xage SECURITY

Enhancing Security using Xage Zero Trust Access with Single Application Mode

To strengthen the security posture of remote desktop environments by enforcing **Single Application Mode**, ensuring zero-trust and least-privilege access principles by restricting unauthorized access and minimizing the attack surface.

Key Features and Benefits

1. **Zero Trust and Least Privilege Access for Specific Applications**
   - Enforces access policies at the application level, allowing users to interact only with predefined applications on a remote RDP host.
   - Limits exposure to sensitive resources and data by granting only the minimal privileges necessary for task completion.

2. **Stops Lateral Movement**
   - Restricts the user's ability to navigate beyond the authorized application environment within the network.
   - Prevents attackers from leveraging compromised sessions to explore or exploit other systems within the network.

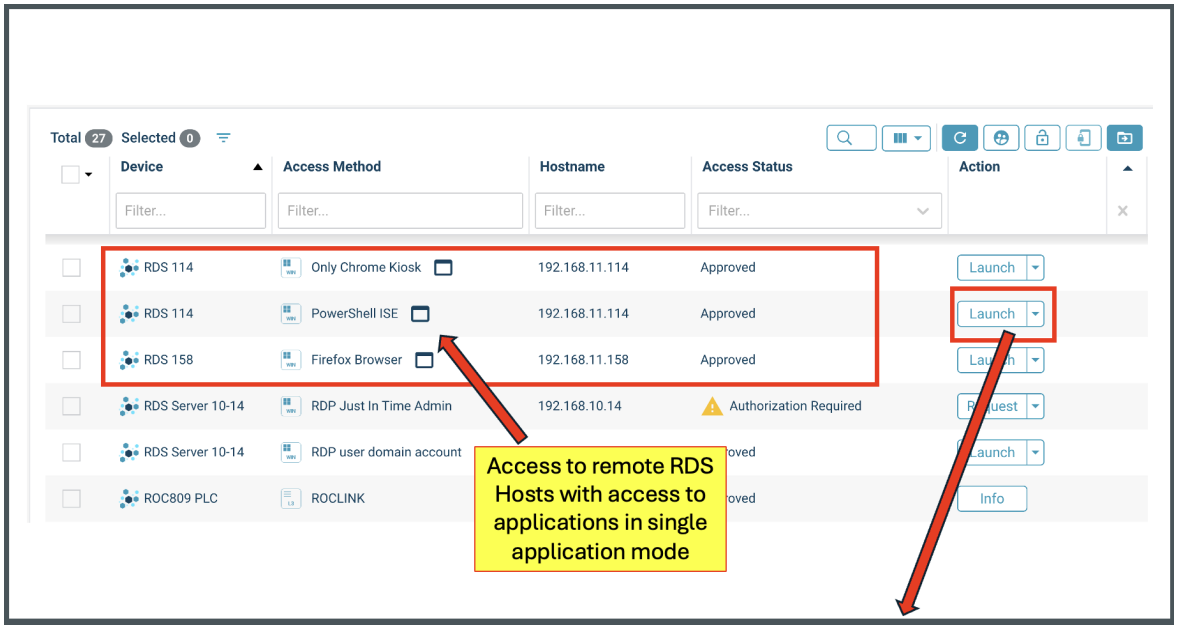
3. **Application-Level Access Control**
   - Provides granular control over which applications users can launch, eliminating access to unauthorized programs or system tools.
   - Ensures compliance with organizational policies by enforcing strict usage constraints.

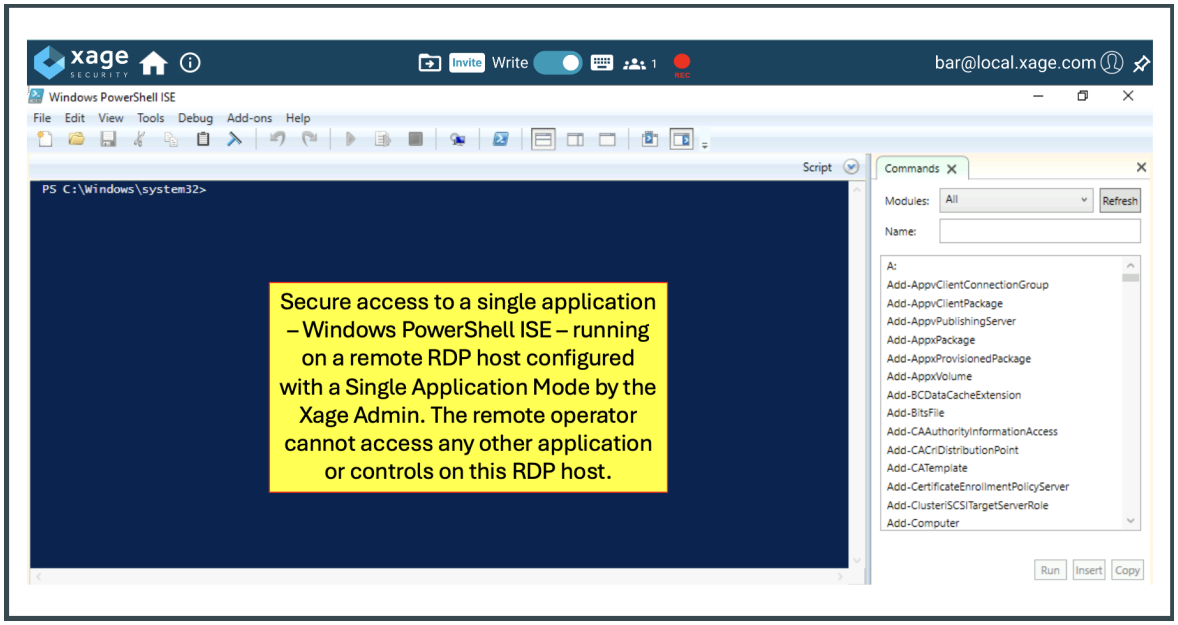
4. **Credential Management and Single Sign-On (SSO)**
   - Integrates credential management tools to securely store and automatically provide credentials for authorized applications.
   - Simplifies user experience through SSO, reducing password fatigue and decreasing the likelihood of credential misuse.

xage SECURITY

5. **Support for Kiosk Mode**
   - If supported by the underlying application, Kiosk Mode ensures a streamlined environment by allowing only a single instance of the application to run.
   - Prevents users from opening multiple instances or accessing unintended functionalities.

6. **Prevention of Unauthorized Access**
   - Utilizes robust authentication mechanisms and policy enforcement to block access to applications not explicitly permitted for remote contractors and 3rd party technicians.
   - Strengthens security by ensuring only contractors and 3rd party technicians that are allowed by the Xage's zero trust policies interact with the designated application.





Implementation Advantages

Enhanced Security

Mitigates risks of unauthorized access, credential theft, and lateral movement attacks.

Improved Compliance

Supports regulatory requirements by maintaining strict access and usage controls.

Streamlined Operations

Simplifies user workflows and enhances productivity while ensuring security remains uncompromised.

Conclusion

Xage Zero Trust Access with Single Application Mode is a critical security measure for organizations relying on remote RDP environments. By enforcing zero trust, limiting user actions, and integrating access controls, it delivers a robust solution to mitigate risks, ensure compliance, and safeguard sensitive resources against threats.

About Xage Security

Xage Security is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere, while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.

xage SECURITY