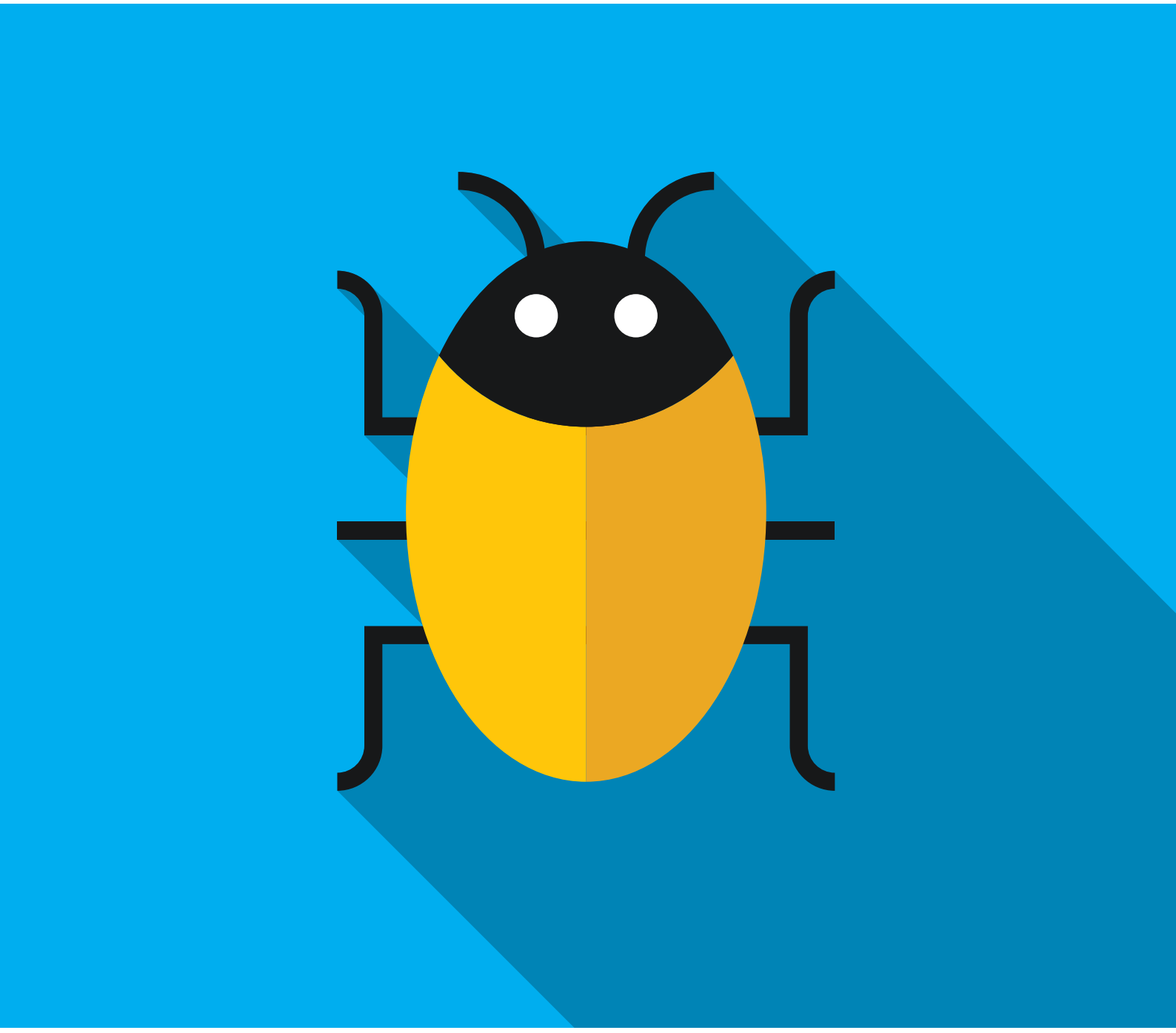
Prinect

Technical White Paper
Cyber Attack Protection.



HEIDELBERG

Anti-Virus
Is your Prinect Workflow safe?

Security is a key concern of today's digital world. Fully protecting your business requires a multi-prong approach. One of those prongs is employing Anti-Virus software at your workstations and servers and, nowadays, your firewall. Often, running Anti-Virus software can consume CPU cycles and use up memory – typically negatively impacting Disk I/O and Network I/O, which are critical components of Heidelberg's Prinect® Workflow. You should perform testing before and after you install your Anti-Virus software to determine whether there is any performance effect on your computers running Prinect Workflow software.

A virus infestation can lead to destroyed or lost data, stolen confidential information, unplanned downtime, and ultimately, system degradation. As a result, you are forced to spend both time and money to identify and eliminate the cause and prevent future attacks. In extreme cases, the virus could propagate outside of your business – to customers, vendors, or to one of your employee's home computers.

This paper is intended to provide guidance on how to best apply/incorporate Anti-Virus software into your Heidelberg Prinect Workflow. Please note that any implementation or interpretations of the concepts discussed in this document are solely the responsibility of the customer. Heidelberg assumes no responsibility for a particular printer's security. In addition, the guidelines are subject to change as the threat landscape evolves.

How Prone Are You to Being Infected? What Should You Consider?

1. Are you protected across your shop? Protecting your Heidelberg Prinect Workflow products is just not enough.
2. Are you using your Prinect Workflow servers to surf the web or for accessing e-mails, especially non-business e-mails? These are products designed to perform a core business function and should be treated as "mission critical" products. They should not be used casually for generic computing needs.
3. How do you accept jobs from your Print Buyers? If you are using a FTP server, your risk is probably a lot higher than using a more secure method. If you are accepting CDs/DVDs or USB sticks, consider first bringing them in on an off-line workstation and then move them onto your production network.
4. Do you have employees that bring their own devices to work and connect them to your plant network? These could also make your systems vulnerable.

Can I use Anti-Virus Software with Prinect Workflow Products?

From a prepress perspective, not only can you use Anti-Virus software on your Prinect Workflow products, but Heidelberg USA strongly recommends that you do use it for our prepress products as well as throughout the rest of your plant. You should keep the software and Virus Definition files (DAT) up-to-date to prevent "Zero-Day" attacks. For guidance on press and postpress products, please refer to those support resources.

What Anti-Virus Software does Heidelberg Recommend?

Heidelberg USA, Inc. does not sell or support any Anti-Virus software, and, thus, cannot recommend a specific product or vendor. Different printers have established different standards for their plant. Anti-Virus is not our core business, and we leave that to the experts.

The most common software we see used is Symantec™ Endpoint Security, McAfee™ Endpoint Security, Trend Micro™ and Kaspersky™ Anti-Virus for Windows™, Microsoft® Windows Defender and freeware like ClamAV® and AVG™. When you choose to run Anti-Virus software, it is an all or nothing scenario: you must run it on all of your workstations and servers. Some customers will only choose select workstations or servers to protect. This strategy is flawed as it still leaves your systems vulnerable to attack.

Some customers believe in layering their virus protection by using different vendors' products on their servers and workstations. The logic is that one software may catch something that another does not. However, with one consistent User Interface, there is only a single point for support and updates.

What approach should I use?

The answer: one you feel most comfortable with.
If you have a Next-Generation Firewall (NGFW), such as the SonicWall® Network Security Appliance (NSA), we recommend licensing their Gateway Anti-Virus (GAV) option as part of your comprehensive security. With GAV, files are analyzed in real time; and, when a threat is detected, those threats are blocked at the gateway. Your users are prevented from ever downloading malware initially, and your network administrator receives notification.

Protecting your Workflow
Prepare for it, before it happens.

Printers, like any business, need to ensure they are proactively preventing breaches before they happen and improving their readiness in the event of an attack.

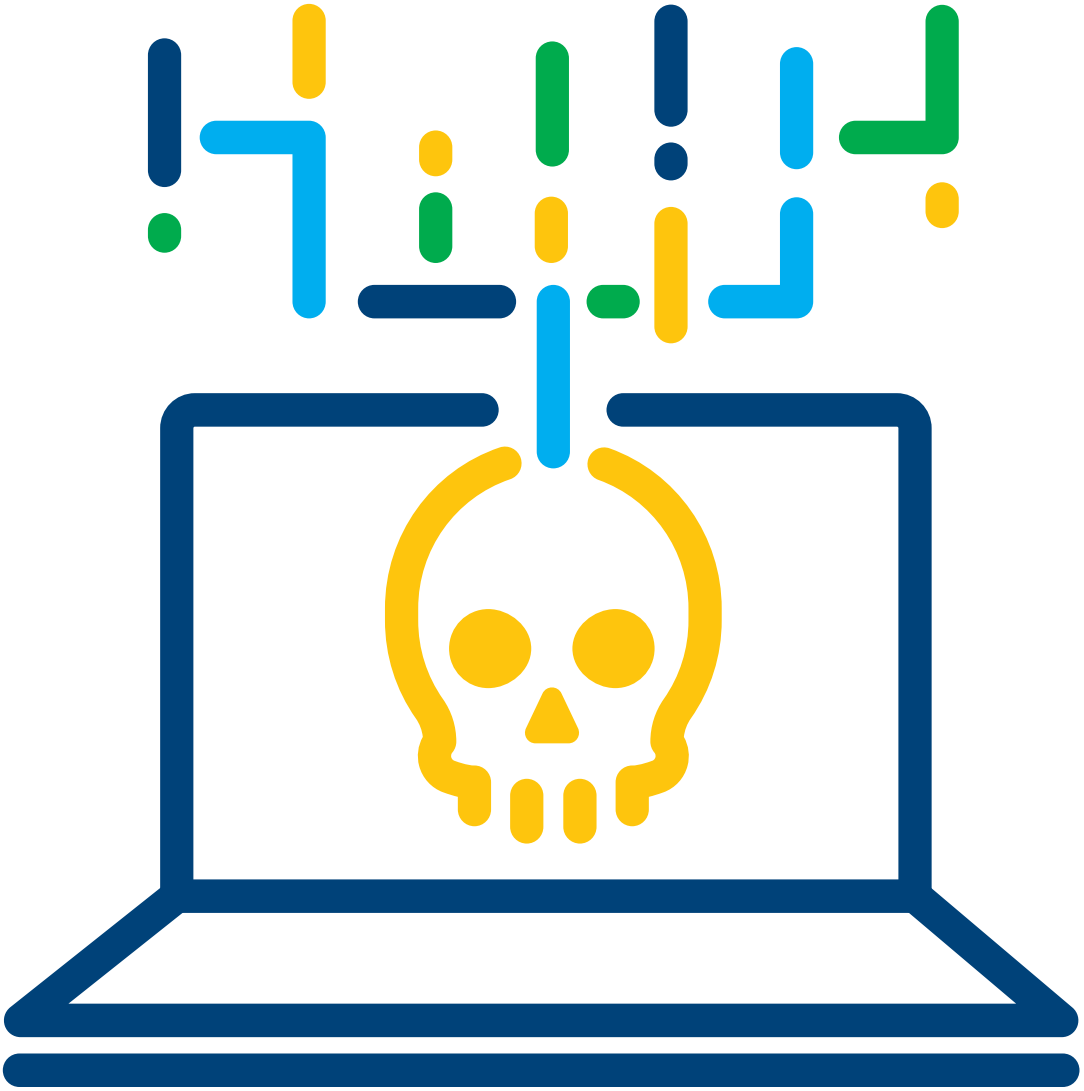
What Settings should I use?

Each product has its own particular user interface; however, there are features and terminology that are common to all products, regardless of vendor.

With Anti-Virus software, you should:

- Scan local drives only; not network-attached drives
- Consider disabling the heuristics mode of scanning which can be very intensive on the system.

Before changing any settings, you should consult your System Administrator to ensure there are no existing standards for your plant.



Exclusions:

What Exclusions should I add?

Each Prinect Server product has its own user interface, however, there are common features and terminology. These general settings should be useful regardless of the product you use. The list below gives the exclusions for specific servers.

SERVER	EXCEPTIONS

MS Windows Server 2019	For the Operating System, Heidelberg provides no direct guidance for anti-virus settings nor have we received specific complaints from customers about settings directly related to Prinect; however, Microsoft Corporation provides guidance at this link: **http://support.microsoft.com/kb/822158/en-us**
	• Turn off scanning of Windows Update related files:
	  • In the folder C:\Windows\SoftwareDistribution\Datastore\ exclude the file DataStore.edb This is the Windows Update database.
	  • In the folder C:\Windows\SoftwareDistribution\Datastore\Logs exclude the following files: Edb*.jrs, Edb.chk, and Tmp.edb The asterisk (*) is a wildcard character meaning that there may be several files.
	• Turn off scanning of Windows Security files:
	  • In the folder C:\Windows\Security\Datastore\ exclude files with the extensions: .Edb,sdb, .log.chk, and Tmp.edb The asterisk (*) is a wildcard character meaning that there may be several files.
	• Turn off scanning of Group Policy related files:
	  • In the folder C:\Windows\System32\GroupPolicy\Machine exclude the file Registry.pol
	  • In the folder C:\Windows\System32\GroupPolicy\User exclude the file Registry.pol
	Unless you are experiencing issues, it is not recommended that any exclusions be applied.

MS SQL Server 2019	For the database, again Heidelberg provides no direct guidance for anti-virus settings nor have we received specific complaints from customers about settings directly related to Prinect; however, Microsoft Corporation provides guidance at this link: **http://support.microsoft.com/kb/309422**
	• Turn off scanning the SQL Server process:
	  • In the folder C:\Program Files\Microsoft SQL Server\MSSQL11.HEIDB\MSSQL\Binn\ exclude the file SQLServr.exe
	  • In the folder C:\Windows\SoftwareDistribution\Datastore\Logs exclude the following files: Edb*.jrs, Edb.chk, and Tmp.edb The asterisk (*) is a wildcard character meaning that there may be several files.
	• Turn off scanning the SQL Server process:
	  • In the folder E:\SQLDATA\MSSQL11.HEIDB\MSSQL\DATA exclude the database and transaction log files:
	  *.mdf
	  *.ldf
	  *.ndf
	Unless you are experiencing issues, it is not recommended that any exclusions be applied.

Prinect 2020	• Turn off scanning log files, for example, the folder: E:\HD_Service\Logs\ • Turn off scanning the SQL Server process: Please note that if you are using a Reverse Proxy in conjunction with your web-based Prinect applications, you do not need to install Anti-Virus software on the Reverse Proxy. This does not store any data in the file system but redirects network traffic.

Summary:

Establish a standard for your plant. Take security seriously, be continuously vigilant and have a plan that includes Anti-Virus protection.

Why are these things important?
They will help protect your assets by minimizing your exposure to breaches or their consequential periods of downtime. Additionally, they will better secure your customers and employees sensitive information and data. When it comes to security, it is better to proactively prevent breaches before they happen and improve your readiness in the event of an attack. Being well informed helps set expectations correctly and makes sure you get the best Return On Investment (ROI) and the lowest Total Cost of Ownership (TCO) on your Prinect Workflow systems. Heidelberg does offer consulting services, training services and technical services that can help Print Shops identify their security holes and better protect their business. Please contact your Account Manager for more information.

To view or download all of our Technical White Papers visit: https://news.heidelbergusa.com/whitepapers/

Please direct any questions regarding this document to Eugene F. O'Brien, Senior Technical Support Analyst at:
(770) 794-6205 or
eugene.obrien@heidelberg.com

Heidelberg USA
1000 Gutenberg Drive
Kennesaw, GA 30144
Phone 800 437 7388
info@heidelberg.com
www.heidelberg.com/us