Delinea

Both RDP Launcher and PRA Launcher offer secure remote access solutions, but they differ in their integration, security features, and session management capabilities. RDP Launcher is more tightly integrated with Secret Server, while PRA Launcher offers broader accessibility and integration with the Delinea Platform.

Here's a comparison between RDP Launcher and PRA Launcher based on the information retrieved:

RDP Launcher	VS	PRA Launcher

Launcher

RDP Launcher

Integration with Secret Server:
RDP Launchers are integrated with Secret Server, allowing users to initiate Remote Desktop Protocol (RDP) sessions directly from the Secret Server interface using stored credentials. This integration enhances security by minimizing the exposure of sensitive credentials.

Security Features:
Credentials are automatically retrieved and used from Secret Server, ensuring encrypted and secure exchanges. RDP Proxy can be configured to prevent secret credentials from reaching the client machine.

Customization and Policies:
Secret owners can enforce RDP launcher policies to control settings like clipboard access and drive mapping. Custom launchers can be created for any application that can be started via the command line.

Browser and Network Configuration:
Requires specific browser configurations and network settings, such as SSL certificates and .NET framework, for proper operation.

Session Management:
Supports session recording and keystroke monitoring if configured. RDP sessions can be launched using short-lived credentials for enhanced security.

PRA Launcher

Integration with Delinea Platform:
PRA (Privileged Remote Access) runs entirely on the Delinea Platform interface, providing seamless access to remote machines through RDP and SSH without the need for a VPN.

Security Features:
Automatically uses credentials to connect with target resources, enabling RDP and SSH connectivity without exposing sensitive parts of credentials to the end user. PRA sessions can be configured to be viewed in real-time and recorded for security auditing.

Portability and Accessibility:
PRA sessions are displayed in the user's web browser, eliminating the need for additional remote access or VPN software. This makes PRA extremely portable and accessible from any location with an internet connection.

Engine and Site Management:
PRA uses engines to connect outbound traffic from your data center to the Delinea cloud, protecting your data center from exposure. Multiple engines can be added for redundancy and high availability.

Session Management:
PRA sessions are integrated into the Delinea Platform UI, allowing users to manage multiple connections to multiple target systems, each running in its own browser tab.

Resources:

RDP Launcher

For more details, you can refer to the following resources:

Remote Desktop Launchers

RDP Proxy Configuration

PRA Launcher

For more details, you can refer to the following resources:

Using PRA

Privileged Remote Access

Choose RDP Launcher for tighter integration with Secret Server and on-premises control, and opt for PRA Launcher for cloud-based, VPN-less access with enhanced portability and session management features.

The choice between using an RDP Launcher and a PRA Launcher depends on your specific needs and the environment in which you are operating. Here are some guidelines to help you decide when to use each:

Delinea

RDP Launcher VS PRA Launcher

When to Use

Integration with Secret Server:
If your organization primarily uses Secret Server for managing credentials and you need a solution that integrates directly with it, RDP Launcher is a suitable choice.

On-Premises Environment:
RDP Launcher is ideal for environments where the infrastructure is primarily on-premises and you have control over the network and security configurations.

Custom Application Launching:
If you need to create custom launchers for applications that can be started via the command line, RDP Launcher provides this flexibility.

Policy Enforcement:
Use RDP Launcher if you need to enforce specific RDP session policies, such as clipboard access and drive mapping, across all users of a secret.

Secure Credential Handling:
If you require a solution that ensures credentials are not exposed to the client machine, RDP Launcher with RDP Proxy can provide this level of security.

Cloud Integration:
If your organization uses the Delinea Platform and requires seamless integration with cloud services, PRA Launcher is the better option.

VPN-less Access:
PRA Launcher is ideal for scenarios where you need to access remote systems without a VPN, providing secure access through the Delinea cloud.

Portability and Accessibility:
Use PRA Launcher if you need a solution that allows access from any location with an internet connection, without the need for additional software installations.

High Availability and Redundancy:
If your environment requires high availability and redundancy, PRA's ability to manage multiple engines and sites makes it a suitable choice.

Real-time Session Monitoring:
PRA Launcher is beneficial if you need real-time session monitoring and recording for security auditing purposes.

Regular RDP Launchers are best suited for controlled, on-premises environments with specific policy enforcement needs, while PRA Launchers are ideal for remote access scenarios, cloud integration, and environments requiring high availability and real-time monitoring.

Here are some typical use cases for both the regular RDP Launcher and the PRA Launcher:

Use Cases

Internal IT Support:
IT teams can use RDP Launchers to securely access and manage internal Windows servers and workstations without exposing credentials to end-users.

Controlled Access to Sensitive Systems:
Organizations can enforce strict access policies for sensitive systems by using RDP Launchers to control who can access these systems and under what conditions.

Custom Application Launching:
RDP Launchers can be configured to start custom applications that require specific command-line parameters, making them suitable for specialized internal applications.

Policy Enforcement:
Use cases that require consistent enforcement of RDP session policies, such as disabling clipboard access or drive mapping, can benefit from the policy enforcement capabilities of RDP Launchers.

On-Premises Infrastructure Management:
Organizations with primarily on-premises infrastructure can use RDP Launchers to manage their systems securely and efficiently.

Remote Workforce Enablement:
PRA Launchers are ideal for organizations with remote employees who need secure access to corporate resources without a VPN.

Third-Party Vendor Access:
Companies can provide secure, temporary access to third-party vendors or contractors using PRA Launchers, ensuring that access is controlled and monitored.

Cloud-Based Operations:
Organizations operating in a cloud environment can use PRA Launchers to integrate seamlessly with cloud services and manage remote systems without additional software installations.

High Availability and Redundancy:
Use cases that require high availability and redundancy, such as critical infrastructure management, can benefit from PRA's ability to manage multiple engines and sites.

Real-Time Monitoring and Auditing:
PRA Launchers are suitable for environments where real-time session monitoring and recording are necessary for compliance and security auditing.

For more content like and follow me:  **@bertblevins**