DIGITAL WORKSPACE ECOSYSTEM ALLIANCE

Securing the Digital Workspace

eBook

TABLE OF CONTENTS

About the DWEA

The Digital Workspace Ecosystem Alliance (DWEA) is a consortium of technology leaders dedicated to helping organizations enable secure productivity for all of their people. Together we are committed to providing the vendor-neutral education and resources needed to empower organizations of all sizes to develop the Digital Workspace strategy that makes sense for their business. The DWEA is a 501(c)(6) not-for-profit organization dedicated to market education.

Your Guide to Zero Trust Security for the Digital Workspace

Contributed By CAMEYO

As workforces return in whole or in part to the office, cybersecurity remains top of mind for many IT departments. And rightfully so. Malware and cyberattacks surged during the pandemic, and the explosive growth in the number of remote users opened up new vulnerabilities and attack vectors for cybercriminals as organizations struggled to find the tricky balance between ease of access and strict security measures.

When the spotlight fell on those vulnerabilities, two common culprits emerged. One was phishing, which tends to exploit human trust and ignorance to turn an unsuspecting employee into an attack vector. The other was the Remote Desktop Protocol, or RDP, which is the technology on which so many forms of remote access rely. In mid-2020, ZDNET went so far as to say that RDP "reigns supreme" when it comes to ransomware exploits.

The identification of RDP as a potential security risk wasn't news to a lot of people in the IT industry. During the pandemic, however, its threat as an attack vector magnified because of how widespread its use became in debilitating ransomware attacks. According to Palo Alto Networks' Unit 42 Cloud Threat Report, 1H 2021, RDP exposures increased by 59% across all cloud providers in the short span between Q1 2020 and to Q2 2020. The 2020 Incident Response and Data Breach Report from the same group found that RDP was the initial attack vector in 50% of the 1,000+ ransomware deployment cases it studied.

What is the Remote Desktop Protocol (RDP) and why does it pose security risks?

The Remote Desktop Protocol is a part of a suite of technologies found on Microsoft Windows systems that are designed to allow users to remotely connect to and control a separate system. RDP works in conjunction with Remote Desktop Services (RDS) to provide a graphical representation of the host's desktop interface on any remote client machine that supports it. This was traditionally used for IT to diagnose and fix issues on a remote user's computer via the GUI, but these days it's far more common to find RDP being used to provide users with virtual desktops or perform remote management.

(As a brief aside for the sake of clarity, Microsoft's official name for their RDP client software is the Remote Desktop Connection. This was previously known as the Terminal Services Client because of its roots in Windows Server's Terminal Services.)

RDP connections pose a security risk for three simple reasons:

1. RDP is the de facto industry standard for providing remote desktop sessions and other services to remote users.
2. The increase in remote work has likewise increased the use of virtual desktop and other remote access solutions that rely on remote desktop services.
3. Because of how RDP works by default, simple RDP vulnerabilities have the potential to grant hackers access to entire networks.

Through the use of man-in-the-middle attacks or phishing campaigns that allow for unauthorized access to a remote client, a malicious actor can use that client as an attack vector to (or through) the remote desktop gateway. Virtual private networks (VPNs) exacerbate this situation because they assume legitimacy and offer network-level authentication to remote clients. Even strong passwords and IP address whitelists don't offer sufficient protection when VPNs are at play.

Yet it's important to note here that infected endpoints aren't the only potential RDP vulnerability. Ransomware.org details what's known as a reverse RDP attack, whereby the threat actor plants malware on the RDP server. Any client that connects to that infected server becomes infected itself. Entire organizations could therefore potentially find themselves on the wrong side of a system-wide lockout.

How does the server become infected in the first place? This is done through brute force attacks that run through authentication permutations until they hit the right combo that gives the hacker RDP access. Many organizations face challenges in preventing this because they have to open their firewall to common RDP ports in order to provide seamless access to authorized remote users.

