Security Compliance Checklist

A practical list to secure endpoint devices in your network.

New regulations are requiring businesses to increase their focus on IT security to ensure valuable customer and company data is protected. In addition, directives, like the EU General Data Protection Reform (GDPR), require businesses to assess, monitor and report on security breaches within days.

With regulations constantly changing, it can be challenging for businesses to find the time and resources to keep up. However, if they fail to offer more than a simple firewall as a guard against attacks, they could be breached and face fines that run into the millions. There's no doubt that every business will experience a breach at some point, so it's essential to identify when it happens and correct it as soon as possible with the right products, processes and tools.

This checklist is a practical resource for those looking to improve their IT security and protect their brand reputation, avoid the costly consequences of a breach and comply with strict new regulations. Starting off with the basics, work your way down the list to maximum security layers and you can be confident that your endpoint security is aligned to these strict new regulations.

This handy checklist will also help your IT department to secure their printer endpoints.

Basic security layer

- Only purchase devices with built-in malware protection and encrypted hard drives
- Update firmware, especially versions with critical security patches – as you would when you update the apps on your mobile phone
- Configure device interfaces, and lock down protocols like FTP and telnet which are not required by your applications
- Review new devices and close ports or protocols not currently in use that could give intruders access
- Apply unique administrative passwords to each device
- Lock-down the front panel to disable access to administration features
- Encrypt data flowing to and from the device
- Set hard disk erase procedures for old data – especially on printers you are trading in

Once this is complete, move onto the next layer of security.

Medium security layer

- Integrate printer systems' log data into your SIEM tool to more fully monitor the network for threats. For new compliance regulations, visibility is key to meet the reporting requirements
- Deploy user authentication at the printer to track who's copying, scanning, faxing from the device. This data is helpful in a forensics investigation after a breach
- Deploy pull printing to avoid sensitive information being forgotten. This also helps your environmental standards by reducing wasted prints

Once this is complete, move onto the final layer of security.

Advanced security layer

- Set-up job tracking and accounting reporting
- Consider setting and automatically enforcing rules regarding who can access and use which printers and why with role-based authorisation
- Deploy unique digital certificates to each printer as you would other internet connected devices on your network
- Deploy a managed mobile printing solution for data encryption, in-network device access, user authentication and tracking

4AA7-1093EEE