How AppSense Integrates with Citrix Ready Secure Remote Access Program

CITRIX READY

AppSense | CITRIX

More employees are working remotely than at any time in history. Some pioneering companies have already moved to a 100 percent remote workforce model. And yet the move toward a remote workforce is only beginning.

Though remote access offers extraordinary levels of convenience, productivity and cost-saving opportunities, it also imposes increased levels of risk. As the remote access of systems and data increases, IT managers are struggling to find ways to keep corporate information safe. But cybercrime is also escalating at an unprecedented rate. And the increase in mobility has added fuel to the cybercrime fire by opening a vast new frontier of opportunity for cybercriminals.

Cybercriminals are using sophisticated ransomware and phishing operations to prey upon employees, turning them into unsuspecting allies in gaining illicit access to enterprise data and systems. And though many security solutions exist, all too often they provide an increase in security at the cost of decreased usability and productivity. This paper discusses the benefits of integrating AppSense user management solutions into a Citrix virtual environment, and also notes the balance between security and usability that can be achieved through this partnership.

Business Challenge Summary

Not so very long ago, corporations were able to protect their most precious assets by placing them under lock and key. But that is no longer the case. Since the dawn of the information age, the safeguarding of access to proprietary data and systems has become a priority.

Ensuring the protection of corporate data and critical IT resources requires preventing unauthorized and potentially malicious software from infiltrating workspace environments. The growing trend toward bring your own device (BYOD) also poses security problems for many corporations. Employees accessing company data and systems from their own devices can create significant security threats without sufficient safeguards in place.

However, traditional perimeter security methods are often difficult to manage, are reactive and can be disruptive to users. And yet the need for information security has never been greater, with cybercrime more prevalent than ever. The US Department of Justice[1] even ranks cybercrime as one of the greatest threats facing the nation.

Unfortunately, most corporations are losing the war against cybercrime. Ransomware attacks, for example, are dramatically on the rise with a 300 percent increase in attacks year-over-year — more than 4,000 attacks occur daily. According to *The Atlantic,*[2] experts estimate the financial impact of ransomware to be in the range of $75 billion per year. So daunting is the ransomware threat that many corporations have begun to keep ransom-ready funds in special accounts: tens of thousands of dollars in Bitcoin kept ready to pay the ransom in the event of

[1] https://www.justice.gov/usao/priority-areas/cyber-crime

[2] http://www.theatlantic.com/business/archive/2016/09/ransomware-us/498602/

an attack — and yet 65 percent of organizations have yet to implement budgetary provisions for a potential attack. And 52 percent of organizations have not purchased insurance against ransomware, phishing, and other forms of cybercrime attacks.

Perimeter security and anti-virus solutions are important weapons in the war against cybercrime. But mounting an effective, comprehensive defense against today's technologically savvy cybercriminals requires an in-depth, multilayered approach that radically improves protection.

In desperation, many organizations have attempted to strengthen defenses by stripping admin rights from users. While diminishing the admin capabilities of staffers can effectively reduce malware and ransomware attacks, the unfortunate side effect is a crippling reduction in productivity.

It is, in effect, a form of capitulation; companies willingly surrender a degree of productivity in the hope of avoiding a brush with cybercrime that will ultimately result in the very same thing: a loss of productivity.

An unfortunate domino effect of additional unintended consequences typically results from such extreme defensive measures. Workers rendered less productive by a poor or frustrating user experience place additional burdens upon supporting infrastructure — increased helpdesk calls, for example. Users may also react to an over-secure workplace by turning to 'shadow IT' to regain lost capabilities, introducing new security risks.

In response to the cybercrime wave, government-imposed security mandates are becoming increasingly burdensome for IT departments. IT faces mounting pressure to deliver without increasing costs for the whole organization. Key application software vendors such as Microsoft are under constant attack, making it imperative that operating systems and applications be kept up-to-date with the latest patches. Though patching can be a huge drag on IT resources, it is mission critical. SANS[3] and the Australian Signals Directorate[4] suggest that 85 percent of all intrusion techniques can be stopped with effective whitelisting, OS patching, application patching and setting administrative privileges correctly.