Older, unpatched versions of RDP also have innate security vulnerabilities that make them susceptible to malware like BlueKeep (CVE-2019-0708), which is a "worm" that can infect a server and spread to connected devices.

Does that mean RDP security is a lost cause?

With so many actual and potential RDP vulnerabilities, it might seem like secure remote access is an impossible task. And if that's true, it presents IT departments with a terrible choice: Either forbid hybrid and remote work altogether or allow hybrid/remote work and accept malware and other security concerns as a necessary consequence.

Fortunately, that isn't the case.

Zero Trust security is a best practice that approaches network security from a different angle — and in doing so aims to provide better balance to the "trust versus threat"

dilemma. Instead of assuming that authentication should equate to full network access, Zero Trust security models treat every device as a possible security risk. It operates on a model of least privilege, so both remote users and those at in-network workstations are only granted permissions to access the apps and data they need and nothing more. You can think of Zero Trust as compartmentalizing and containing users rather than just opening a single door to the organization's entire network.

Any Zero Trust model will both require and strengthen a secure remote desktop policy. To put that another way, organizations can leverage Zero Trust security to empower their hybrid/remote workforce even as they mitigate the security risks associated with remote-enablement technologies like RDP. But much of that depends on sourcing and implementing the solutions that also prioritize that balance.

VAD is a building block of a Zero Trust Network Architecture

For organizations that are as serious about Zero Trust as they are about hybrid and remote work, Virtual App Delivery (VAD) systems can help them provide their people with seamless access to apps from any device while bolstering security with Zero Trust.

VAD platforms are able to do this in part because they are OS-independent. They don't require a special client; all apps are delivered to the user via a dedicated encrypted HTTPS (TLS/SSL) HTML5 browser session. This means that clients running operating systems like Windows, ChromeOS, iOS, Android, and Linux can all work with software that retains its full desktop functionality, yet the software is never running on the remote device itself. This likewise means that all user interaction with the app is abstracted from the host machine — so the attack vector is obfuscated for malware payloads.

And since VAD platforms do use industry-standard RDP for remote access (just like their VDI & DaaS counterparts), you should check with your VAD vendor (or VDI/DaaS vendor) to make sure they have systems in place to safeguard your networks against brute force attacks, ransomware and other cyberattacks. Below is a checklist that you can use to make sure the vendors you are evaluating have a true Zero Trust security model in place:

- Single Architecture – It should not rely on acquired/bolt-on technologies or third party products that significantly increase the surface of attack for hackers.
- Eliminate Open Firewall Ports – It should leverage a proxy server between the end user device and your serves, eliminating the need to open firewall ports to direct inbound traffic. It should also eliminate the need for VPNs because the end user device is completely isolated from the corporate network. Both are a major attack vector for hackers.
- Eliminate Open RDP Ports – It should close HTTP, HTTPS, and RDP ports at the Windows firewall and dynamically opens them to authorized users only when they need access. Server ports are another favorite for hackers.
- Least Privilege Principle – Users must have ZERO admin privileges. In the event a hacker gains access to a user session, they should be locked into the session and unable to move to other areas of the corporate network.

- **Non-persistent Servers** – When a user closes a VAD session, their data and entire user profile should be deleted. Be sure to find a VAD technology that stores the updated user profile separately and seamlessly syncs the user profile upon session relaunch for a seamless experience without compromising security.
- **HTTPS security and encryption** – All servers should be automatically created with HTTPS to ensure all data/sessions are encrypted.
-

Through this combination of secure RDP technologies and Zero Trust, VAD platforms can provide your hybrid/remote work users with seamless, secure access to all their apps from any device while simultaneously solving RDP security issues and reducing your overall attack surface.

You can learn more and download a Zero Trust security checklist and white paper here.

* * *

Enhancing Digital Workspace Security: Context-Sensitive Printing

Contributed By tricerat

In today's digital age, where sensitive information is at risk from cyber threats, securing the digital workspace is of paramount importance. While we often focus on data stored on servers and in the cloud, we cannot overlook data that is transmitted through printing workflows.

