uniFLOW online

ZERO TRUST MEETS UNIFLOW ONLINE

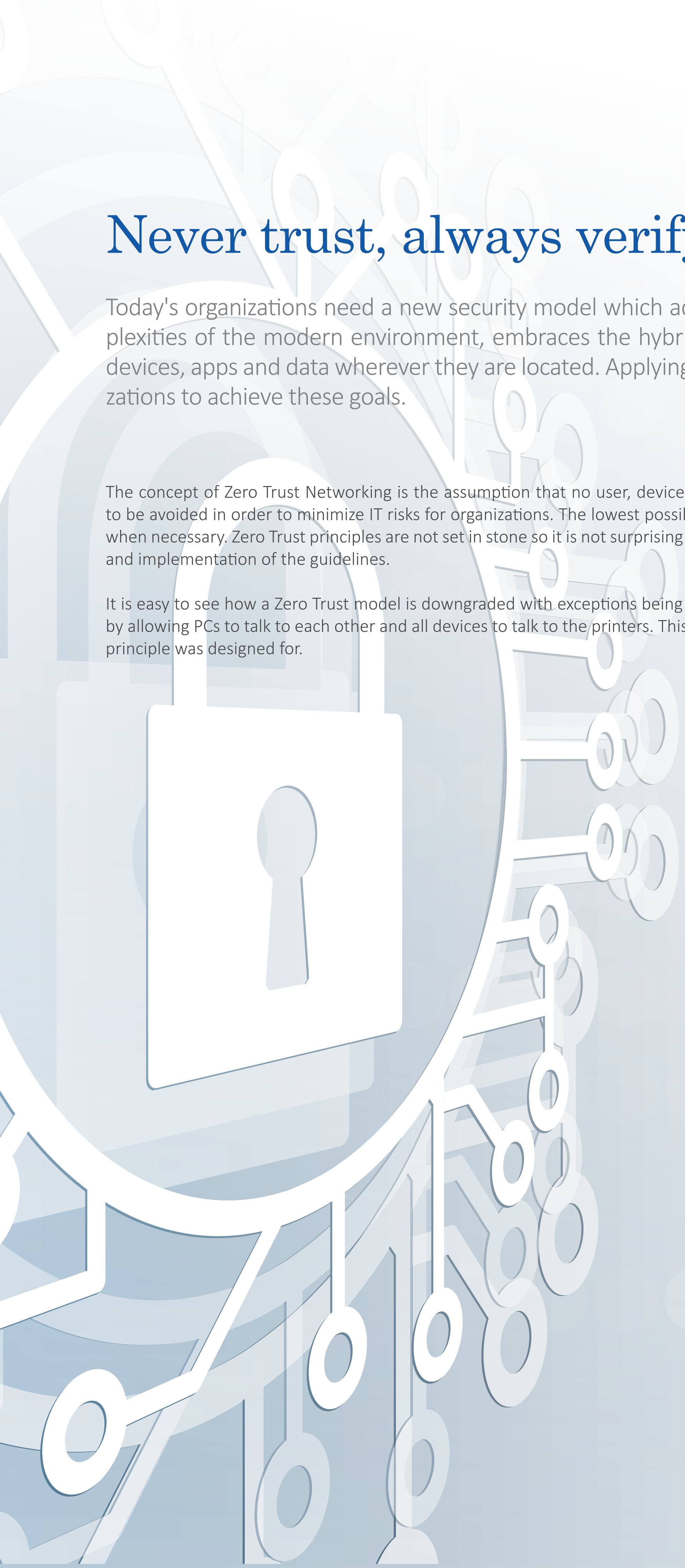
www.uniflowonline.com

Never trust, always verify

Today's organizations need a new security model which adapts more effectively to the complexities of the modern environment, embraces the hybrid workplace and protects people, devices, apps and data wherever they are located. Applying Zero Trust principles helps organizations to achieve these goals.

The concept of Zero Trust Networking is the assumption that no user, device or service can be trusted. Unfounded trust is to be avoided in order to minimize IT risks for organizations. The lowest possible authorizations and access are granted only when necessary. Zero Trust principles are not set in stone so it is not surprising that there are different views on the definition and implementation of the guidelines.

It is easy to see how a Zero Trust model is downgraded with exceptions being made to the network, to incorporate printing, by allowing PCs to talk to each other and all devices to talk to the printers. This is the opposite of what the original Zero Trust principle was designed for.



