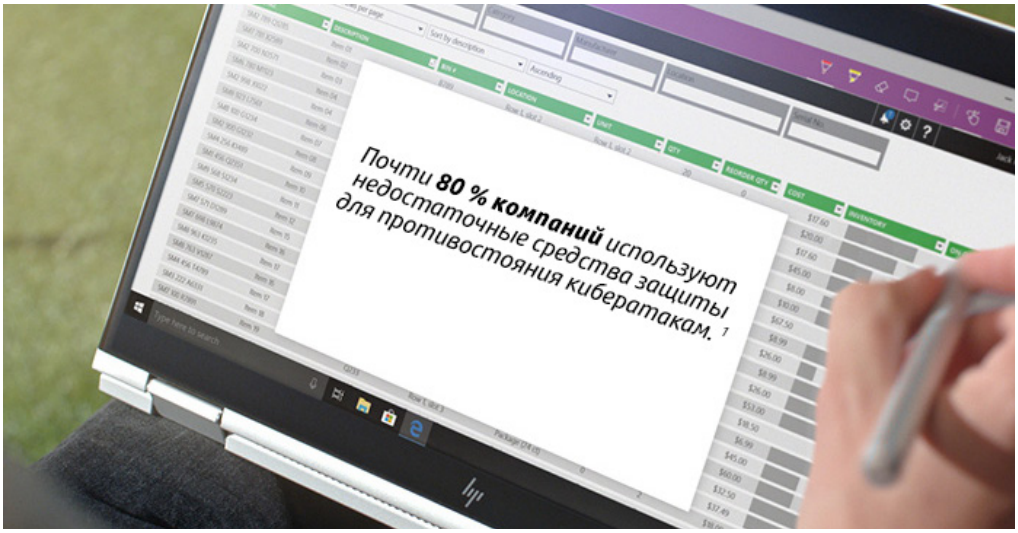
# Каким образом автоматическая защита поможет спасти ваши бизнес-устройства

Подробнее




**Как бороться с угрозой, которая скрывается за вашей линией обороны? Внедрять автоматизацию.**

600 миллиардов долларов в год. Такова сумма убытков от киберпреступности по всему миру за 2017 г.[2]. Эта цифра увеличивается по мере того, как совершенствуются навыки и техники хакеров. Согласно последним данным 20 % предприятий малого и среднего бизнеса были вынуждены немедленно приостановить бизнес-операции, а 12 % потеряли свою прибыль в результате кибератаки[3]. Одной из самых современных скрытых атак, ставших кошмаром для ИТ-менеджеров, является атака на аппаратное обеспечение в процессе загрузки компьютера: атака на систему BIOS.

Миллионы компьютеров имеют уязвимые системы BIOS, т. е. их может взломать даже хакер с самыми скромными способностями. Несколько лет назад на одной из конференций исследователи Зено Ковач и Кори Калленберг представили новый тип атаки, которая позволяет в течение нескольких часов удаленно взломать и заразить BIOS на нескольких устройствах[4]. Поскольку большинство систем BIOS основаны на одном и том же коде, достаточно один раз взломать его, чтобы через некоторое время научиться обходить защиту многих других компьютеров.

Опасность атаки этого типа состоит в том, что она нацелена на незащищенный участок системы. Между операционной системой и оборудованием есть скрытый участок, который традиционно игнорируется. Ваша сеть может быть несокрушимой, а устройства могут находиться под защитой лучшего в мире антивирусного ПО, и, тем не менее, остается короткое мгновение между загрузкой системы и включением защиты.

Поскольку ПО для обеспечения кибербезопасности, как правило, размещается на уровне операционной системы, оно не сможет обнаружить проникновение вредоносного ПО в BIOS (перед загрузкой с последующей передачей в режим управления системой). В этой точке хакеры получают полный контроль над вашей системой. Они могут похитить ваши данные, сделать их нечитаемыми или распространить новое вредоносное ПО в сети компании. Что хуже всего, обнаружить это нарушение безопасности и заражение может быть практически невозможно.

Лучший способ обеспечить безопасность устройств компании — использовать многоуровневую защиту. Вашим ИТ-специалистам больше не придется тратить время на бесконечные проверки и ручные исправления. HP предоставляет меру автоматического реагирования —в рамках широкого ассортимента решений для обеспечения безопасности — HP Sure Start[5].

«Это решение стало результатом наших совместных усилий с HP Labs, направленных на то, чтобы помочь компаниям в управлении рисками и защите пользователей и ИТ от вредоносных атак, ошибок обновления и других непредвиденных или неизвестных угроз»,

**— говорит Вали Али, директор по технологиям безопасности и конфиденциальности в подразделении Персональных систем HP PC.**

## Каким образом автоматическая защита поможет спасти ваши бизнес-устройства

HP Sure Start — это защита на уровне BIOS с функцией самовосстановления. Мы называем этот подход устойчивостью к кибератакам. Система создает эталонный образ BIOS, который шифруется непосредственно на устройстве. Таким образом, при попытке взлома BIOS она автоматически перезапускается и загружает эталонную версию, стирая зараженный файл и сообщая об атаке. Иными словами, компьютер сам себя «лечит».

Это позволяет избежать перерывов в работе. И сократить расходы. И обеспечить соответствие устройств нормативным требованиям. И, кроме всего прочего, так намного проще работать.

Если вы ищете простейший способ предоставления устройств с функцией HP Sure Start вашим пользователям, рассмотрите решение HP Device as a Service (DaaS)[6]. Это современная модель обслуживания IT-оборудования, благодаря которой коммерческие организации смогут экипировать своих сотрудников нужным аппаратным обеспечением и аксессуарами, управлять парком устройств с разными ОС и получать дополнительные услуги в течение срока службы этих устройств. HP DaaS предоставляет простые универсальные планы с оплатой за каждое устройство, которые обеспечат бесперебойную и эффективную работу сотрудников.

Конечные устройства и точки доступа должны контролироваться на всех уровнях. Пришло время пролить свет на скрытые участки наших устройств. Каждый пользователь, каждая компания и организация по всему миру могут укрепить безопасность и отказоустойчивость с помощью предложений HP, включающих HP EliteBook x360 с опциональными процессорами Intel® Core™ i7 8-го поколения. Это устройство из семейства HP Elite включает в себя технологию обеспечения безопасности, в том числе встроенную функцию HP Sure Start.

**Откройте преимущества решений HP для обеспечения безопасности вашего бизнеса.**

---

**Источники:**


1. Statista Survey ID 622857, Small and medium sized enterprises in the U.S (Предприятия малого и среднего бизнеса в США), исследование, проведенное агентством Statista в октябре 2016 г.
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. Osterman Research при финансовой поддержке Malwarebytes: Second Annual State of Ransomware Report: US Survey Results (Второй ежегодный доклад о состоянии программ-вымогателей: результаты исследования в США), июль 2017 г.
4. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems
5. Разные поколения HP Sure Start доступны для некоторых конфигураций систем HP Elite и HP Pro.
6. Планы и (или) включенные компоненты HP DaaS зависят от региона или уполномоченного сервисного партнера HP DaaS. Чтобы получить подробную информацию по вашему региону, обратитесь к местному представителю HP или уполномоченному партнеру DaaS. Услуги HP регулируются условиями и положениями HP, применимыми к предоставляемой услуге или определенными в момент покупки. Заказчик может иметь дополнительные законные права в соответствии с применимыми местными законами. Такие права не затрагиваются условиями и положениями оказания услуг HP или ограниченной гарантией HP, предоставляемой с продуктом HP.



4AA7-3219RUE, апрель 2019 г.