SafeNet Authentication Service — неотъемлемый фактор двухфакторной аутентификации

Обзор функциональных возможностей решения SafeNet Authentication Service, сертифицированного в конце 2013 г. и позволяющего поддерживать процедуры аутентификации как в частных, так и в публичных облаках.

Рожнов Михаил – ведущий эксперт компании "Сертифицированные информационные системы".

Введение

Сегодня каждая информационная система настолько сложна, что добавление нового элемента в нее влечет изменение архитектуры. В большой степени данное утверждение справедливо и для функций безопасности, в части такого элемента защиты как аутентификация. Аутентификация всегда была первым звеном в защите информационной системы от несанкционированного доступа, первым показателем защищенности, определенного в нормативных документах регуляторов. Процедур проверки подлинности пользователя существует огромное число, и нередко достаточно сложно выбрать предпочтения, найдя экстремум между уровнем защиты, простотой внедрения, соответствием требованиям регуляторов и, конечно же, стоимостью владения. В данной статье рассмотрено решение SafeNet Authentication Service, разработанное компанией SafeNet Inc. В соответствии с декабрьским аналитическим отчетом Gartner, решение SafeNet Inc. занимает лидирующую позицию на рынке средств защиты, связанных с аутентификацией пользователей, которое поможет ответить на следующие вопросы: 1) нужна ли двухфакторная аутентификация на базе бесконтактных аутентификаторов (генераторов одноразовых паролей); 2) сложно ли интегрировать решение, не изменяя существующую архитектуру; 3) насколько разнотипные аутентификаторы могут быть применимы к различным пользователям (стационарным, мобильным); 4) насколько решение, в основе которого лежат генераторы одноразовых паролей, может соответствовать требованиям новых нормативных документов регуляторов.

В корпоративном секторе все растет число мобильных пользователей – этот тренд будет и дальше увеличиваться благодаря тому, что каждый день на рынке появляются мобильные девайсы, которые помимо базовых функций и развлечений помогают решать и бизнес-вопросы. Сегодня, наверное, каждый выйдя из дома и забыв телефон, – обязательно за ним вернется. Однако мобильное удобство для специалистов по безопасности несет немало вопросов по обеспечению надежной аутентификации, которая не должна противоречить концепции мобильности. С одной стороны, применение статических паролей недопустимо в корпоративной среде в связи с тем, что инструменты для организации атак типа брутфорс, перехват паролей или хэшей с возможностью их дальнейшего восстановления через канал передачи данных (включая SSL-канал – инструмент для раскрытия sslstrip) уже включены в состав «классических» дистрибутивов для выполнения тестов на проникновение: Backtrack Linux, Kali Linux. Электронная почта, корпоративный портал – иногда возникает необходимость получить доступ к данным «здесь и сейчас», не задумываясь о том, что доступ будет осуществлен через открытую сеть WiFi -сеть. А если доступ осуществляется и через защищенную беспроводную сеть, то нет никакой гарантии, что вы в этой сети один и нет никого, кто с помощью того же reaver или aircracking (инструменты для взлома WiFi-сетей, входящие в состав дистрибутивов для тестов на проникновение) не получил к ней доступа и не пишет видео о перехвате паролей в сети кафе. Решение очевидно одно – усиливать функции аутентификации за счет добавления дополнительных факторов проверки, то есть применять механизм двухфакторной аутентификации – то есть для подтверждения своей подлинности предоставлять «то, что у меня есть» и «то, что я знаю». Классическим примером такого подхода является аутентификация, в основе которой лежит инфраструктура открытых ключей. Инфраструктура PKI существовала и продолжает развиваться в том числе и в мобильном направлении: компании, которые занимаются механизмами аутентификации выпустили на рынок ридеры для смарт-карт, которые интегрируются с устройствами от компании Apple. Но тут сразу стоит отметить и проблемы, возникающие при внедрении инфраструктуры PKI для организации двухфакторной аутентификации. Если в компании небольшое число сотрудников, то управлять жизненным циклом ключей достаточно просто, используя встроенные механизмы операционных систем, но когда число пользователей возрастает, стандартными средствами уже не обойтись – здесь необходимо оптимизировать процесс генерации сертификатов, отслеживать их валидность, обеспечивать возможность переиздачи сертификата или формирования временного сертификата, при утере ранее выданного. Если предполагается использовать аутентификацию на мобильных устройствах, то сразу необходимо отметить, что универсальных ридеров (а USB-разъемы есть не на всех устройствах) не существует на данный момент, и, в лучшем случае, вам придется просто импортировать сертификаты на устройства, не обеспечив при этом наличие второго фактора – защита PIN-кодом, либо использовать различного рода microCD-токены, тем самым «привязав» пользователя к устройству.

