What is zIPS?

Zimperium Mobile Threat Defence (zIPS) is an enterprise class, on-device security engine for Android and iOS devices that protects your mobile device against harmful WIFIs and malicious apps. Developed for mobile devices, Zimperium uses patented, behaviour-based analytics on the device to detect threats in real time. The app has also been optimized for battery consumption to ensure a great user experience.

Isn't my antivirus app sufficient?

No, signature-based technology can't keep pace or protect against unknown or dynamic threats. It protects for known malware and it can take days to update the databases. It won't protect you against mobile network attacks and device exploits either.

What about my privacy?

zIPS only collects threat and device information in the event of an attack. This information is used to make the device owner aware and help take steps to remediate the problem.
To further protect user privacy, zIPS does not view, store or send any information such as location, contacts, email, SMS or browser traffic flowing through your mobile device.

How does zIPS work?

Much like a doctor can diagnose an illness by analysing the symptoms your body is exhibiting, zIPS can detect both known and unknown threats by analysing the behaviour of your mobile device. By analysing slight deviations to the mobile device's operating system's statistics, memory, CPU and other system parameters, the detection engine can accurately identify not only how the attack occurred but also recommend actions to take to help keep your data and mobile safe.

Are there any other benefits to this on-device protection solution?

Yes, since the solution is on-device, it doesn't require an internet connection. So the detection and alerting is real-time and no latency is introduced. This also means that a device can be protected in airplane mode and when roaming – unlike security solutions that depend on an internet connection and that attackers can easily take down when a device has been compromised.

Why Should I Care?

Today we use our mobile your mobile for both personal and work related activities. 90% of our mobile usage is attributed to infotainment apps, productivity apps, e-commerce apps and search engines. But a third (3.3 million apps) of the apps available to us today are malware capable of stealing your personal, banking and enterprise data from your device. This risk is further amplified when you habitually connect to free Public Wi-Fis for faster connectivity and better mobile experience. Hackers are well aware of these behaviours and lurk in popular places to exploit your mobile device.

What happens when there is an attack or threat detected on my device?

In the event of an attack zIPS first alerts you on your device via a notification. Upon clicking the notification, you will be able be taken into the app to see additional information regarding the threat and and remediation actions you can take to help remain safe. The threat information is also reported to your Enterprise's Security Group to ensure they can help keep other users and the enterprise safe from similar

threats.

What are some key features of zIPS?

- On Device Protection; doesn't need internet connectivity
- Protection from Malicious Apps
- Protection from harmful WIFIs
- Protection from known and unknown threats (Mobile Handset Protection)
- Recommendations and decisions when malicious activity is discovered.

Who can I contact to get more information about zIPS?

https://www.zimperium.com/zips-mobile-ips

I have an iOS device. Am I still vulnerable?

iOS devices have been proven to be vulnerable time after time. All the major OS versions had publicly available jailbreaks within days of the updates making them significantly more vulnerable.

What is the typical battery usage for zIPS?

zIPS consumption on average ranges between 0.3% to 0.8% per hour depending on your usage throughout the day.

I have an iOS device, is my device protected if I swipe off the App?

Yes. The app communicates with the server periodically and runs in the background. zips will alert you only in case of threats and as per the alerting policy set forward by your administrator.

What happens when there is an attack or threat detected on my device ?

First zIPS sends automated alerts to both the Security Group and the device in the event of an attack. Further remediation actions on the device will automatically occur as defined within Enterprise Threat Management Policy.

Who can I contact to get more information about zIPS or Threat Management Policy?

<Customer to fill in the details of the Internal Support Contact>

I forgot my password to log into zIPS, how can I reset it? (Applicable for manual login)

Please contact your Administrator (Email/Phone) to obtain username/password. Shortly after you will receive a new password in your inbox.

Who can I contact to get more information about Mobile Device Management? (applicable for MDM/EMM

<Customer's MDM/EMM Administrator/support team>

How do I activate the App?

Customers not using MDM : Click on the zips App icon on your device to open the App. Enter your username & password to login. You should see the app screen refresh with the message "You are

protected" "Device is Safe"

Customers using MDM : Click on the zips App icon on your device to open the App. The app should auto log you in and You should see the app screen refresh with the message "You are protected" "Device is Safe". User does not have to enter username or login.

Why isn't the application asking me for my login? (Applicable for MDM/EMM)

The application is configured for Auto-Login via MDM/EMM.

What is my Username and Password? (Applicable for manual login)

<Customer specific response> Your Username & Password was sent out to your email address on mm/dd/yyyy with subject: Welcome. Please contact your Administrator (Email/Phone) to obtain username/password.

I forgot my password to log into zIPS, how can I reset it? (Applicable for manual login)

Please contact your Administrator (Email/Phone) to obtain username/password. Shortly after you will receive a new password in your inbox.

How to calculate the battery usage of zIPS on iOS?

Consider the case on the following screenshot attachment :

Some definitions are :

- Usage : Time that the phone was used (i.e. not asleep)
- Standby : Total time the phone was without charge, including time on deep sleep (i.e. when the screen is off).

- zIPS percentage : Is the percentage of the total battery that was used by zIPS.

Using the data from the above screenshot as an example, here is how the battery consumption for zIPS can be calculated :

Battery drain = 100-53=47%
Drain by zIPS = 0.21 x 47% = 9.87%
Drain by zIPS per hour = 9.87 % / 16.25 hs = 0.60% per hour