CITRIX® XenDesktop

Virtual desktop infrastructure (VDI) environments delivered through Citrix XenDesktop are often adopted to centrally manage and secure user workspaces, reducing security risks and increasing worker productivity. Unfortunately, user resistance is the leading cause of VDI project failure. Switching from a physical desktop to a virtual desktop can present certain difficulties and discomforts to users, such as:

- Personalizing their own (virtual) workspace can be difficult
- Support for printers and other external devices can be problematic
- User experience may be device- and location-dependent

The key to success in making the transition to a VDI environment hinges upon making VDI more user friendly. Improving the user experience and reducing VDI complexity help break down the barriers of user resistance that so frequently foil the implementation of a VDI environment.

The need for a user management solution that can provide an effective defense against cybercrime without frustrating users to distraction has never been more obvious or urgent. Accordingly, more and more organizations are seeking a user management solution that combines effective security with usability and dependability.

Top Features to Consider in a User Management System

Maximizing the potential of a user management solution requires the installation of a system that delivers a full range of key capability and usability features. In particular, the following should be considered must-have features for any user management solutions undergoing evaluation for deployment in any organization:

1. **Visibility:** Increased visibility — knowing what is on your network — helps to reveal attack threats that might otherwise go undetected. Enhanced visibility strengthens the ability to spot suspicious endpoint behaviors such as unknown processes starting at logon, or unauthorized fluctuations in admin rights and self-elevation trends. Increased endpoint visibility also makes it easier to spot suspicious files and unauthorized applications introduced to endpoints, and to refine access policies based on application usage, aiding in license control.

[3] https://www.sans.org/reading-room/whitepapers/analyst/improving-application-privilege-management-critical-security-controls-update-36912

[4] http://www.asd.gov.au/infosec/mitigationstrategies.htm

2. **Authorization Enforcement:** Allow the known; stop the unknown. Only authorized applications should be allowed to run. The use of unauthorized software destabilizes user environments and makes it more difficult for IT teams to troubleshoot corrupt desktops. Apps that circumvent perimeter security should be prevented from running.
3. **Privilege Management:** User productivity should be balanced with security needs by dynamically controlling end-user privileges. Privilege management should occur at the application or individual task level rather than at the session or account level.
4. **Trusted Ownership:** Whitelisting overhead should be reduced or eliminated by accurately identifying and empowering trusted users and by limiting the privileges of installing and running applications to this group.
5. **Remediation:** Installed ransomware should be quickly identified, stopped from spreading, and eliminated from the system.
6. **Data Protection:** Data residing in documents, drives and files should be protected from unauthorized deletion.
7. **Secure Self-Service:** Empowering users to access and run applications securely reduces support costs, improves the user experience and increases productivity.
8. **Context Aware:** Risk varies based on user context. Policies and privileges should be modified as appropriate in response to user-contextual variables such as location, device, type of connection, time of day, and others.
9. **Personalization:** The transition from a physical to a virtual work environment often forces users to abandon device-specific personalization and preferences. Accommodating personalization across a virtual environment helps to limit the sense of constraint and unfamiliarity that is often a factor in increasing users' resistance to the adoption of a virtual workspace.
10. **Detachment:** The implementation and management of VDI can be simplified, and user acceptance amplified, by detaching users from devices, applications and the operating system.
11. **Simplified Image Management:** The solution should enable the use of a single golden image as a virtual desktop template, while enabling the personalization of the template to accommodate individual user needs and preferences.
12. **Lowered Server & Storage Costs:** Increasing the efficiency with which system resources are utilized can help reduce total costs by maximizing the number of users allocated per server.
13. **Enforced Compliance & Security:** Removing access on a per-app or per-Windows component basis reduces corporate risk and desktop software licensing costs, as you pay only for what you use.

CITRIX® XenApp

CITRIX® XenMobile

CITRIX® NetScaler

Citrix Ready Secure Remote Access Program Overview

Citrix solutions deliver a complete portfolio of products supporting the secure access of apps and data anytime, at any place, on any device and on any network. These include:

1. XenApp and XenDesktop to manage apps and desktops centrally inside the data center
2. XenMobile to secure mobile applications and devices while providing a great user experience
3. ShareFile to provide controlled and audited data access, storage and sharing, both on-premise and in the cloud
4. NetScaler to contextualize and control connectivity with end-to-end system and user visibility

Citrix solutions also integrate with third-party security products to provide advanced levels of system management and identity, endpoint and network protection. The Citrix Ready Secure Remote Access program was launched to identify and showcase partner products that are proven to smoothly integrate with Citrix products, and that work to enhance Secure Remote Access by adding extra layers of security. The Citrix Ready Secure Remote Access program serves as an aid to IT executives in quickly and easily finding and sourcing solutions for their Secure Remote Access needs, helping to secure organizations' corporate networks from theft of data, DDoS and other security attacks that may be perpetuated via Remote Access.

