CITRIX®

White Paper

Work Outside the Box: A Profitable, Audit-Friendly, Secure Workspace for Any Cloud Infrastructure

CITRIX Ready | KANGURU™ Secure. Anytime. Anywhere. | squadra technologies

Executive Summary

With the advent of new workstyles and progressively more complex IT environments, it has become increasingly frustrating for people to get work done in a productive and efficient manner. Users are often forced to remember multiple logins as they switch between applications. It has become all too common for users to waste significant time searching across locations for information — all while incurring the risk that's involved for organizations when transactions of data assets are unmonitored and imported from external sources outside of a secure network.

Together, Citrix Workspace, Kanguru Defender, and Squadra SecRMM deliver a portable, audit-friendly, secure workspace for any cloud infrastructure. They enable people to do their best work securely, while maintaining a high-quality user experience.

Most technological advancements are not panaceas; they often come with unintended consequences. This is certainly true with removable drives. The increased difficulty of protecting data — the single most valuable resource of any company — is often a major problem.

Some companies have resorted to rather extreme measure to meet (or rather avoid) this risk. IBM, for one, has decided to completely ban the use of USB drives.

Today, more than ever, companies require the ability to make data portable, mobile and accessible anytime, from any place. But providing that capability poses difficult challenges.

Challenges of an Always-On Strategy

We live in a multi-device, multi-cloud world. Data is our new currency, and it lives everywhere. Given the good-as-gold status of data, it's fitting that ensuring the protection of data assets is now of paramount importance to security teams.

But as data has grown in value, the task of protecting that asset has come more difficult. The ability of mobile devices to connect from anywhere, including public networks, has exponentially increased most organizations' exposure. Routine actions such as accessing SaaS applications for downloading information on insecure networks, the copying of files onto removable drives, and visiting insecure websites can wreak havoc, leaving security teams scrambling.

Security lapses can occur in many ways. Drives can be lost. Bad actors inside and outside the organization can misuse downloaded information. Users can accidentally acquire access to information to which they have no rights. Deploying additional point security solutions only further complicates the environments, increasing the surface areas exposed to attack. Instead, organizations need an integrated security approach that places the user at the center.

Banning drives or blocking SaaS application access may indeed enhance security — but only in the short-term. These actions severely impact end-user productivity, motivating users to bypass restrictions without the knowledge, approval and oversight of the security team. Organizations need ways to leverage the unmatched ubiquity and utility offered by removable drives and SaaS applications while controlling access and maintaining enterprise security.

The use of virtual desktops is a partial solution which keeps the data and application in the data center. But users still require access to SaaS applications, and the quality of the user experience can suffer when delivered remotely.

For all of the above reasons, the combination of Citrix Workspace, Kanguru Defender and Squadra SecRMM presents a compelling security solution. Instead of attacking each of the security issues individually, organizations adopting Citrix Workspace enjoy an always-on, secure digital workspace that protects data when stored online. Kanguru Defender provides encrypted, enterprise-grade drives that assure data security when stored offline. And Squadra SecRMM integrates natively with both Citrix Workspace and Kanguru Defender, helping audit usage of removable drive storage with detailed security information.

SecRMM acts in unison with Citrix Analytics in collecting data across network traffic, users, files and endpoints in Citrix environments. The actionable insights provided enable security teams to proactively handle user and device security threats, improve application performance and optimize IT operations.

Citrix Ready Bundled Solutions Program

The Citrix Ready Bundled Solution Program tests, integrates, and markets two or more Citrix Ready validated solutions together. Resulting solutions help unify workspace management by addressing more complex use cases and can dramatically reduce risk and deployment time for our joint customers. The Citrix Ready brand builds trust and confidence, and the Bundled Solutions program helps deliver a consistent and verified solution.

The Citrix Ready Program

The Citrix Ready technology partner program offers robust testing, verification, and joint marketing for Digital Workspace, Networking, and Analytics solutions—with over 30,000 partner verifications listed in the Citrix Ready Marketplace.

Tested and verified as part of the Citrix Ready Bundled Solution Program, this solution provides significant benefits:

- **Secure by Design:** This bundled solution approach utilizes features in Kanguru Defender when data is stored offline, and in Citrix Workspace when data is stored online. This always-secure architecture ensures the end-to-end security of data assets. In addition, the Squadra SecRMM Data Loss Prevention (DLP) solution is content-aware, even at the USB layer level. This capability further enhances the value of this bundle in supporting and driving the key security initiatives of any enterprise.

