

Document and data security

Beware of unauthorized access to MFPs installed in public areas – implementing appropriate data security policies is essential here. After all, sensitive data stored on the MFP hard disk over a period of time as well as confidential prints left in the MFP output tray are not protected and might easily fall into the wrong hands. DEVELOP offers a comprehensive range of tailored security measures to curb any such attempts and ensure complete document and data security.

Network security

Within your corporate network, our printers and MFPs act as sophisticated document processing hubs that scan, print and copy documents to network destinations, or send data via email. Office technology from DEVELOP is subject to the same security risks as any other networked device. Which is why we ensure that all our equipment complies with the strictest security standards and offers multiple features against potential security leaks that might attempt to use your network connection.

Cyber security

Connected to networks, MFPs are possible gateways to a threatening digital environment. Unprotected devices open up an easy path for anyone out to corrupt, wipe out or steal corporate data. Any information, whether employee data or else, as well as your company's intellectual knowledge, may be subject to cyber attacks. With our unique virus scanning solution developed in cooperation with Bitdefender®, we offer you all-encompassing protection for your MFP fleet.

copybox
DOCUMENT SYSTEMS

KEEP DATA WHERE THEY BELONG – ACCESS CONTROL

With their advanced functionality, today's MFPs can easily be misused to copy and distribute confidential information within and beyond actual and virtual corporate boundaries. The logical consequence must be to prevent access from anyone not authorized, and to complement this with strict security measures governing the actual use of devices. At DEVELOP, we achieve this without restricting the user-friendliness of your equipment in any way.

copybox
DOCUMENT SYSTEMS

User authentication:

Start by setting down a policy defining and configuring individual users and user groups allowed to use a device. You can specify individual limitations to access rights, such as restrictions to colour printing. The authentication information is either stored on the MFP (encrypted) or uses existing data from the Windows Active Directory. Three basic technologies for users to log on are available:

- **Personal password:** Users have to enter their individual alphanumeric code with up to 8 characters at the MFP panel. Administrator and user passwords can be created and centrally managed.
- **ID card authentication:** Most DEVELOP devices can be fitted with an ID card reader that offers enhanced user convenience and speed; users no longer need to manually enter a code.
- **Biometric finger vein scanner:** The biometric characteristics of the finger vein are almost impossible to falsify, which makes this form of identification extremely reliable. Comparing the image of the scanned-in finger vein patterns with those in the memory, our state-of-the-art technology is an advance on the more common fingerprint scanners. Users don't need to remember passwords or carry cards.

Account tracking:

Using the data collected from users logging on and off enables efficient monitoring at a various of levels (e.g. user, group and/or department, the frequency of functions used, etc.). Offering enhanced transparency, analysis and trending of this data provides robust information about MFP usage from a number of different viewpoints: the data can be applied to ensure compliance and trace unauthorized access; usage can be monitored across the entire fleet of printers and MFPs in a corporate, business, or office landscape.

Individually restricted access:

Access to various MFP functions can be limited on an individual user basis. Our entire range of access control and security functions not only provides greater security against threats that might result in financial and reputational damage; the functionality can also help ensure better governance and enhanced accountability.

Log information:

Monitoring the access and usage of individual devices not only enables the immediate detection of security breaches; it also facilitates accounting and cost allocation to users and departments: Administrators can individually review audits and job logs for various device functions. Also, DEVELOP print controllers have electronic job logs that record all print jobs sent to the output device. And our very own Job Log Utility provides comprehensive electronic tracking of all user activities.

NO MORE LOOPHOLES DOCUMENT & DATA SECURITY

Countless MFPs and printers are located in public areas without restricted access. This makes the implementation of an appropriate data security policy essential. To avoid critical information falling into the wrong hands, DEVELOP offers various security measures that ensure complete document and data security.

Secure print:

There is no easier way for anyone unauthorized to gain access to confidential information than grabbing it lying unattended in a printer output tray. The secure print feature ensures document confidentiality by obliging the print originator to protect the print file with a password and entering this at the output device immediately before printing.

Printing with individual authentication:

Touch & Print needs authentication via finger vein scanner or ID card reader while ID & Print requires user authentication via ID and password. The print job is output only after the user has thus authenticated at the MFP. The advantage here is the speed: there's no need for additional security print ID and password.

No unauthorized copying:

The copy protection feature adds a watermark to prints and copies during printing. Hardly visible on the original print, the watermark moves into the foreground on any copy of the original document.

