AppConnect and AppTunnel: Advanced Security for Mobile Apps and Data

The sharp rise in mobile and cloud technologies enables global enterprises to ramp up productivity like never before. With that productivity comes a great challenge – and a great opportunity – for your mobile security team. Success in the Everywhere Workplace means securing the devices, app and cloud services that access critical enterprise data. Here's what that looks like:

- Securely enabling personal devices for work.
- Ensuring personal apps can't access enterprise data and cloud services.
- Protecting data-at-rest on the device and in transit to the cloud or enterprise backend.
- Preventing data from being shared or accessed through unauthorized apps, such as a personal version of Office 365.

AppConnect and AppTunnel work together to help you meet all these mobile and cloud security requirements.

AppConnect

AppConnect containerizes apps to protect app data-at-rest without touching personal data. Each app becomes a secure container. Within that container, data is encrypted, protected from unauthorized access, and removable. Each app container is also connected to other secure app containers through the Ivanti management platform, so policies such as app single sign-on (SSO) can be easily shared and updated across devices.

AppTunnel

AppTunnel protects network data with a dynamic multi-OS app VPN that supports Android and iOS devices. AppTunnel provides granular, per-app session security to connect each app container to the corporate network. As a result, organizations can secure traffic from enterprise apps without interfering with personal traffic, such as a user posting a family photo on social media.

Key benefits

- Secure app data on the device and in transit to the cloud or enterprise backend.
- Separate enterprise and personal apps and data on the device.
- Enable secure app access without a VPN.
- Configure, deploy and update apps and policies - no user intervention required.
- Support both SDK and wrapping methods for app containerization.
- Deploy across Android and iOS devices.
- Administer in-house and public apps.

Capabilities

AppConnect

AppConnect creates a secure app container through either an SDK and wrapper (iOS) or a wrapper (Android). This container connects to other secure app containers through the Ivanti console and provides management capabilities like these:

- **Authentication.**
  Confirm identity through domain username and password or certificates so only approved users can access business apps.
- **SSO.**
  Simplify user authentication across app containers.
- **Authorization.**
  Allow or block app usage or storage based on device posture.
- **Configuration.**
  Configure and silently push personalized settings such as username, server name and custom attributes without requiring user intervention to activate.
- **Encryption.**
  Ensure that all app data stored on the device is encrypted.
- **DLP controls.**
  Set data loss prevention (DLP) policies, such as copy/paste, print, and open-in permissions so sensitive data doesn't leave the container.
- **Dynamic policy.**
  Update app policies across all managed devices or a subset of devices based on group, user role and other factors.
- **Reporting.**
  Generate detailed app usage statistics, audit logs and other reports to improve management and simplify compliance.
- **Selective wipe.**
  Remotely wipe enterprise apps and data without touching personal data.

AppTunnel

AppTunnel provides several layers of security for mobile app data without requiring a VPN. Capabilities include:

- **Unique connection.**
  Allow only authorized apps, users and devices to connect to enterprise resources.
- **Certificate-based session authentication.**
  Effortlessly configure devices with identity certificates and VPN configurations, enabling seamless and secure enterprise access for the employee.
- **Access control rules.**
  Block network access if app-side security is compromised.
- **Ivanti Sentry.**
  AppTunnel builds upon the Sentry technology, which provides an in-line gateway that manages, encrypts and secures traffic between the mobile device and backend enterprise systems.
- **Ivanti Access.**
  AppTunnel also supports Ivanti Access, which ensures only authorized endpoints, users, apps and cloud services can access enterprise data and provide additional security through multi-factor authentication.

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work.
For more information, visit www.ivanti.com

ivanti.com
1 800 982 2130
sales@ivanti.com