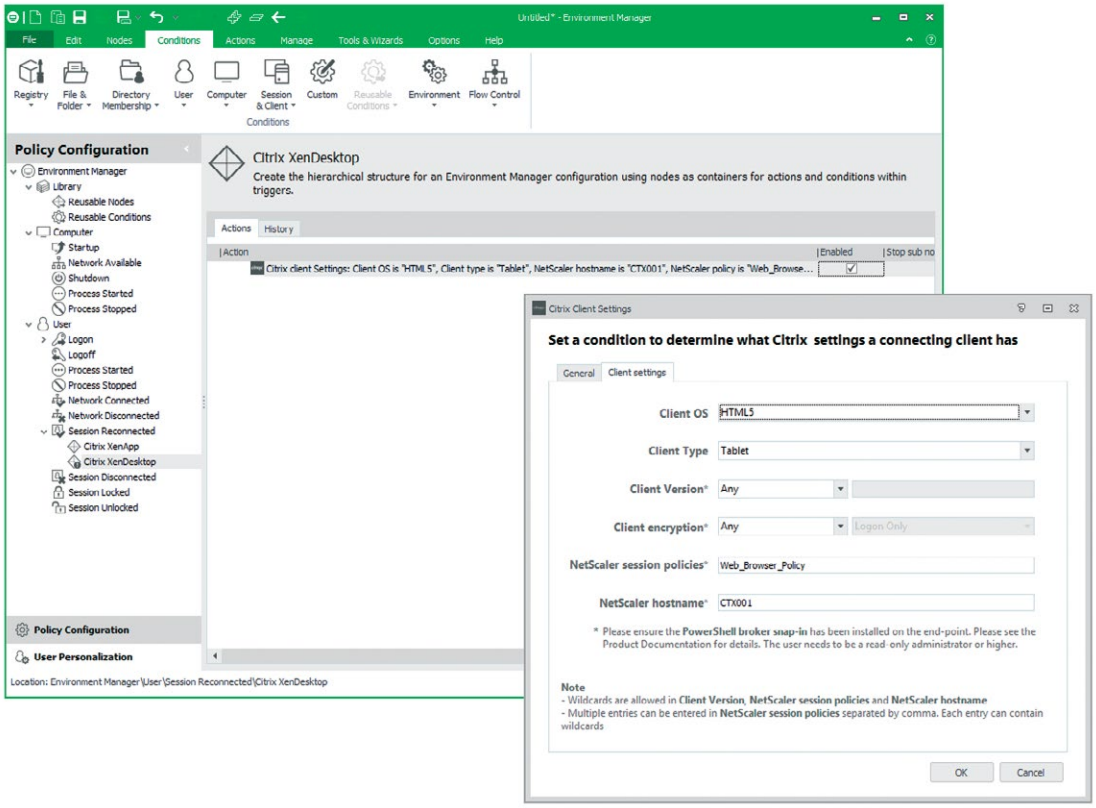
Citrix advises that organizations can best defend against security attacks that might occur through Remote Access by following five best practices — pillars of focus that support enterprise security:

1. **Identity and Access:** Administrators must be able to confirm the identity of users requesting access to a system and limit the degree of access granted. In comparison to simple password-based systems, two-factor authentication offers a vast improvement in the ability to properly confirm user identity in requests for access. The degree of access granted to each individual user should be based on context. The principle of least privilege helps to ensure that users are granted rights that are limited only to those required in the performance of their jobs.
2. **Network Security:** The growing demand for remote access complicates the process of securing a network. Yet the integrity of network security must be maintained while supporting remote access for mobile and third-party users. Network and host segmentation can be useful in shrinking surfaces that are vulnerable to attack. And implementing a multi-layer approach helps to boost network security while ensuring availability.