Control via Copy Guard:

With Copy Guard/Password Copy, a concealed security watermark is added to an original print to prevent this from being copied. While barely visible on the protected original, the security watermark blocks ineo devices from copying such documents. Only the Password Copy feature can override Copy Guard and allow copies to be made when the correct password is entered at the MFP panel.

copybox
DOCUMENT SYSTEMS

Smart PDF encryption:

Encrypted PDFs are protected by a user password: Permission to print or copy the PDF and permission to add PDF contents can be configured during the scanning phase at the MFP.

PDF digital signature:

This useful feature adds a digital signature to the PDF during scanning and thus allows monitoring any changes to the original PDF content.

User box security:

Available for single users as well as groups, user boxes allow for any document to be securely stored on the MFP hard disk before output of the print or copy job. User boxes are protected with an eight-digit alphanumeric password that needs to be entered to access/view the documents in the box.

Secure fax reception:

When activated, any faxes received are kept safe in a protected user box.

HDD/SDD security:

Hard disks and memory on MFPs retain many gigabytes of confidential data collected over long periods. In DEVELOP systems, a number of complementing features ensure the safekeeping of such sensitive corporate information:

- Auto delete – Data stored on the hard disk are automatically erased after a set period.
- HDD/SDD password protection – Any read-out of data stored on the hard disk requires password entry, with the password linked to the device. Data are therefore no longer accessible once the HDD/SDD is removed from the device.
- HDD* overwriting – The most secure method of formatting a hard disk is by overwriting stored data. This is performed in accordance with a number of different methods conforming to various (e.g. military) specifications.

HDD/SDD encryption:

HDDs/SDDs in DEVELOP devices can be encrypted using the Advanced Encryption Standard (AES); this supports a 256-bit key length and satisfies corporate data security policies. After encryption, the data on the HDD/SDD cannot be read or retrieved, even if the HDD/SDD is physically removed from the MFP.

PROTECT COMMUNICATION INSIDE & OUT – NETWORK SECURITY

DEVELOP's office devices are based on a concept of communication and connectivity. This complies with strict security standards concerning user access, encryption of data and protocols used for information transmission. Trust us to ensure that your data will get to the desired destination securely and will not be tampered with.

User authentication:

Besides governing access to output devices, the need to authenticate with a unique user ID and password prevents unauthorized users from accessing the network. The feature can be configured to authenticate to the network or directly at the MFP or printer.

SSL/TLS encryption:

It protects communication to and from output devices, covering online administration tools, the Enterprise Server and Active Directory transmissions, etc. This communication type prevents from man-in-the-middle attacks where the attacker would be able to record the data communication.

DEVELOP devices support IPsec for the complete encryption of any network data transmitted to and from the MFP. The IP security protocol encrypts the entire network communication between the local intranet (server, client PC) and the device itself.

IP address filtering:

An internal basic firewall provides control of protocol and port access as well as IP address filtering, which can be set at the machine: the MFP's network interface card is programmed to only grant access to a specific IP address range from client PCs.

Secured ports and protocols:

In the administration mode at the machine or remotely via Web Connection or Device Manager, ports and protocols can be opened, closed, enabled and disabled. The administrator mode itself is accessed by a 16-digit alphanumeric password that can only be changed by the service engineer or administrator. If required, a web interface closing functionality also allows the disabling of the web interface for all users.

SMTP authentication:

Ensuring advanced email security, SMTP authentication (Simple Mail Transfer Protocol) will authorize a machine to send email when activated. Companies not hosting their email services can use an ISP mail server. For secure communication, it is also possible to combine POP before SMTP, APOP, SMTP authentication or encryption using SSL/TLS.

S/MIME encryption:

To secure email communication from the MFP to certain recipients, the system supports S/MIME (Secure/ Multi-purpose Internet Mail Extensions). S/MIME encrypts the email message and content with a security certificate. Opening S/MIME encrypted emails requires the decryption key (private key).

Changing "From" address:

When user authentication is activated, it is not possible to change the 'From' address; it will always be the logged-in user's email address. This feature prevents spoofing and provides audit trails for administrators.

Manual destination prohibit:

This function bars the direct input of an email address or scan destination; only registered destinations from the internal system address book or LDAP can be chosen.