Что может прийти на помощь в решении, кажется, не такой уж сложной задачи, но содержащей в себе достаточно много «а если». Это программно-аппаратный комплекс, позволяющий выполнять процедуру двухфакторной аутентификации с использованием бесконтактных аутентификаторов. Именно термин «бесконтактный» позволяет обеспечить универсальность применения генераторов одноразовых паролей в различных инфраструктурах и на различных устройствах. Рассмотрим решение SafeNet Authentication Service (SAS) более подробно.

SafeNet Authentication Service

SAS – программно-аппаратный комплекс, представляющий собой сервер для обеспечения двухфакторной аутентифи-

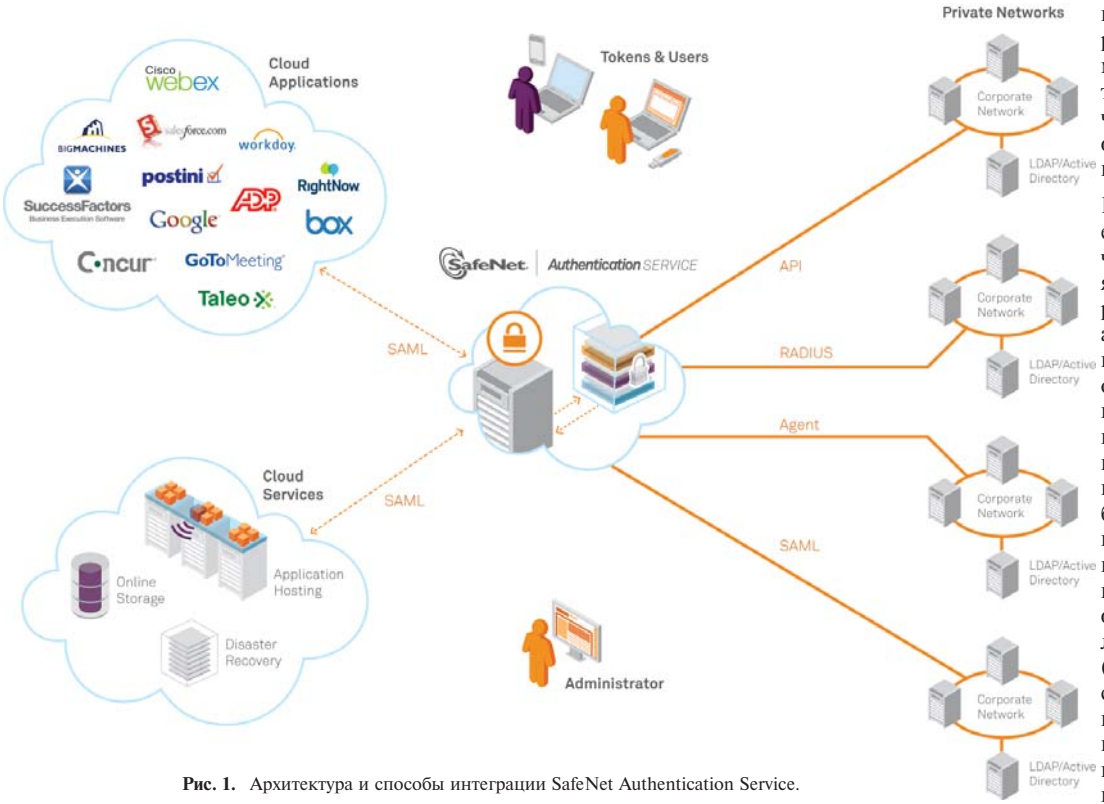

Рис. 1. Архитектура и способы интеграции SafeNet Authentication Service.

кации с использованием бесконтактных токенов (аппаратных или программных, именно по этой причине решение является программно-аппаратным комплексом, хотя сам по себе сервер представляет собой программное обеспечение) и специализированных токенов, которые формируются на стороне серверов (рис 1.). Для интеграции с сервисами, в которых планируется выполняться двухфакторная аутентификация, используются специализированные агенты, либо протоколы RADIUS и SAML 2.0, предоставляемые самой средой функционирования службы. Для сопоставления пользователя с некоторым токеном используется либо хранилище LDAP, либо внутреннее хранилище, при этом необходимо сразу отметить, что при условии синхронизации с LDAP-хранилищем в базе данных SAS хранится только информация о субъекте (именной идентификатор, имя и фамилия пользователя, почтовый ящик и номер мобильного телефона субъекта), но не его пароль или хэш. На текущий момент доступны следующие агенты:

- агент для синхронизации с LDAP-хранилищем (32/64 бит);
- агент для Cisco Any Connect (32/64 бит);
- агент для Citrix Web Interface(32/64 бит);
- агент для работы с IIS 7 – Terminal Services Web иRemote Desktop Web (32/64 бит);
- агент для Microsoft Outlook Web Access 2007, 2010, 2013 (32/64 бит);
- агент для службы MicrosoftNPS/IAS (32/64 бит);
- агент для Microsoft SharePoint (32/64 бит);
- агент для Windows Logon для операционных систем Widnows XP/Vista/7/8 (32/64 бит).

Интеграция в Linux/UNIX-системах происходит через RADIUS-протокол. Для этого выполняется инсталляция RADIUS-агента в операционной системе, и в настройках PAM-модуля прописывается требование для выполнения процедуры аутентификации через внешний RADIUS-сервер. Данная процедура позволяет настроить вход в систему по одноразовому паролю для всех сервисов, поддерживающих PAM, а это большинство служб операционной системы – начиная от входа в консоль и графические оболочки заканчивая SSH, telnet, FTP и т.д. Более того, гибкость PAM-модулей позволяет совмещать различные типы аутентификации для сервиса. Например, пользователь может использовать цифровой сертификат для входа на рабочую станцию, при условии, что субъект не может предоставить данный сертификат, ему предлагается использовать значение одноразового пароля. Если и в этом случае пользователь не смог подтвердить свой идентификатор, то ему предоставляется возможность использовать статический пароль. Дополнительно есть возможность прописать обязательный механизм аутентификации и вторичный механизм проверки подлинности.

Если говорить об облачных сервисах, то, при условии поддержки данным сервисом протокола SAML 2.0 и технологии SingleSignOn (SSO), интеграция происходит в несколько кликов мыши – просто прописывается URL-страница, на которую будет перенаправлен субъект для прохождения процедуры проверки пользователей. К данным сервисам можно отнести такие облачные решения как Google Docs, Salesforce, Office 365. Если компания стала сторонником таких сервисов и готова мигрировать в облачную инфраструктуру, то компания SafeNet готова предложить облачный сервис аутентификаци, который по своему функционалу ничем не уступает решению, разворачиваемому самостоятельно, за тем лишь исключением, что сам сервер аутентификации функционирует в датацентре SafeNet.

Решение SAS поставляется совместно с SDK, что позволяет компаниям-разработчикам интегрировать в свои решения аутентификацию по одноразовым паролям. Это обеспечивает повышенный уровень аутентификации в собственных решениях (ДБО-системы, порталы, мобильный банкинг и т.д.) без внесения изменений в собственный проект. Для доказательства данного факта ниже представлен листинг на языке PHP (берется готовый класс, создается объект и вызывается процедура проверки подлинности на внешнем сервере), который представляет собой RADIUS-клиент и позволяет интегрировать механизм двухфакторной аутентификации в портальное решение:

```
$radius = new Radius($SAS_IP,$SAS_Secret);
if ($radius->AccessRequest($_POST['user'], $_POST['pass']))
  {?>
   <br /><imgsrc="img/accept.png"/><br />
   <strong>Authentication accepted.</strong>
   <?php
   }
else
   {?>
    <br /><imgsrc="img/deny.png"/><br />
    <strong>Authentication rejected.</strong>
     <?php
    }
```

Такое количество строк понадобится добавить в проект на других языках разработки и воплотить в жизнь функцию двухфакторной аутентификации в собственном проекте.

После того, как мы рассмотрели решение и способы интеграции с различными сервисами, необходимо рассмотреть линейку аппаратных и программных генераторов, доступных при использовании сервера аутентификации. На сегодня решение SafeNet поддерживает следующие аппаратные генераторы (рис. 2):

- SafeNet eToken 3000 (ранее известный как eTokenPASS) – пластмассовый брелок, позволяющий формировать значение одноразового пароля с синхронизацией по событию;
- SafeNet KT4/KT5 – пластмассовый и металлический брелоки, позволяющие формировать значение одноразового пароля с синхронизацией по событию;
- SafeNet eToken 3400 – генератор одноразовых паролей, выполненный в форм-факторе смарт-карты, позволяющий формировать значение одноразового пароля с синхронизацией по событию;

Рис. 2. Аппаратные генераторы одноразовых паролей.

– SafeNet eTokenGOLD – брелок-«калькулятор», работающий в двух режимах: challenge–response и генератор одноразовых паролей с синхронизацией по событиям;
– SafeNet eTokenRB-1 – брелок-«калькулятор», работающий в двух режимах: challenge–response и генератор одноразовых паролей с синхронизацией по событиям;
– SMS (Short Messaging Service) – генерация одноразового пароля осуществляется на стороне сервера с дальнейшей доставкой значения OTP в виде SMS. На сегодня SafeNet Authentication Service поддерживает работу с заранее преднастроенными SMS-шлюзами, а также имеет возможность добавлять собственные SMS-шлюзы, позволяя создавать один или два одновременно работающих шлюза, обеспечивая тем самым гарантированную доставку SMS.

С выходом нового релиза SafeNet Authentication Service стали поддерживаться два схожих по своей структуре программных токена – MP-1 и MobilePASS (который, в свою очередь, был мигрирован из проекта SafeNet Authentication Manager). Программный токен представляет собой софтверное решение, функционирующее либо в среде операционной системы (на данный момент это Windows и MacOS), либо инсталлируемое на мобильную платформу, под управлением одной из следующих операционных систем: Android, iOS, J2ME, Windows Mobile, BlackBerry. Очевидный плюс программных токенов – отсутствие необходимости приобретения аппаратных токенов – каждый пользователь может использовать свой мобильный гаджет как генератор одноразовых паролей. Если в компании развернуто MDM-решение, то «заливка» программного токена может происходить автоматически, после этого пользователю приходит почтовое уведомление с вектором инициализации, который необходимо импортировать в ключ. В завершение пользователь задает PIN-код на токен и приступает к работе.

В начале статьи мы упомянули о неком токене, который формируется на стороне сервера – пришло время рассказать и о нем. Данный токен называется GrIDsure и работает по следующему принципу: конечному пользователю предоставляется матрица ячеек в процессе инициализации токена одного из размера – 5x5, 6x6, 7x7, содержащая случайный набор символов, из которых субъект составляет некоторую траекторию движения – personal identification pattern (PIP). После этого, когда пользователь решит аутентифицироваться в некотором сервисе, защищенным SAS, ему будет предложена матрица такого же размера, в которой ему необходимо будет выбрать свою «траекторию движения». Именно эта траектория и будет определять значение OTP. Каждый раз, когда будет возникать матрица, значения в ее ячейках будут меняться – это защитит от попытки перехватить траекторию. Данный токен может применяться для аутентификации в следующих сервисах – вход на рабочую

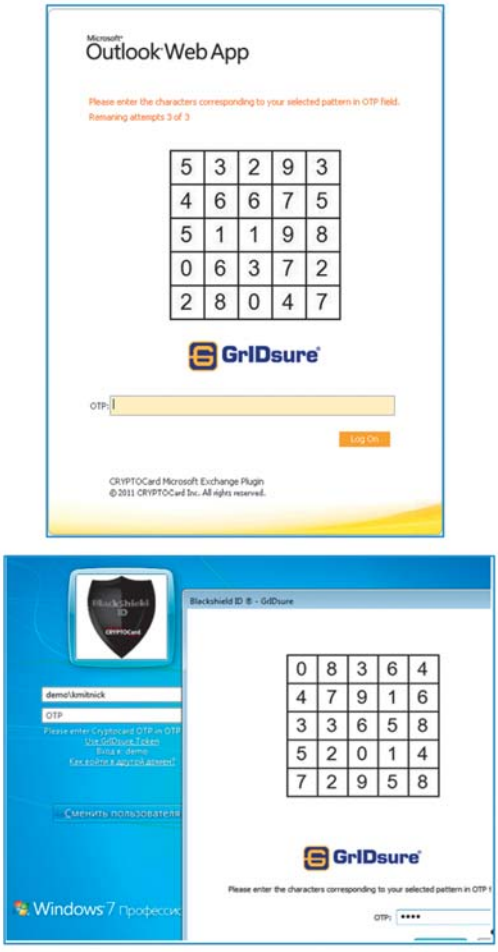

Рис. 3. Применение токена GrIDsure.

стацию Microsoft, различные web-порталы (ранее приведенный пример поддерживает работу с GrIDsure), Microsoft Outlook WebAccess, Microsoft Terminal Services Web и Remote Desktop Web, Microsoft SharePoint (рис. 3).

Компания SafeNet не обошла стороной и других производителей токенов. Так, SAS, помимо своих токенов, может работать и с генераторами одноразовых паролей от компании RSA (RSA SecureID), а также токенов с поддержкой OAuth-протокола.

Мы рассмотрели архитектуру решения, процедуру синхронизации пользователей, механизмы интеграции в сервисы и линейку поддерживаемых токенов, и теперь внимательный читатель скажет: «А где двухфакторная аутентификация? То, что я имею, могут просто украсть». Действительно, не хватает еще одного фактора. Но этот фактор тоже есть. Решение SAS позволяет настроить политики на весь ряд токенов, и, одно из основных свойств политик – использование PIN-кода для вашего токена. Это означает, что динамический пароль будет выглядеть как PIN-код на токен плюс значение одноразового пароля. Предположим, что у вас украли генератор паролей, но вы в безопасности – значение PIN знаете только вы. Допустим, что кто-то настроил снифер и, применив инструмент sslstrip, читает трафик, инкапсулированный в SSL-канале – вы также находитесь в безопасности, так как значения OTP формируются только вами, и все неверные значения будут отброшены сервером (а при многократном вводе неверных значений учетная запись пользователя будет заблокирована, либо будет деактивирована на небольшой промежуток времени с дальнейшей автоматической блокировкой). Стоит повторить, что данная политика применима ко всем типам токенов, включая SMS и GrIDsure. Это означает, что решение SAS предоставляет полноценную процедуру двухфакторной аутентификации с использованием бесконтактных аутентификаторов.

Теперь стоит поговорить о лицензировании – именно политика лицензирования определяет стоимость владения системы. В части SAS все очень просто – лицензирование осуществляется по числу пользователей, при этом в это понятие вкладываются и техническая поддержка, и абсолютно бесплатный токен MP-1, для инсталляции на мобильную платформу или стационарную рабочую станцию. Аппаратные токены приобретаются отдельно, как и отдельно приобретаются токены GrIDsure. Здесь также необходимо отметить, что одному субъекту системы можно назначить два и более токенов. Это позволит использовать разные типы токенов при аутентификации в разных сервисах и в разных ситуациях – система будет проверять все возможные значения OTP от разных токенов. Также стоит отметить, что в лицензию включена возможность работы SAS в кластере, что является обязательным для обеспечения отказоустойчивости.

Решение SAS должно очень понравиться администраторам – оно из разряда «поставил и забыл». Решение позволяет автоматизировать процесс присвоения гене-

ратора одноразовых паролей пользователям – достаточно один раз прописать правило, что всем новым пользователям из группы инициализировать определенный тип токенов, и в будущем при добавлении нового субъекта в систему, он автоматически получит уведомление о регистрации и сможет пройти ее самостоятельно без привлечения администратора. У генераторов одноразовых паролей есть один минус – они могут рассинхронизироваться, то есть после того, как пользователь многократно сгенерирует одноразовые значения и не использует их для аутентификации в сервисе, он не сможет более использовать этот генератор до тех пор, пока не синхронизирует его в системе. Но и в этом случае нет необходимости обращаться к администратору – SAS предоставляет портал самообслуживания, на котором пользователь может аутентифицироваться по одноразовому паролю, который ему доставит система по SMS или по электронной почте, и далее выполнить любую необходимую операцию: синхронизировать токен, сменить PIN-код, сменить PIP.

Заключение

В заключение стоит отметить те преимущества, которые предоставляет SAS:

- *поддержка широкой линейки токенов (аппаратных, программных, генерируемых на стороне сервера), которые позволяют каждому пользователю выбрать определенный тип токена для своих индивидуальных нужд;*
- *двухфакторная аутентификация, которая может быть использована там, где сейчас используются статический пароли за счет применения индустриальных стандартов, таких как RADIUS и SAML, а также агентов для интеграции со службами;*
- *поддержка генераторов одноразовых паролей сторонних производителей, что позволяет мигрировать на новую платформу, используя приобретенные токены в компании;*
- *высокий уровень автоматизации позволяет снизить расходы на управление и администрирование SAS;*
- *неограниченный срок действия токенов, которые могут быть переинициализированы для новых пользователей, тем самым снизив общую стоимость владения системой;*
- *возможность присвоения пользователю более одного токена, что позволяет выполнять процедуру аутентификации с различных устройств;*
- *предоставление портала самообслуживания, снижая тем самым нагрузку на администрирование и сокращая время решения проблем, связанных с генераторами одноразовых паролей;*
- *SAS сертифицирован в системе сертификации ФСТЭК России на соответствие требованиям технических условий. В соответствии с приказами № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», SAS может применяться для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в государственных информационных системах 3-го и 4-го классов защищенности, а также для обеспечения 3-го, 4-го уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 3-го типа.*

Рожнов Михаил,
компания "Сертифицированные информационные системы".