3. **Application Security:** All types of applications are potential targets for hackers, but the veritable explosion of apps has created many additional points of vulnerability for most enterprises. Apps on mobile devices are particularly susceptible to exploitation. An important step in reducing risk is enacting centralization and the encrypted delivery of applications. Containerization for mobile apps and inspection of incoming data streams can help to reduce app-related security vulnerabilities.

4. **Data Security:** The security of enterprise data can be enhanced by the centralization and hosted delivery of data by enforcing secure file sharing (to reduce data loss) and by the containerization of data (both in-transit and at rest).

5. **Monitoring and Response:** Vigilance and fast action are required to successfully counter the attacks that most enterprises face on a daily basis. A rapid response to breaches is also critically important, given that even the most secure systems are not completely invulnerable to successful attacks. Rapid detection and response to successful attacks serve to minimize damage and help to limit susceptibility to imminent additional attacks. End-to-end visibility into application traffic supports faster identification of security breaches and system anomalies.



The Benefits and Burdens of Remote Access

Remote access has enabled an entirely new paradigm of workplace flexibility and productivity. Indeed, the very meaning of the word "workplace" must be redefined to be less location-specific, and more worker-specific. The adoption of mobility enhancing tools such as tablets, smartphones and other devices has transformed many enterprise roles into an any place, any time proposition. Workers have benefited from schedules that offer more flexibility, helping to enhance both work- and home-life. Companies have benefited from the leaps of productivity that remote access enables.

But this ongoing paradigm shift has required that enterprises find ways to balance the protection of sensitive data with the impact of remote access upon user flexibility — the widespread use of VPNs over unsecured networks, for example.

While remote access does increase the burden of safeguarding enterprise systems and data, the benefits of remote access justifies the need for an increased focus upon security. The Citrix Ready Secure Remote Access program is designed to help enterprises conform to the five security pillars listed above while meeting the skyrocketing demand for more remote access capabilities.

AppSense has been selected to participate in the Citrix Ready Secure Remote Access program. The AppSense DesktopNow Plus Platform integrates seamlessly with Citrix products in delivering fully personalized, dynamic desktops for all end users and has demonstrated the ability to support the five security pillars of the Secure Remote Access program.

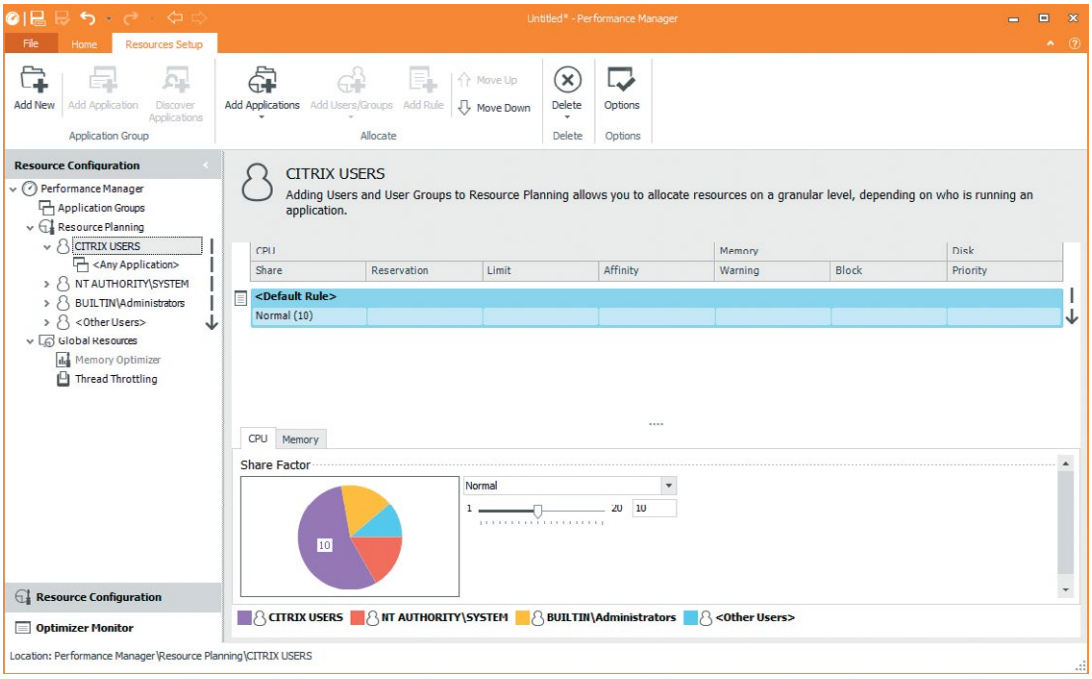
AppSense secures virtual desktop infrastructures while simultaneously improving user acceptance of XenApp and XenDesktop environments, removing risks to both enterprise security and worker productivity when implementing a desktop virtualization project. The solution supports the use of a single golden image as a virtual desktop template, accelerating virtual desktop deployments for both physical-to-virtual and virtual infrastructure upgrades. The number of use cases is increased for virtual desktops by removing transition and configuration issues.