Context-Sensitive Printing

Context-sensitive printing is an approach that tailors a user's access to printers and settings based on the context of their tasks and the sensitivity of the documents they are handling. Here's why it's essential.

1. User-Based Access Control - Context-sensitive printing ensures that users are granted access only to printers and settings relevant to their roles and tasks within the organization. For example, HR personnel should only have access to HR-related printers and settings, while finance teams should be limited to finance-related resources. This provides not just a better user experience, but also simplifies printing workflows and reduces chances of sensitive data being mistakenly sent to the wrong printer.

1. Enhanced Data Security - By matching users with appropriate printers and settings, organizations reduce the risk of sensitive information being inadvertently exposed. This minimizes the chances of printing confidential documents on a shared, unsecured printer.
2. Streamlined Workflows - Context-sensitive systems streamline document management by minimizing user effort. Users don't need to manually select printers or settings; the system intelligently does it for them.
3. Efficient Resource Utilization - By ensuring that users utilize the right printer and settings for their specific tasks, organizations can optimize printer usage and reduce waste, thereby saving costs and environmental resources.

Follow Me Printing: Convenience Meets Security

Follow Me Printing is a protocol that offers the perfect blend of convenience and security in the modern workplace. It allows users to send print jobs to a centralized queue and then release them securely at any authorized printer within the organization.

1. Increased Mobility - With Follow Me Printing, users are no longer tied to a specific printer. They can print from their laptops, smartphones, or desktops and pick up their documents at any printer when they're ready.
2. Enhanced Security - Since print jobs are held in a secure queue until the user releases them at the printer, sensitive documents are not left exposed on the output tray. This eliminates the risk of unauthorized access to sensitive information.
3. Cost Efficiency - Follow Me Printing reduces paper waste as users can review their print jobs before releasing them. Unnecessary or duplicate prints can be easily avoided, saving resources and reducing costs.
4. Streamlined Workflows - Users can prioritize and release print jobs on their schedule, improving workflow efficiency and reducing congestion at the printer.

How to Implement Context-Sensitive Printing and Follow Me Printing

1. Choose the Right Print Management Software - Invest in a robust print management solution that supports context-sensitive printing and Follow Me Printing. Many solutions offer customizable rules and policies to match your organization's needs.
2. Configure Access Control - Set up user-based access control to restrict printer access based on roles and responsibilities.
3. Implement Secure Print Release - Enable secure print release mechanisms, such as PIN codes, card authentication, or biometrics, to ensure documents are only printed when the rightful owner is present.
4. Define Context Sensitivity Rules - Create rules that automatically assign users to appropriate printers and settings based on their roles and the context of their tasks.
5. Train Your Team - Provide training and awareness programs for your employees to ensure they understand the importance of context-sensitive printing and how to use Follow Me Printing effectively.

Securing the digital workspace is a multifaceted endeavor, and context-sensitive printing is a vital component. By implementing this solution and enhancing it with features such as follow me printing, organizations can not only enhance security but also improve efficiency and reduce costs. Prioritizing the protection of sensitive information in both digital and hard copy forms is essential in today's ever-evolving threat landscape. Make sure your organization stays ahead by incorporating these practices into your workspace today.

* * *

Boosting Digital Workspace Security With Remote Browser Isolation (RBI)

Contributed By FORTINIUM

In today's age, where hybrid and web-centric work is the new norm, ensuring the security of our digital workspaces has become paramount. Cyber threats are on an exponential rise, targeting not only businesses but also individuals. In this landscape, Remote Browser Isolation (RBI) emerges as a game-changing solution to bolster digital workspace security as you switch from 'identify and eliminate' to 'isolate and ignore' improving your protection level from web based malware to 'near 100%'.

