INFRASI
INFRASTRUCTURE SOLUTIONS INTERNATIONAL

Mobile security with a geofence perspective

Whitepaper – October 2016

Contents

Introduction

Mobility is all around us. It's pushing businesses to re-evaluate their approach to cyber security. The mobility needs of a business are more than control of a device; it also encompasses a discussion on what corporate data users need access to.

Understanding the data that is extended to a mobile user should answer the questions as to who, what, when, and why. That information should validate the transition to a data/information-centric cyber security approach. The framework for a cyber mobility strategy is about aggregating the mobility domain, corporate data, and security risk approach.

The administrative burden associated with creating a security policy and designing the infrastructure to enforce the policy is a challenge. This is where we see geofencing as a situational awareness capability to support a data/information-centric cyber security strategy. The intent of this paper is to understand how geofencing can be used to address mobile security.

Simplifying a geofence

Data in transit with mobile refers to data as it moves across network boundaries. With the adoption of cloud computing, corporate data is located everywhere, private, public, or hybrid environments. Accessing this data remotely typically uses tunneling (i.e. virtual private network (VPN)) solutions from remote locations. If we think about the data access as the user and/or device moves, we can also think of it as a form of data in transit.

Mobile operating systems have location application program interfaces (API) that can be used to create a geofence. The significance of this is that location capabilities are available that allow businesses to use longitude, latitude, and radius variables to define a virtual perimeter and leverage position triggers for security purposes based on the boundaries.

This service leverages a wireless connection, Wi-Fi, GPS, or cellular connection. The precision of the location will be based on the connection type. Further if we correlate our data in terms of asset management, people, and business workflows, we can control what goes in and out of the geofence. The correlation should show a relationship that helps support a mobile experience.

The factors driving the geofence use case

Mobile technologies are important to a business as it allows employees to fulfill their responsibilities, customer engagement with the business, and so forth. However, it has introduced a threat environment with an expanded attack surface.

If you think about the insider and outsider threat, it’s a challenge to prioritize who is the bigger threat. Previously external threats were of great concern to most organizations, which drove security requirements and budgets. Now the insider threat is becoming more important due to the borderless environment mobility has created.

Anytime and anywhere access to corporate data is a standard characteristic of mobility. However, it's a culture change to most organizations’ security policies because now control is distributed outside corporate boundaries. The confidentiality, integrity, and availability (CIA) is still important in this realm. However, with mobility we have to continue to apply layered and defensive in-depth strategy. With geolocation capabilities available to most application developers, gathering location information is easily accessible and can support the security strategy.

There is a vast amount of data available with mobile. At the same time there are multiple questions and insights that can be gathered. As cyber incidents increase, organizations need to use all the data they can to be proactive when it comes to security.

Integrating geofencing into the security plan

The security associated with mobility is driven by understanding data and the threat landscape. The information gathered from these activities is incorporated into an organization’s mobility strategy. Below are key considerations for unifying your security strategy around geofencing.

- ★ Security Infrastructure
- ★ Data Controls
- ★ Device Strategy
- ★ Geofence Triggers
- ★ Location Enablement Activities

Security Infrastructure

The infrastructure for a business needs to be adaptive to the complex environment. It's about more than prevention and includes detection alignment. Currently a majority of organizations are phasing in mobile changes to their infrastructure. This includes integration of enterprise mobility management (EMM) systems, identity and access management, hybrid cloud deployments, mobile threat protection (MTP), next-generation firewall (NGFW), and so forth. As you can see, there is no shortage of work when it comes to the infrastructure build-out.

The governance infrastructure associated with mobility should include multiple systems. As you react to the changing needs of your users, define the asset needs in terms of location. Start with a limited perimeter and scale out as need be. This will not only utilize data segmentation strategies, but also building location profiles that leverage automation.

Data controls

A breakdown of what data is available to mobile users, risks associated with lost/stolen data, and access management. Build a risk profile for your organization that will vary based on the requirements. The security should emphasize data in use, data at rest, and data in transit. With most organizations moving towards hybrid cloud environments, corporate data can be anywhere. The controls associated with data need to be correlated with users and where they are. The dwell time before an event can be triggered is a unique feature that can enhance a data governance strategy.

Device approach

It's important to understand that not all devices are considered the same. The device management strategy these days is shifting from simple corporate-owned, to bringing your own device (BYOD) and corporate-owned personally enabled (COPE). The importance of the device relates to balancing privacy vs corporate risks. Location data requires using device capabilities and ensuring users know why it's being collected. An acceptable usage policy should be communicated to a user community so that they are aware.

Geofence Triggers

An application's ability to leverage a geofence operates either as a background or active processes. The importance is the impacts on battery and the event triggers capabilities, considering that not all events are the same or require the same administrative attention. Geofence priority levels are needed to manage the various triggers. While the ideal approach is to automate the actions associated with an event, the event still needs to be regularly assessed to determine the administrative burden associated with the actions.

Priority Level	**Description**
1	Immediate analysis
2	Can be analyzed in a timely manner
3	Can be deferred as needed

Table 1: Event triggers priority levels

Location enablement activities

Location data is great, but the next level is expanding the prevention and detection capabilities of geofencing into continuous monitoring activities. The geofence radius will increase or decrease depending on business needs. We believe the location information should operate as key inputs for the following activities: behavior profiles and security incident predictions.

- Behavior profiles - the challenge with the unknown of where a user is located or how they use the devices will continue to be a problem with physical, network, malware, and vulnerability threats. If you can profile a user based on device ownership type, you can leverage answer the who, what, where, why, and when to continuously monitor the distributed access to corporate data.
- Incident predictions - mobile incidents is an unknown territory that is broad and disrupts current processes. An internal discussion is needed around the mobile component of the business impact analysis. Location information can provide situational awareness. If you can predict, you then, in turn, can react proactively before disruption. The goal is to prevent the misuse or loss of data due to mobility.

Geofencing going forward

We outlined how geofence helps a security strategy. A concern with mobility from the business perspective is a loss of control and fear that without control we are in danger of a cyber incident. To a certain extent that is valid. The mobility market is changing rapidly. Moving at this pace is impacting a business's ability to stay secure. What does a connected environment that has a broad attack vector and multiple threat actors look like? In shifting to a data/information-centric business, framing the discussion around these questions will assimilate your organization into the current cyber environment. Alignment of location technology and security is the ideal state to make this happen or call the third party after an incident that negatively impacts your business.

About Us

Infrastructure Solutions International (INFRASI) is an enterprise mobility and wireless solutions company constantly developing new, breakthrough solutions that leverage mobility.

For more information please contact us at info@infra-si.com or visit us at www.infra-si.com.