- **Flexibility:** This bundled solution enables security teams to offer users complete flexibility in performing their jobs in any environment, from any location, without loss-of-control worries, while accessing any SaaS application via Citrix Access Control. The bundled solution also eliminates threats that may stem from operations such as copying files from VDI onto enterprise-grade drives secured by Kanguru Defender, even if connected over a public network. Squadra SecRMM reliably audits such operations conducted through USB ports, providing detailed security information to system administrators. And Citrix Analytics proactively provides actionable insights using machine learning spanned across security, performance and productivity needs of the enterprise.

- **Built for the Cloud:** Organizations seeking to modernize their infrastructure by adopting cloud-oriented technologies require future-proof solutions: solutions that work now and into the future. This solution provides for short-term needs while maintaining the flexibility to deploy, manage and optimize workloads on any cloud infrastructure using Citrix Cloud.

Key Features of the Joint Solution

Citrix is committed to constantly improving user experience and productivity for an increasingly mobile workforce. This bundled solution helps to fulfill that commitment by providing significant functionality for auditing, access control and data portability that is secure, easy to use, and seamlessly integrated. The resulting benefits include:

- The protection of company information residing on removable drives.
- The enablement of secure data sharing. Data remains secure and assessable regardless of where it resides.

Citrix Cloud

Citrix Cloud makes it easy for IT teams to consolidate and deliver secure workspaces in hours, not weeks, while placing your sensitive app, desktop and data resources on any cloud or hybrid cloud and provide workers flexibility storing data offline using Kanguru Defender and connecting from anywhere without losing control and visibility using Squadra SecRMM.

- The delivery of mission-critical applications, securely and efficiently.
- The enablement of mobile users to thrive in productivity, free from concerns about data security and the accompanying restrictions that often strangle both efficiency and motivation.

The ideal solution will have a remote worker log in to Citrix Workspace and copy content on a secure USB drive, but only under the specific policies that the administrator has enforced and with the administrator maintaining full back-end control.

Each partner in this bundled solution works to enable that ideal solution. Kanguru's encrypted USB drives ensure that data is kept secure once written to the device. Data can be remotely disabled or deleted if the device is lost. And once an authenticated user logs in to Citrix Workspace, Squadra SecRMM helps maintain access and data control on the back end.

Citrix Workspace, Kanguru Defender, and Squadra SecRMM

The Citrix, Kanguru and Squadra solution is integrated to provide a truly seamless environment for both cloud and virtualized applications and desktops. This brief overview outlines the benefits provided by each partner in enabling this bundled solution:

Citrix Workspace

Only Citrix offers the most complete and integrated workspace to enable people to securely access their apps, desktops, and data from anywhere. Rely on Windows app and desktop delivery from Citrix Virtual Apps and Desktops, device security from Citrix Endpoint Management, secure file sync and sharing with Citrix Content Collaboration, and network security with Citrix Gateway. Only Citrix Workspace offers you complete choice of device, cloud and network, streamlined for IT control and simple, secure access for users.

Citrix Workspace. Whether delivered on-premise or in the cloud, Citrix Workspace offers the most complete and integrated workspace on the market. Workspace enables mobile users to securely access their applications, desktops and data from anywhere. Ultimately, Citrix Workspace helps companies to achieve levels of productivity and profitability that only a more engaged workforce can provide. Most corporate executives agree that a superior virtual work culture helps to attract and retain superior talent.

Increasingly, companies rely on enterprise applications and desktop delivery from Citrix Virtual Apps and Desktops, device security from Citrix Endpoint Management, secure file sync and sharing with Citrix Content Collaboration, and network security with Citrix Gateway.

Only Citrix Workspace offers organizations complete choice of device, cloud and network, streamlined for IT control and with simple, secure access for users.

Squadra SecRMM. When a security breakdown occurs within an organization, it's crucial that the security team has access to details — both to understand the risks involved, and to help in preventing future similar breakdowns. SecRMM provides those details by collecting forensic security data about removable media write activities. The level of detail provided ensures that security teams will be able to understand the exact nature of the security incident. (In contrast, competing solutions are not even capable of reporting the files that may have been illicitly copied from a local computer or network.)