AppSense maximizes the number of users per server supported on existing hardware, lowering server and storage costs. AppSense architecture also offers unequalled scalability, expandable to hundreds of thousands of users across multiple site locations. The solution enables the deployment of reliable, highly available desktops in mission critical environments. Ultimately, AppSense provides a practical and cost-effective means of future-proofing existing Citrix investments.

Key features of AppSense include:

- **Scalability:** The solution architecture supports massive and easy scalability, capable of serving hundreds of thousands of users across multiple locations. AppSense scalability is not just a claim; it is demonstrated daily through service to eight of the world's top 10 banks.

- **Granularity of Control:** Provides unequalled out-of-the-box functionality. Admins have more flexibility, greater control and enhanced self-sufficiency.
- **Performance:** Patented technology enables across-the-board quickness that delivers a better user experience by speeding common tasks such as user logons and file delivery. A multi-tiered backend database infrastructure provides full enterprise resilience along with fast and efficient operations.
- **Cloud-Ready:** HTTPS architecture assures an easy transition to the cloud for organizations considering offsite operations, including distributed datacenters.
- **Simplified Security:** The unique AppSense approach lightens the administrative load involved with managing user permissions.
- **Contextual Control:** Integration with Active Directory provides a unique level of contextual control of users through the monitoring of many user variables such as location, device and much more.



Overview of AppSense

The superior granularity of application control offered by AppSense helps to stop ransomware and other malicious executables. Privilege management on a per-user / per-application basis provides IT with greater control over admin rights. A common problem for thousands of users, “double hop” — a logged-on remote user able to logon to another desktop or access unauthorized backend systems — has been eliminated through Application Network Access Control, an AppSense feature.

AppSense sophisticated and highly flexible personalization of a single golden image or virtual desktop template facilitates one desktop for all different users, e.g. task-workers, professionals, systems administrators etc. This radically reduces the cost and effort of managing desktop updates, e.g. “patch Tuesday”. Also, the ability of users to securely self-serve in accessing and running applications and modifying workspace settings reduces support costs, improves the user experience and increases productivity.

AppSense works to enhance productivity by:

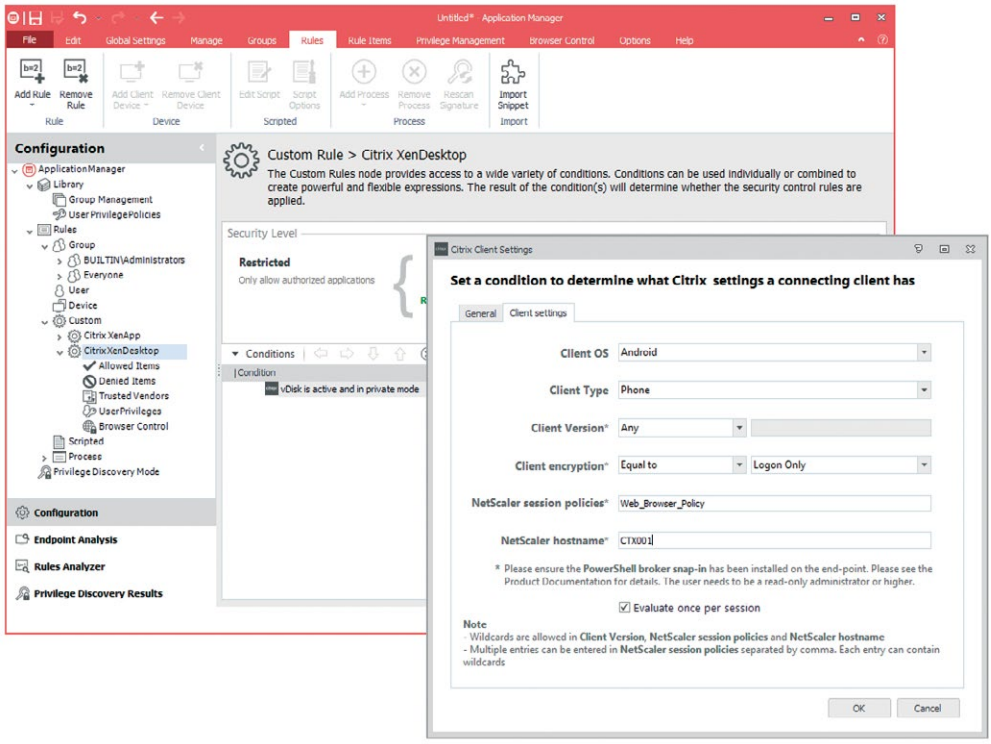
- Simplifying policy configuration
- Eliminating logon scripts and GPOs for faster logons
- Eliminating profile corruption
- Improving workspace and application response times

AppSense enhances security by:

- Providing endpoint application visibility
- Providing user activity details (who is using what)
- Stopping unauthorized scripts
- Enabling control without relying on traditional blacklists and whitelists
- Empowering users to run apps securely
- Recognizing imminent security threats
- Providing data protection
- Strengthening privilege management
- Simplifying policy management
- Taming GPO sprawl
- Providing context-aware access to network resources

The integration of AppSense with Citrix products provides a number of unique benefits. Removing unnecessary admin rights, protecting endpoints, reporting on risky behavior and enabling regulatory compliance all work to increase security without degrading the user experience. Providing users with the applications, personalizations and privileges they need in the performance of their jobs fosters a sense of empowerment, and in turn helps to increase user acceptance of digital workspaces. On-demand personalization and fine-grained, contextual policy control also work to optimize the user experience while helping to protect endpoints.

Successfully implementing and managing VDI requires fewer resources and less manual effort by focusing on end user needs, while the application of simple controls helps to secure VDI endpoints and boost performance. In sum, the integration of AppSense with Citrix enables more productive end users, from any location, on any device, with IT empowered to centrally manage all aspects of the user workspace.



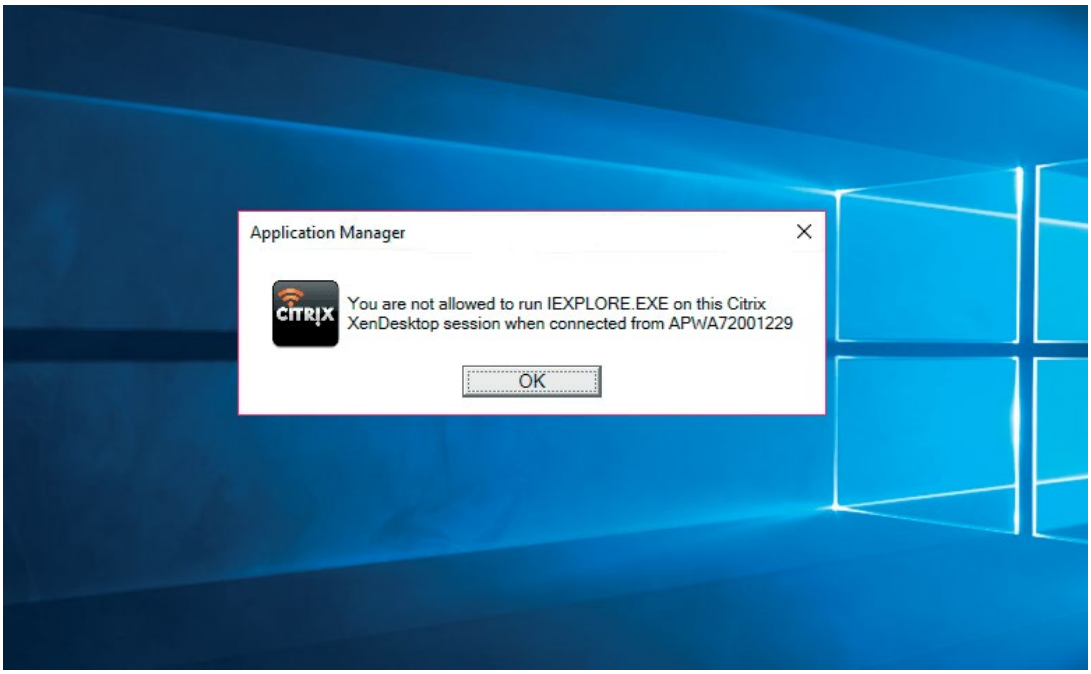
AppSense unique offerings include:

- Security based upon Trusted Ownership™: the ability to enforce application access policy without scripting or list management
- Comprehensive context-aware security policies
- On-demand personalization across physical and virtual desktops and servers, irrespective of OS, platform or app delivery mechanism
- License management for auditable, controlled access to applications within a VDI image
- Per-device license control
- Multi-threaded logon scripts and policy engine that provides fast user logons
- Patented CPU Thread-Throttling resource control

AppSense Solution Detail

Each managed endpoint, whether a Citrix XenApp Server, a virtual desktop delivered by XenDesktop or a physical device, requires an agent and an associated configuration deploying to it. The agents and configurations are self-contained and can continue to work offline without any backend infrastructure.

An optional three-tier solution can be implemented to manage deployment of agents and configurations, and to store user personalization settings as required. Small virtual appliances (with associated web interfaces) can be used to provide endpoint analysis into user workspaces or to act as a secure broker for file sync with on-premise data storage.



AppSense and Citrix share a user-centric view of enterprise computing. As the leading secure user workspace solution recommended by Citrix, the AppSense DesktopNow Plus Platform enables rapid, seamless, low-cost migration to a Citrix environment, and provides a personalized physical-to-virtual user experience while reducing IT operation and infrastructure costs.

Citrix FlexCast technology enables IT departments to deliver "IT as a Service" to all users, from any location and through any accessing device. AppSense DesktopNow Plus extends these capabilities by configuring the desktops and applications based on the user, location, time, network connection and device context, ensuring a secure, personalized experience across the entire Citrix FlexCast platform.

AppSense allows rapid planning, integration and deployment of virtualized desktop solutions with less risk, lower cost and increased user satisfaction, making it easier to transform desktop computing environments. As Citrix FlexCast delivers a pristine desktop and application environment for the user, AppSense ensures that the desktop is dynamically tailored and personalized to their requirements, moving the end-user settings from their physical PC to their virtual desktop and back again without the user ever having to think about the technology — all while securing the user workspace, increasing productivity and simplifying IT administration.

A Proven Partnership to Enhance the Security and Productivity of Digital Workspaces

Citrix and AppSense have forged respected reputations as industry leaders in their respective areas of expertise. AppSense is a distinguished founding member of the Citrix Ready program, and in 2010 Citrix named AppSense the Citrix Ready Solution Provider of the Year. This annual award recognizes the company that best excels in delivery solutions complimentary to Citrix technology, and that plays an integral role in driving the adoption of Citrix solutions.

Working together, Citrix and AppSense have made great strides in aligning product development, enhancing the adoption, security and usability of digital workspaces. The result has been a thriving, prosperous relationship between AppSense, Citrix and thousands of joint customers and partners worldwide. This enduring relationship ensures that AppSense customers are provided with leading-edge secure user workspace solutions and future-proof technologies, providing a worry-free, long-term investment for all clients.

For more information about AppSense, please visit: http://www.appsense.com/

To learn more about the Citrix Ready Program partnership with AppSense, please visit: https://citrixready.citrix.com/appsense-ltd.html

Appendix

Learn more about the enterprise security advantages provided by Citrix NetScaler Unified Gateway at: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/best-practices-for-enterprise-security.pdf

To learn more about security solutions for business enterprises, contact Citrix and AppSense.

To view success stories from some of AppSense's 3,500 customers, please visit: http://www.appsense.com/customers/

About Citrix Ready

Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.

About AppSense

AppSense is the leading provider of User Environment Management solutions for the secure endpoint. AppSense technology allows IT to secure and simplify workspace control at scale across physical, virtual and cloud-delivered desktops. AppSense solutions have been deployed by 3,600 enterprises worldwide to nine million endpoints. AppSense is part of the LANDESK family with offices around the world. For more information, please visit www.appsense.com.