Windows 10 Is Coming, Ready or Not

Windows 10 is moving into the enterprise. When it moves into yours, we urge you to seize the opportunity to future-proof your terminal emulation software at the same time. This paper tells how you can expect to encounter Windows 10 (hint: it's different from other Windows updates)—and how you can strengthen mainframe security by making terminal emulation a part of your security strategy.

Key Shipping and Support Dates

- **November 2016:** Dell, HP, and Lenovo stopped shipping Windows 7 and 8 with their PCs.
- **January 2017:** Dell will ship only Intel Kaby Lake processors, which require Windows 10, with their PCs.
- **January 2020:** Microsoft Windows 7 Extended Support ends, which means there will be no more security updates.

Why You Should Pay Attention to Windows 10

With the enterprise version of Windows 10, Microsoft is taking a more aggressive approach to its upgrade campaign. The company has stated that it won't support Windows 7 or 8 on the new Intel Kaby Lake (7th generation) and AMD Zen processors. Desktops and laptops using these processors, including Dell, will support only Windows 10. Important note: Starting January 2017, Dell will ship only Intel Kaby Lake processors.

Windows 10 also marks the start of a new way to build, deploy, and service Windows—called Windows as a Service, which is a continuous delivery model. Unlike the consumer versions of Windows 10, enterprises will now be able to control when operating system updates are applied to their environments. Once customers install Windows 10, they will be registered with Microsoft to receive rolling feature additions, improvements, and updates for free.

This new delivery model is a good thing, unless you’re not on Windows 10—because Windows 10 may represent the last major Windows release ever.

How Does Your Terminal Emulation Garden Grow?

Many of our customers tell us that they have lost control of their terminal emulation environments. Like weeds in a garden, multiple versions, nonsecure macros, rogue emulation clients, nonstandard configuration files, and other IT undesirables have taken over. If you find yourself in that position, your move to Windows 10 provides the perfect opportunity to regain control of your terminal emulation environment—to pull the weeds, standardize your configurations, and firmly secure the clients that access your most critical data and systems.

We all know that mainframe systems and applications remain vital to the enterprise. But the cost and complexity of changing them to work...
with modern security requirements, productivity tools, web technologies, and mobile devices can be daunting—even if you have the necessary skills. When adopting a new technology like Windows 10, the last thing you want to do is modify an essential mainframe application that has been around for decades to make your systems work together.

Desktop migrations are notoriously complex and expensive—especially for widely deployed applications like your terminal emulators. That’s why at Micro Focus we stay focused on finding innovative ways to enable your terminal emulation software (and therefore your mainframes) to work seamlessly with emerging technologies like Windows 10.

**Terminal Emulation and Your Security Strategy**

Current Micro Focus® Reflection® Desktop, Rumba+ Desktop, and InfoConnect® Desktop terminal emulation solutions support both Windows 7 and Windows 10. Delivering the most powerful IT security capabilities in the terminal emulation market, they deliver a modern user experience with uninterrupted access to business-critical applications.

In fact, our Windows 10-compatible terminal emulators can play a vital role in your overall security strategy by helping you to:

- **Meet external requirements.** Our products are certified for the U.S. Department of Defense Public Key Infrastructure (DoD PKI) and offer strong SSL/TLS and SSH encryption validated for the U.S. government’s FIPS 140-2 standard. This high level of security facilitates compliance with PCI DSS, Sarbanes-Oxley, HIPAA, and Basel III requirements.

- **Restrict user access.** With the Microsoft User Account Control (UAC) security platform, you can block access to terminal emulation features—features that only an administrator should be allowed to enable.

- **Contain macro sprawl.** Macros are definite time-savers, but they can also be a security risk. With our Trusted Locations feature, administrators can predefine desktop or network locations from which settings files can run—preventing unauthorized macros containing malicious code from compromising mainframe data and applications.

- **Protect sensitive data.** Information Privacy Filters mask sensitive data, such as social security and credit card numbers, within mainframe applications and at all Office integration points (such as the Clipboard). With Information Privacy Filters enabled, data is hidden when users employ features such as Screen History, Recent Typing, AutoComplete, Print Screen, and Cut/Copy/Paste. Mainframe data can also be excluded from emails.

- **Take centralized control.** Our terminal emulators work with another Micro Focus solution, Host Access Management and Security Server (MSS), to strengthen security through effective management. Working with your Identity and Access Management (IAM) system, MSS seamlessly propagates changes to application settings and user-specific content from a central server. With MSS, you can lock down 100s (or 1000s) of desktops with ease, grant or deny access based on group or role, and make post-install adjustments on the fly. The changes are immediate.

- **Perform easier installs.** You can install our products on all your desktops using industry-standard Microsoft Installer (MSI) technology. An MSI editing tool lets you completely customize installations prior to deployment—making it easier to add new security capabilities or limit user access to specific features when you upgrade.

- **Leverage virtualization technologies.** Our terminal emulators are optimized for the most popular virtualization platforms from VMware, Microsoft, and Citrix. In fact, our products have earned both the VMware Ready and Citrix Ready logos.

There was a time when your valuable mainframe data traveled a protected path to and from a trusted terminal. Not anymore. Today, shielding it from the bad guys requires the strongest protection there is. By upgrading your operating systems and terminal emulators simultaneously, you gain the latest security controls available today while positioning yourself to be security-ready tomorrow.

**Which Micro Focus Products Support Windows 10?**

<table>
<thead>
<tr>
<th>Supports Windows 10</th>
<th>Does Not Support Windows 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>InfoConnect Desktop 16.0</td>
<td>Extra!® X-treme™ 9.4 and before</td>
</tr>
<tr>
<td>Reflection Desktop 16.0</td>
<td>Reflection 14.x and before</td>
</tr>
<tr>
<td>Reflection for Secure IT Windows Client 8.0 (Coming February 2017)</td>
<td>Reflection for Secure IT Windows Client 7.2 SP5 and before</td>
</tr>
<tr>
<td>Rumba+ Desktop 9.4</td>
<td>Rumba+ Desktop 9.3 and before</td>
</tr>
</tbody>
</table>
Make Your Migration Count

Terminal emulation software is used to access your most critical systems and data. In other words, this software is a corporate necessity that must be maintained, secured, and controlled. For practical reasons, your move to Windows 10 marks the best time to upgrade your terminal emulators. You’ll maximize your investment in the new operating system—and position your business to take centralized control of these complex configurations, lock them down, and move them into the new world of security.

More About Host Access Management and Security Server (MSS)

Modern IAM systems were never designed to work with legacy mainframe systems, and vice versa. But MSS and its add-on components work with your IAM system to centrally manage and secure mainframe access through your Micro Focus terminal emulators.

With MSS, you can:

- **Take centralized control**
  Manage host-access operations from your central MSS console. Lock down 100s (or 1000s) of far-flung desktops with ease. Grant or deny access based on group or role. Apply changes quickly to align with business needs. Make post-install adjustments on the fly. Do it on your schedule, not someone else’s.

- **Reinforce security as you remove passwords**
  With MSS, you can bring your host into the IAM fold. That means you can replace weak, eight-character passwords with strong, complex ones. Implement best-fit multifactor authentication methods. Say goodbye to host passwords and automatically sign users on to their mainframe applications.
  It's safe, manageable, and economical with MSS.

- **Build a wall of security in front of your mainframe**
  MSS works with the MSS security proxy, which sits between your desktops and your hosts. The security proxy accepts SSL/TLS encrypted packets and decrypts them before they are delivered to the host. Once decrypted, packets can be monitored by intrusion detection, content inspection, and other security devices for possible attacks or data leaks.
  MSS is a nonintrusive solution that requires no changes to your mainframe applications or your IAM system.

www.microfocus.com