DIEBOLD NIXDORF

BS2 Penki kontinentai group

Vynamic™ Security

Защита устройств самообслуживания от взлома и других атак

Vynamic™ Security

Защита устройств самообслуживания от взлома и других атак

Vynamic™ Security - решение, обеспечивающее комплексный подход к защите устройств самообслуживания (банкоматов, платежных киосков, электронных кассиров и др.) от любых типов взлома, хакерских атак и других угроз. Модульная система позволяет закрыть наиболее уязвимые части терминальной инфраструктуры банков и других организаций.

ФУНКЦИИ И ПРЕИМУЩЕСТВА

Комплексный подход

Использование прогрессивных методик защиты ИТ-инфраструктуры, таких как создание списков доверенного программного обеспечения (whitelisting) и ограниченной среды выполнения каждого, из разрешенных процессов (sandboxing), позволяет системно подходить к обеспечению безопасности терминальной сети.

Гибкое внедрение

Решение представляет собой три самостоятельных модуля: Hard Disk Encryption (шифорование жесткого диска), Intrusion Protection (защита от проникновения) и Access Protection(защита доступа), каждый из которых используется против угроз конкретного типа.

Многоуровневая защита

Архитектура Vynamic Security подразумевает наличие нескольких уровней защиты. В случае падения первого уровня уязвимое место будет защищено благодаря запуску специальных сценариев.

Работа с терминалами разных производителей

Vynamic Security является мультивендорным решением, которое может быть внедрено для защиты устройств разных производителей. Это позволяет унифицировать процессы обслуживания терминалов и снизить итоговую стоимость владения терминальной сетью.

Простота эксплуатации

Развернутое на устройстве программное обеспечение не требует постоянного обновления антивирусных баз и сканирования системы. Таким образом, решение существенно упрощает процессы администрирования терминальной сети и снижает стоимость владения.

Соответствие стандартам безопасности

Решение работает с операционными системами Windows XP, Windows 7, Windows 10 и полностью соответствует стандартам безопасности PCI DSS, а также может быть адаптировано к требованиям различных регулирующих органов.

ПРИМЕНЕНИЕ

Кража жесткого диска

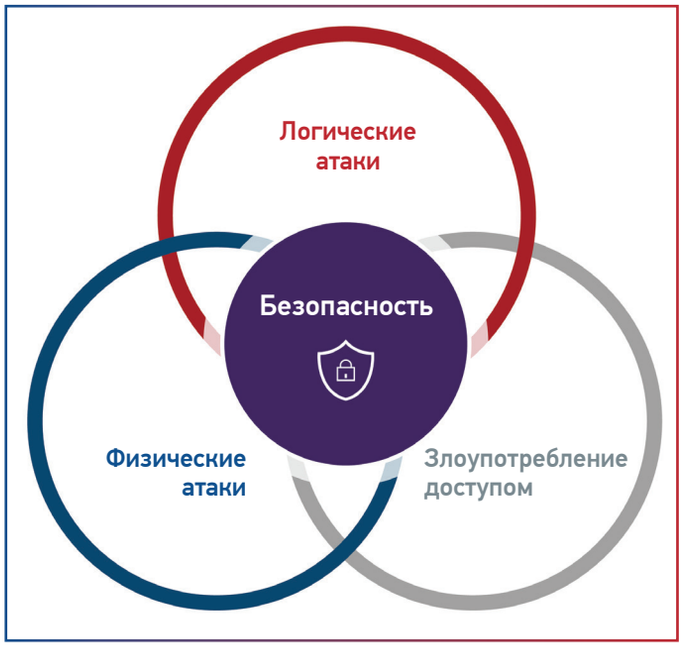
Находящиеся на жестком диске банкомата данные, зашифрованные при помощи модуля Hard Disk Encryption, обеспечивают работу устройства только в заданной программно-аппаратной среде.

Попытки проникновения в систему

Модуль Intrusion Protection позволяет устранять различные уязвимости программного обеспечения, а также предоставлять пользователям, процессам и приложениям только необходимый для работы уровень доступа и ресурсы.

Злоупотребление доступом

Модуль Access Protection позволяет создать строгую и абсолютно контролируемую систему предоставления прав разным группам пользователей: сервисным инженерам, системным администраторам и другому персоналу.



BS2 Penki kontinentai group
ЗАО Penkių kontinentų bankinės technologijos | ул. Карейвю, 2, LT-08248 Вильнюс | Литва | Тел: +370 5 266 45 95 | Эл. почта: info@bs2.lt | www.bs2.lt