Fax line security:

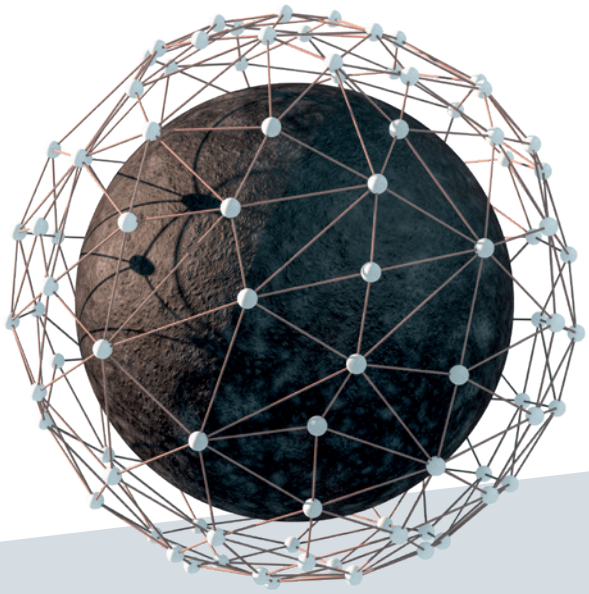
Using only the fax protocol for communication – no other communication protocols are supported – provides advanced fax line security. DEVELOP devices block any intrusion attempts as threats, including intrusions of a different protocol over public telephone lines, as well as any attempt to transmit data that cannot be decompressed as fax data.

Fax rerouting:

Incoming faxes can be automatically forwarded to any destination within the internal address book including email addresses, or to the user boxes on the device's internal HDD. Storing incoming faxes in a user box is considerably safer; printed faxes are not left in the output tray. Rerouting also speeds up communication, as faxes reach recipients sooner. And it helps to save paper – the recipient can decide whether the fax needs to be printed.

Network access control:

Most DEVELOP devices support the IEEE802.11x standard for network access control to WANs and LANs. The standard secures the network by shutting down any network communication (e.g. DHCP or HTTP) to unauthorized devices, with the exception of authentication requests.



copybox
DOCUMENT SYSTEMS

ALWAYS ONE STEP AHEAD OF THE ATTACK – CYBER SECURITY

Today's workplaces and work styles have changed; and threats are continually increasing. This is why DEVELOP's latest devices employ unique Bitdefender® anti-virus scanning technology. Its highly sophisticated real-time scanning goes far beyond common security standards. This is how we ensure that your MFPs cannot be harnessed as gateways for potential attacks.

These days, our customers use their DEVELOP MFPs as IoT devices – usually connected, they process and print information from the cloud, not just from the installed applications. In today's hugely changed office environment, we all face ever more threats: Between 2006 and 2019, data breaches increased by 130%[1] – with extreme consequences. The total cost of a successful cyber attack is estimated at over 4.6 million Euros or 280 Euros per employee[2]. The reputational damage and information loss can be even worse. And the future is likely to present further challenges, with 230,000 new malware samples produced every day – plus the prediction that such threats will continue to grow rapidly[3].

Bitdefender® real-time scanning:

Most likely, you and your team print from different applications and various mobile devices. With Bitdefender® real-time scanning, it does not matter where a job comes from or what type of file is printed or faxed. All incoming and outgoing files are scanned, without any disruption whatsoever to using the device. If a threat is detected, the MFP will inform you accordingly.

Periodic & manual scanning:

Enhancing security standards further, periodic scanning times can be set up on DEVELOP MFPs. In line with individual requirements, your devices can be set up to scan on a daily, weekly or monthly basis. This scanning functionality also covers SMB share folders as well as device and S/MIME certificates. Of course, if you need a scan right away, you can still start the manual scanning process and will get your scan immediately.

Automatic Bitdefender® updates:

Bitdefender® updates the MFP database every 4 hours with the latest information to ensure that our devices remain capable to always identify even the newest threats. Furthermore, with Bitdefender® you can track on each device the time of the last information upload, when the last manual/periodic scan was performed, and when the last risk/threat was detected.

1 https://www.bluefin.com/bluefin-news/highlights-ibm-security-ponemon-institutes-2019-cost-data-breach-study/
2 Ponemon
3 Panda Security

copybox
DOCUMENT SYSTEMS

SECURITY AS THE KEY ELEMENT OF OUR OVERALL STRATEGY

At DEVELOP, we take pride in our position as market leader as well as being a strong and experienced partner for our customers in all matters of security. In 2019, Quocirca recognized DEVELOP as a company for which “security is one of the key pillars underpinning its managed print services offering. DEVELOP has adopted an ITIL-based methodology designed to improve security and compliance, and believes that organizations that treat the procurement of MPS services as the start of an ongoing consultative relationship with their provider rather than as a one-off transaction will benefit the most, particularly in the face of continually evolving security risks.“

Source: Quocirca Global Print Security Landscape 2019; Quocirca; 2019;

copybox
DOCUMENT SYSTEMS

DEVELOP

Konica Minolta Business Solutions Europe GmbH
Europaallee 17 30855 Langenhagen Germany Phone +49 511 7404-0 www.develop.eu

copybox
DOCUMENT SYSTEMS