RSA и Pivotal: архитектура Big Data for Security Analytics

Февраль 2014 г. – RSA, подразделение безопасности корпорации EMC, объявила о выпуске эталонной архитектуры Big Data for Security Analytics, созданной совместно с Pivotal. Новое решение позволит организациям повысить гибкость и эффективность аналитических систем безопасности, а также заложит основу для более активного инвестирования в средства ИТ-аналитики. Эталонная архитектура предоставляет новый уровень видимости (которая намного превосходит возможности традиционных решений на базе журналов) и продвинутые возможности аналитики, которые позволят специалистам оперативно обнаруживать угрозы и принимать решения на основе аналитических данных. Она также поможет организациям внедрить новую стратегию "озера данных" (Data Lake), снизить расходы и повысить эффективность ИТ-систем.

Новая архитектура отлично демонстрирует, как соединение технологий обеих компаний позволяет организациям быстро выявлять и расследовать инциденты безопасности и реагировать на них до того, как они смогут повлиять на работу предприятия. Возможности, которые дает аналитикам и специалистам по безопасности совместное использование технологий RSA и Pivotal, это:

- *расширенная видимость* за счет полной записи всех сетевых пакетов, сбора журналов и обогащения данных контекстом для выявления угроз, действующих в обход стандартных средств безопасности;
- *улучшенные возможности аналитики* в момент записи пакета и в течение всего его жизненного цикла вплоть до архивирования и удаления — для выявления аномалий и признаков атаки или уязвимостей в системе безопасности;
- *ускоренное принятие решений на основе аналитических данных* благодаря наглядной визуализации, мониторингу подозрительной активности и отображению уведомлений на основе приоритетов, что позволяет аналитикам адекватно реагировать на угрозы;
- *возможности развертывания и масштабирования корпоративного уровня* с использованием распределенных горизонтально масштабируемых архитектур с высокой доступностью, обеспечивающих гибкое масштабирование до максимального масштаба среды;
- *гибкость и оперативность* за счет возможности использовать новые модули аналитики и источники данных еще на этапе их разработки и интеграции.

В результате система безопасности совершенствуется по мере развития угроз и бизнес-процессов.

За счет использования открытого хранилища данных Hadoop решение RSA Security Analytics делает инновации, предлагаемые в экосистеме Hadoop, доступными для широкого круга заказчиков.

Intel: бесплатный антивирус McAfee

Март 2014 г. – McAfee объявила о выпуске полнофункциональной бесплатной версии McAfee Mobile Security (доступна на 30 языках, включая русский) для защиты данных мобильных устройств под управлением Android и iOS.

В бесплатной версии McAfee Mobile Security для Android доступны новые функции защиты и обеспечения безопасности в сетях Wi-Fi (программа проинформирует пользователей, если сеть окажется потенциально опасной или незащищенной паролем), а также поддержка Intel® Device Protection Technology.

Решение не только защищает от вирусов, но и сохраняет личные данные от проникновения, потери и кражи. Пользователи смогут отследить местоположение устройства при хищении, защитить приложения, сделать фильтрацию звонков и коротких сообщений. Также есть возможности обнаружить попытки джейлбрейка, сделать резервное копирование и др.

Согласно отчету McAfee о мобильных угрозах за третий квартал 2013 г., объем вредоносного ПО для Android увеличился практически в три раза за период с 2012 по 2013 г. В 2012 г. 1,6 млн американцев стали жертвами кражи смартфонов. Стоимость украденных мобильных телефонов и хранящихся на них данных пользователи оценили в $30 млрд. В случае хищения, например, когда преступник совершает несколько неудачных попыток разблокировки устройства, можно дистанционно активировать функцию CaptureCam, в результате чего камера сделает снимок человека, вводящего пароль. Изображение и сведения о местоположении отправляются владельцу.

Благодаря технологии Intel Device Protection, McAfee Mobile Security теперь может поддерживать безопасность на уровне ядра. Данная разработка позволяет блокировать и защищать устройства от вредоносного ПО, сохраняя высокую скорость работы техники при экономном расходе заряда аккумулятора.