FireDroid enables organisations and end-users to retain control of corporate data across mobile devices by:

- **Controlling the behaviour of Apps** by providing an extensible set of security policies that can be enforced without the need of repackaging or modifying the Apps or the underlying OS.
- **Seamlessly separating personal and corporate data** using standard native Apps without disrupting the user experience.
- **Allowing real-time monitoring of corporate data** access and dissemination patterns and singling out abnormal or suspicious behaviours as soon as they happen.

FireDroid targets Android and monitors and mediates ALL application behaviour through a policy based mechanism with low overhead. Among others, FireDroid provides the following main features:

**Patching**
Critically, it enables quick patching of vulnerabilities, such as the well-publicised Heartbleed. Patches can be developed using an IDE extension coupled with a cloud-based management console to deploy patches Over-The-Air to the enrolled devices.

**Native App Control**
Dissemination of corporate data (such as emails, attachments, business meeting details, etc.) is strictly controlled using unmodified native Apps.

FireDroid can stop the native email client sending corporate data to unauthorized or non-corporate recipients. Additionally, attachments can be viewed and edited by only corporate authorised Apps.

**Per-app Policies**
Pre-installed system Apps and third-party Apps downloaded by the user can be controlled independently allowing administrators to specify App-specific policies. Furthermore, app domains can be used to provide a higher degree of control and productivity.

Only corporate Apps can have access to the corporate VPN and use corporate-grade data encryption. Access to corporate data and/or specific device resources can be defined independently for each App.

**Context-based Policies**
Policies enforcement takes into account contextual information. This enables context-fencing through multiple dimensions such as geolocation, date and time, and device state.

Allow a device to behave as a pure corporate device in certain locations such as meeting rooms or provide an extra degree of security and productivity by, for instance, disabling the camera for non-corporate Apps, or completely block access to all corporate data if the device state has been compromised.

**Unrestricted App Choice**
One of the main advantages of today's mobile operating systems is being able to select from a wide variety of Apps for the tasks at hand and dynamically change the installed Apps to meet the requirements of an ever-changing corporate environment. However, to protect the confidentiality of the corporate data, each App has to be securely controlled and the security policies have to be correctly enforced.

Any App can be controlled without the need to modify/repackage the App. Apps will be automatically under control as soon as they are installed and executed on the device.

**Seamless User Experience**
To be productive, users have to execute multiple Apps and switch between them effortlessly. Disrupting the user experience by enforcing cumbersome security checks will negatively impact the user productivity.

Users can seamlessly move between Apps executing their business and personal tasks while security policies are enforced in the background. The user might be aware of FireDroid only if they violate security policies.

**IP Position**
Granted patent in the United States, various patents pending in the United States and China.
OS/Vendor Agnostic

FireDroid enables the specification and enforcement of policies independently of device-specific characteristics. In contrast, all Mobile Device Management (MDM) solutions are limited to vendor-specific API, which over complicates the configuration as each device may support a different set of policies.

Administrators can specify just one security configuration across the whole fleet of devices.

Domain-specific Policies

Vendor-specific policies are device-wide meaning that they would apply to the whole set of apps installed on the device. For instance, remote deletion of data would affect both corporate and private data. FireDroid provides support for policies that will apply to just a subset of the Apps and/or data on the device.

Once an employee leaves the company, the corporate data can be wiped by the administrator, leaving the personal data on the device untouched.

Alerts and Logs

All the operations Apps execute are actively monitored. When an App executes unauthorised/suspicious operations alerts are sent in real-time to the system administrator. Logs are also collected and can be sent to the system administrator for further analysis.

The corporation can be made aware of a potential confidential information leak as soon as it happens.

The University of Auckland

The University of Auckland is New Zealand’s world-ranked university. We rank in the top 100 in the QS World University Rankings, and are the only New Zealand university ranked among the world’s top 200 universities by the Times Higher Education World Rankings of Universities. The University of Auckland is also the highest ranked New Zealand university in the Shanghai Jiao Tong Academic Ranking of World Universities.

The University of Auckland is an international centre of learning and academic excellence. It is New Zealand’s pre-eminent research-led institution and has key linkages with many of the world’s top research intensive universities. The University actively seeks to work with government, other universities, research organisations, businesses and commercial consultancies in research, development and education.

Established in 1883, it is an international centre of learning and academic excellence. It is New Zealand’s largest University with over 5,000 full-time staff, 8,000 casual staff and 40,000 full-time students, including over 5500 international students.

Auckland UniServices Limited

Auckland UniServices Limited is the commercial research, knowledge transfer and custom education company for the University of Auckland - dedicated to connecting the University’s capabilities to business and investors, Government and the community. UniServices is a wholly-owned company of the University of Auckland.

In just 25 years UniServices has grown to produce an income of over NZ$130 million per annum, far surpassing any similar organisation in New Zealand and Australia. Our income derives from contract research and consulting, customised education programmes for 25,000 students around the world and from transferring intellectual property developed by staff and students at the University to the public and private sectors.

We are a substantial organisation with over 600 employees, working in 37 countries, and with access to many more academic staff from the University of Auckland. The work of UniServices supports the leadership position of the University of Auckland, and allows the University to expand and enhance its capabilities in commercial and basic research.

Contact

Stephen Flint
Commercialisation Manager
📞 +64 9 923 4989 or +64 21 240 3076
s.flint@auckland.ac.nz

Auckland UniServices Limited

Level 10, UniServices House, 70 Symonds Street, Auckland
Private Bag 92019, Victoria Street West,
Auckland 1142, New Zealand
📞 +64 9 373 7522 | www.uniservices.co.nz