The Need for Enhanced Security

The digital workspace has transformed the way we work, offering flexibility and efficiency in tools and even location we work from. However, this shift has also increased our exposed attack surface and made us more vulnerable to cyberattacks. Phishing attempts, malware, and malicious websites lurk on the internet, waiting to compromise our data and systems. Traditional security measures, while essential, often fall short in providing comprehensive protection and limit our productivity as they operate by limiting what we can access to mitigate risk.

What Is Remote Browser Isolation?

Remote Browser Isolation is a cutting-edge security technology that isolates web browsing activities from the local environment. When users access websites from their browser or click on links, instead of rendering web content directly on their devices, RBI redirects these activities to a remote, isolated session. Users interact with the web content remotely, and only safe, sanitized information is sent back to their devices.

Benefits of RBI:

1. Protect from (un)known Web-Based Threats: RBI acts as a shield, preventing malicious code from reaching user devices. Even if a user accidentally stumbles upon a malicious website, the threat remains contained within the isolated environment.

2. Enhance User Productivity and Experience: With RBI, web content is processed on powerful servers, reducing the strain on local devices. RBI even allows remote access to company internal websites without the need of VPN or 3rd party protocols. Finally RBI also allows you to eliminate web site blacklisting as every site becomes 'equally safe'.

3. Simplified Endpoint Management and Security: By isolating web activity, RBI reduces the attack surface of endpoints. As RBI does not require any local agent to be installed it simplifies endpoint security management and lowers the risk of breaches.

4. Flexible Endpoint Strategy will Lower Cost: As all your web-based work and security is managed through RBI you may open your device strategy to new concepts without additional risk – BYOD, Chromebook, Shared device, Access from a Hotel Convenience Terminal or even a Smart TV … it makes no difference.

5. Improve Compliance & Privacy (GDPR/DSGVO): With remote execution of active web content and document transfer policies available within RBI all upload and download of documents may be restricted, eliminating not only security risks but also data theft.

Sample Use Cases

While many people still have not heard of RBI, market adoption is on a strong rise as use-cases and deployment benefits are so obvious.

- Improve productivity and flexibility enabling users for risk-free access to any website from any device and place – while keeping control of what documents may be up- or downloaded

- Access defined company internal web service from any place – without the need of a client configuration or VPN – for employees but also for external partners, contractors or as part of a M&A situation
- WorkOnAnyDevice allows instant work after loss of device or a corporate emergency – but also opens saving potentials with BYOD

Implementing RBI

Deploying RBI in your digital workspace involves a few key steps:

- Assessment: Identify your organization's specific security needs and the web browsing habits and demands of your users.
- Set Security Standards: Define what existing security standards may be adapted due to RBI (e.g. Blacklisting, BYOD) and which users to participate (all or just specific groups/individuals)
- Deploy RBI Solution: Define what components you want to operate yourself and what to consume from a service provider. Integrate the infrastructure with your network to ensure a seamless user experience.
- Notify & Educate Users: Instruct users on the usage of the solution – but keep up also general Cybersecurity Training to keep users sensitive on their web behaviour.

Conclusion

Remote Browser Isolation is a powerful tool in the arsenal of digital workspace security. It offers protection against web-based threats, enhances productivity, reduces data compliance issue and simplifies security management. In a world where the internet is both a boon and a potential hazard, RBI provides the safety net needed to navigate the digital landscape securely.

By adopting RBI and following best practices, organizations can safeguard their data, maintain user productivity, and stay one step ahead of cyber threats in the ever-evolving digital workspace.

* * *

THANKS

About the DWEA

The Digital Workspace Ecosystem Alliance (DWEA) is a consortium of technology leaders dedicated to helping organizations enable secure productivity for all of their people. Together we are committed to providing the vendor-neutral education and resources needed to empower organizations of all sizes to develop the Digital Workspace strategy that makes sense for their business. The DWEA is a 501(c)(6) not-for-profit organization dedicated to market education.

NEXT STEPS

Visit us at digitalworkspacealliance.com and subscribe to our blog to receive updates on our latest research. And join the DWEA group on LinkedIn, or follow us on Twitter: