AIRGAP

SOLUTION BRIEF

Secure Asset Access

Protect your organization against breaches due to lost or stolen credentials with strong MFA authentication.

Each year, thousands of enterprises are silently attacked by malicious cybercriminals who seek to compromise enterprise applications through the use of brute-force attacks, guessing weak passwords, or more effectively by leveraging stolen credentials (aka "Credential Stuffing"). For an enterprising cybercriminals, compromised credentials provide direct access onto an enterprise through an insecure application, enabling them to easily exfiltrate sensitive corporate data.

Organizations have responded by enabling Multi-Factor Authentication on employee access to their SaaS and Cloud Application through their (Single-Sign on) SSO providers. The use of MFA protects these services by providing an additional layer of security validation such as phone or token to verify a user's identity before granting access. A cybercriminal who might have guessed or obtained an enterprise user credentials would be immediately blocked at the next stage of authentication.

Unfortunately, authentication to legacy applications have not caught up with modern cloud-based applications, creating a blind-spot for organizations. An enterprise application that is in active use by users can attract the attention of cybercriminals who recognize it as a vulnerable entry-point to gain access to an organization.

Closing the Gap of Multi-Factor Authentication

Airgap's Asset Access (SAA) solution was built to immediately close the authentication gap with legacy enterprise applications with a seamless MFA(Multi-Factor Authentication) solution. Sitting behind a customer existing VPN solution, Airgap SAA provides legacy applications with a modern MFA authentication that exactly mirrors how users are granted access to existing SaaS and Cloud based applications. Integrating with the organization's existing SSO provider, security teams can extend the second layer of MFA authentication across all applications. What results is universal MFA authentication across all applications, extending an extra layer of security across an entire organization.

Strong Authentication Enforcement

- Security-First principles with multi-layer defenses
- User/device trust-based authentication using SSO
- Dual trust access control (Airgap & Enterprise specific)
- PKI based certificate exchange and strong encryption

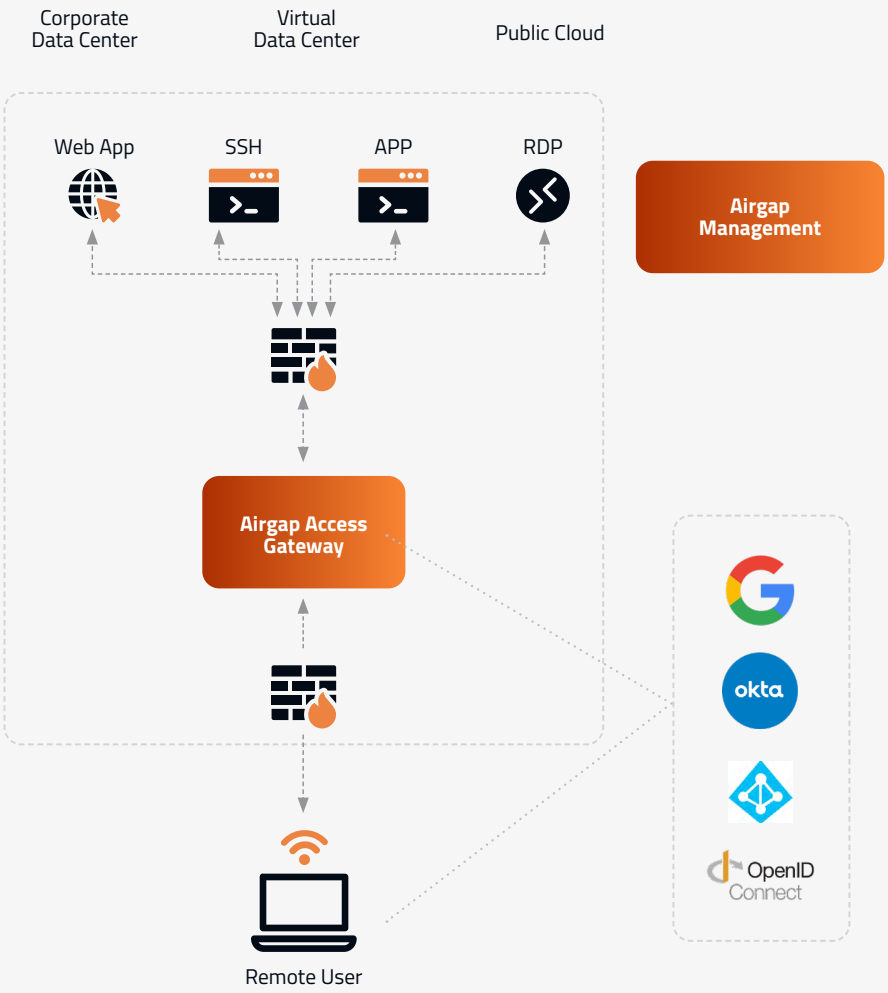
Secure Web and Non-web App Connectivity

- Application network infrastructure hidden from the users
- Protect from RDP-Based Protocol Vulnerability
- Multiple layers of firewall and access control checks

Any Device. Any Application. Any Location.

- Cloud hosted and delivered as a SaaS
- Support non-web protocols: SSH, RDP
- Works with native OS apps/ browsers

AIRGAP



Seamless Deployment

Requiring no changes to an existing VPN's security policy, it works transparently sitting behind your VPN as a virtual appliance to enable MFA authentication for your legacy enterprise applications. Users who need access to a variety of applications in order to get work done will be required to identify themselves via MFA before being granted access to an application. For example, If a user that needs to access a RDP server or a legacy banking application will be confronted with MFA authentication to verify their identity before they are granted legitimate access to critical applications.

Organizations need a solution that can ensure private applications are **accessed securely** while delivering a **frictionless user experience.**

Securing Web and Non-Web Application Access

Across both web and non-web applications, Airgap SAA can enable MFA authentication. It builds upon MFA authentication by also analyzing user traffic and preventing

AIRGAP

attempts to breach the applications, essentially acting as a web application firewall. An end-user clicking on a phishing email or browsing to malicious websites can download malware. Direct and network level access can lead malware to compromise a vulnerable or unpatched application and subsequently the rest of the organization. Airgap SAA protects all application bound traffic, analyzing against a comprehensive threat signature database. For compliance and audit purposes, Airgap SAA also can act as digital video recorder (DVR), enabling all connected sessions to be recorded, ensuring that 3rd party contractors are monitored and don't pose a risk as risky insiders. All sessions are recorded to the cloud and can be viewed as needed especially for compliance and auditing purposes.

Ransomware Kill Switch™ and EDR Integration

Customers who deploy Airgap's Ransomware Kill Switch for Endpoints with leading EDR solutions can also gain an additional layer of granular security policy that helps to regulate user access to applications. For example, a policy can be constructed where a contractor who should not have full access to finance or Active Directory servers will be restricted in their access to those specific corporate resources. Furthermore, Airgap's Ransomware Kill Switch for Endpoints can enable a posture based access mechanism that can be established for endpoints that have vulnerable operating system versions, lack of security patches or high-risk applications, etc. In this way, customers can implement a security access policy that is dependent on the security posture level of all endpoints. This additional layer of security ensures that access security policies can be granularly defined to include endpoint security posture levels, restricting access as needed.

Use Cases

Enable MFA for Legacy Applications

- Extend MFA capability provided by your SSO (Single-Sign on) provider to your legacy applications

Granular Policy Access

- Integration with Airgap's Ransomware Kill Switch can enable granular policy access to corporate applications.

Block Web Application threats

- Identify and block web threats such as malicious malware from insecure endpoints

BENEFITS

Reduced Enterprise Security Risk

By deploying Airgap SAA, you're reducing the risk of cyber-breach by ensuring that an additional layer of security blocks illegitimate access to your application.

Universal MFA

Seamless user experience with Multi-Factor Authentication(MFA) integration across all your SaaS and hosted applications.

Enable Zero Trust Security

Enable the strongest authentication and authorization protocols to ensure that least-privilege access is enabled for all users and applications within your organization.

Maintain your VPN investment

SAA deployment is seamless, enabling enterprises to continue to maintain their existing VPN deployment and security policies.

Additional Layer of Security

Seamlessly enable an additional layer of authentication security without any disruption to your existing security and network infrastructure.

AIRGAP

Use Cases *(continued)*

Posture-Based Access

- Restrict access to legacy applications from low security posture endpoints

DVR (Digital Video Recorder) Playback

- Selectively record each user session for security, training, and compliance purposes

Summary

With recent rising Ransomware attacks from Colonial Pipelines to Kaseya attacks, cyber criminals are leveraging out-of-date remote access solutions and weak authentication protocols like RDP or TeamViewer to infiltrate the enterprise infrastructure. Unlike other legacy solutions that might check a device only at the beginning of an application session, Airgap SAA adapts to your current network security configuration without fork-lifting migration and delivers the cloud-like seamless application access innovation to monitor with the IdP SSO enforcement throughout the application session. Airgap Secure Asset Access, SAA, practices security-first principles and enforces the integrated SSO before accessing any applications, from any device and any location. For more information or a demo, contact **info@airgap.io**.

BENEFITS

No disruption to your infrastructure

Airgap SAA deployment does not require any changes to your existing infrastructure.

Granular Access Policy

Enable granular security access policy that can define user, group, device risk posture to ensure that high-risk users or devices do not have unrestricted access.

Future-Proof your security investment

No changes are required to your existing VPN, SSO, security infrastructure or enterprise security policies to implement Airgap SAA.

About Airgap

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication.

airgap.io

AIRGAP