Industry-leading Zero Trust principles

Zero Trust is not a product or software. Zero Trust is a security principle for organizations to adhere to so that information security is guaranteed. Since there is no universal definition of Zero Trust, organizations can interpret the term as they see fit. This leads to a wide variety of benchmarks because not all organizations give the same priority to data security. Following market and industry leaders, such as Microsoft and Google™, on their Zero Trust journey empowers organizations to build their own guidelines.

Previously the Microsoft cloud services, such as the Microsoft Azure cloud, were already one of the safest places to store data online. Now, with Zero Trust[1] becoming the cutting-edge data security principle[2], Microsoft has defined its own guidelines[3]:

1. Verify explicitly

Always authenticate and authorize based on all available data points.

2. Use least privileged access

Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.

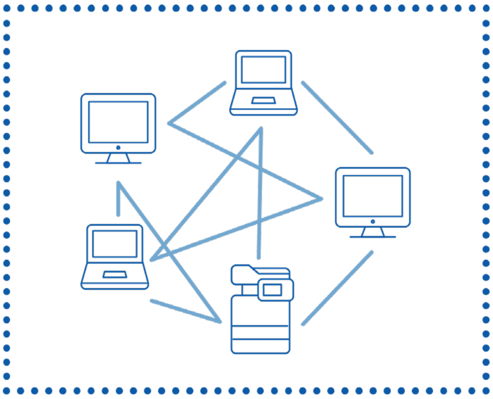
3. Assume breach

Minimize blast radius and segment access. Verify end-to-end encryption and use analytics to get visibility, drive threat detection, and improve defenses.

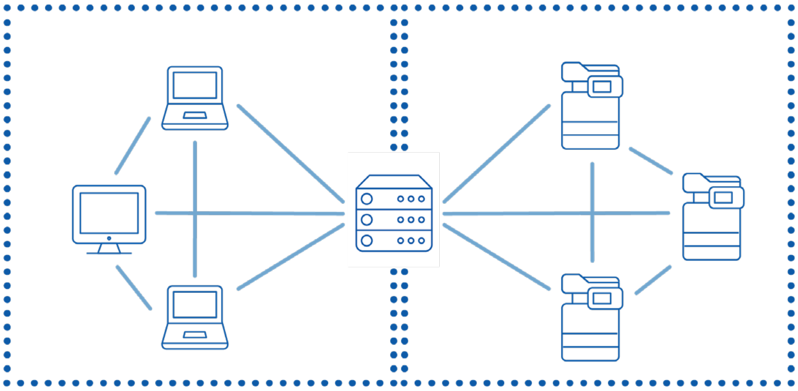
[1] https://www.microsoft.com/en-us/security/business/zero-trust
[2] https://www.microsoft.com/security/blog/2021/01/19/using-zero-trust-principles-to-protect-against-sophisticated-attacks-like-solorigate/
[3] https://www.microsoft.com/security/blog/2021/06/30/the-critical-role-of-zero-trust-in-securing-our-world/?culture=en-us&country=US

Challenges of printing in a Zero Trust environment

When organizations talk about applying Zero Trust principles to protect their infrastructure, printing might not be the first thing that comes to mind. However, if the Zero Trust implementation does not include the printing and scanning infrastructure, things can rapidly fall apart.