The unauthorized execution of programs is one of the most common routes through which malware finds its way into data centers. SecRMM provides an additional layer of security enhancement by preventing programs, scripts, batch files and office macros from unauthorized execution. SecRMM also generates a file that contains tracking data with every write to a removable drive. Administrators can use this tracking data to determine where a device has been used, and the security policies that were in place at the time of the write.

Additionally, SecRMM provides the option of using a mobile app for adding an additional layer of security authentication. This optional security feature ensures that a device will not appear as a USBs to Windows unless the end-user has successfully logged in from a mobile device.

Kanguru Defender. Defender integrates natively with Citrix Workspace, virtualizing the removable drive into Citrix Virtual Apps and Desktop environments. This capability ensures that users can access, store and transfer data securely from anywhere.

All Kanguru Defender® Secure External Drives are password protected with AES 256-bit hardware protection in XTS mode. AES is widely recognized as the standard for encrypting and decrypting data and is used worldwide by many organizations including military, government and financial institutions. AES 256-bit protection provides the most sophisticated degree of AES protection available. Defender also offers an annual subscription to anti-virus/anti-malware software with automatic updates. A free 30-day trial is available.

The risks of unauthorized logins, viruses and malware are not the only risks that threaten the security of USB flash drives. Physical tampering is also a threat. Kanguru Defender counters that threat by ensuring that the USB design incorporates features that enhance physical security, including:

- Tamper-resistant epoxy
- Waterproof enclosure
- Rugged alloy housing

Defender also features brute-force prevention, with configurable auto-disable or delete after seven invalid login attempts. Defender's keylogger prevention capability foils spyware that is designed to secretly log keystrokes. FIPS 140-2 validation helps ensure that Defender is appropriate for federal agencies and regulated organizations to use securely.

It's No Longer a Work Place

In today's world, work is no longer a place. Instead, it's a dynamic activity that people expect to be as adaptable as they are. The modern work environment is about how you work, not where you work. In this environment, work can be performed anywhere, anytime. Without that capability and flexibility, users simply can't provide the production necessary to remain competitive.

But the mobility and portability of data comes with an inherent security risk. And the risks presented by unprotected removable data storage devices are among the most virulent of security risks. Infosec, a leading provider of security training and education, notes that "ease of use and convenience is part of the problem with removable media … as malware and viruses are able to easily replicate and distribute themselves to unprotected storage devices that are not write-protected."

Fortunately, organizations need not resort to the extreme measure of banning USB flash drives. The bundled solution of Citrix Workspace, Kanguru Defender and Squadra SecRMM provides organizations with the ability to capitalize upon the competitive advantages provided by removable storage media, while avoiding the security shortfalls that often accompanies the use of these productivity-enhancing devices. The result is an always-on, secure digital workspace that protects data when stored online.

In sum, this bundled solution provides a portable, audit-friendly, secure workspace for any enterprise wishing to successfully compete in the modern business landscape.

To learn more about how to prevent data loss and maintain access control with USB drives in a virtualized environment, check out Kanguru and Squadra in the Citrix Ready Bundled Solutions Program.

About Kanguru

Kanguru develops innovative and highly secure data storage solutions for a variety of industries around the world, including Government, Defense, Financial, Energy/Utilities, Medical/Healthcare, Enterprise, Education, and SMBs looking to meet high security standards and industry regulations. Learn more at kanguru.com.

About Squadra

Squadra is a security software company focusing on the niche of providing robust control and auditing of internal organizational data/file transfers. In the era of major data breaches organizations are reassessing their data loss prevention ("DLP") policies. Squadra recognizes that substantial security holes exist by data leakage coming out of removable media storage devices connecting through the USB. With the above-mentioned market pressures in mind, Squadra began development in 2011 of secRMM. It has seen successful sales in key market verticals including healthcare, banking/finance, manufacturing, mining, legal, and the Department of Defense. Learn more at squadratechnologies.com.

About Citrix Ready

The Citrix Ready technology partner program offers testing and verification for joint Digital Workspace, Networking, and Analytics solutions. After a robust testing process, validated partner solutions are listed in the Citrix Ready Marketplace, giving customers and channel partners a simple and effective way to explore and select Citrix Ready verified solutions—increasing confidence while reducing risk. Learn more at citrixready.citrix.com.

CITRIX®

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States