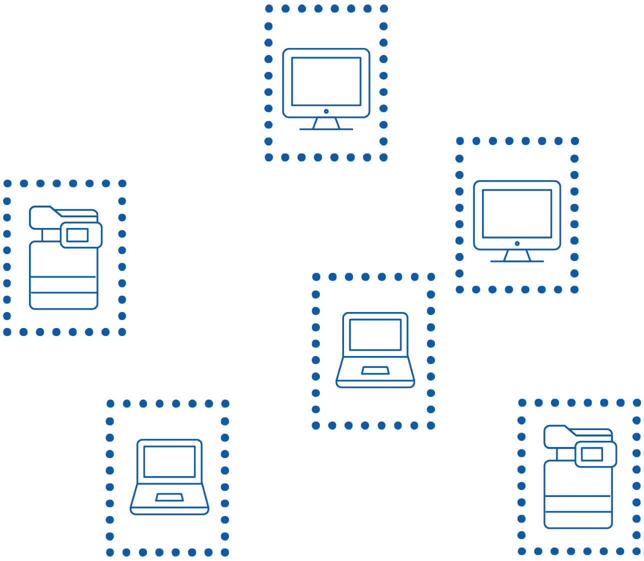
No Zero Trust network segmentation



Partial Zero Trust network segmentation with separate VLANs

In the traditional office, PCs and printers are typically all on the same network or split into different virtual networks (VLANs) with a print server bridgeing the gap. However, in a Zero Trust model, as part of the 'assume breach' principle, the 'blast radius' of a potential breach is reduced by isolating each network endpoint as much as possible from all other network points. This can also mean that internet access is only available from the internal network, i.e., no other communication routes are allowed. Should one PC become infected or compromised, it cannot spread because it cannot 'talk' to anyone else.

With a full Zero Trust micro segmented network, companies are not only securing their business-critical data, but they are also able to remove their local on-premise infrastructure to free capital bound in server hardware, maintenance, and IT services.



Full Zero Trust network micro-segmentation.

Adopting industry-leading principles

Due to the close collaboration with Microsoft, uniFLOW Online being hosted within the Microsoft Azure cloud and the effortless integration of Microsoft services into uniFLOW Online, the Zero Trust principles of uniFLOW Online were developed in accordance with the principles defined by Microsoft:

1. Verify explicitly

All users connect to uniFLOW Online using their existing login credentials such as Azure AD, Google Workspace™ or OKTA. This includes full support for multi-factor authentication and other policies defined by the IT department.

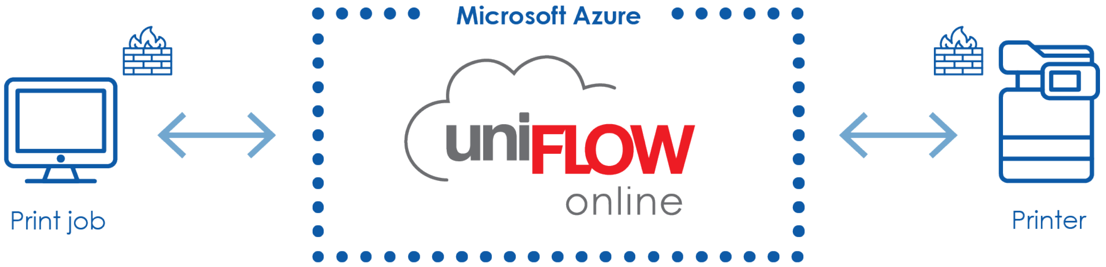
2. Use least privileged access

Multiple levels of privileged access are available so different users can only access the parts of uniFLOW Online applicable to their role e.g. maintenance staff have no insight into user data, neither do budget managers have access to the rest of the system.

3. Assume breach

All communications and the print path can be made via the internet. No lateral connections between PCs and printers are required on the internal network. All communication and print traffic is encrypted.

Since the launch of uniFLOW Online, security has been one of the focal points during the development process. Users use personal secured print queues, allowing them to print from any location using any device, and their encrypted print jobs are stored in the local Microsoft Azure data center from where they are released when needed.



Perfect match - uniFLOW Online and Canon devices

Canon devices connected to uniFLOW Online, such as the Canon imageRUNNER Advanced DX, Canon imageCLASS or i-SENSYS, are the perfect match for the implementation of industry-leading Zero Trust principles. The only thing the printer needs is a power supply and internet connection.

Great flexibility

- 100% cloud-printing, or local job storage – uniFLOW Online supports it
- Print securely from desktop PCs, mobile devices, cloud storage services and BYOD
- Collect print jobs at any device with My Print Anywhere and modify documents on demand before releasing

Superior security

- No need for local infrastructure, such as clients, Edge mesh, Edge nodes, servers, boxes, VPNs, or hubs
- Operates within any network configuration, such as Zero Trust networks
- Secure printing, using personal secure print queues and restrict device access to authorized personnel only, is fully compliant with the Zero Trust

Gain control

- Allow access only to priviledged user, based on defined rules and following Zero Trust guidelines
- Isolate every device to ensure network security is not compromized

Eliminate risks

- Remove all local print servers, without compromising performance or security
- No capital tied up in server hardware and maintenance
- More than 99 % uptime in the cloud and always the latest software version

www.**uniflow**.global
www.**uniflowonline**.com

V2 | January 2022