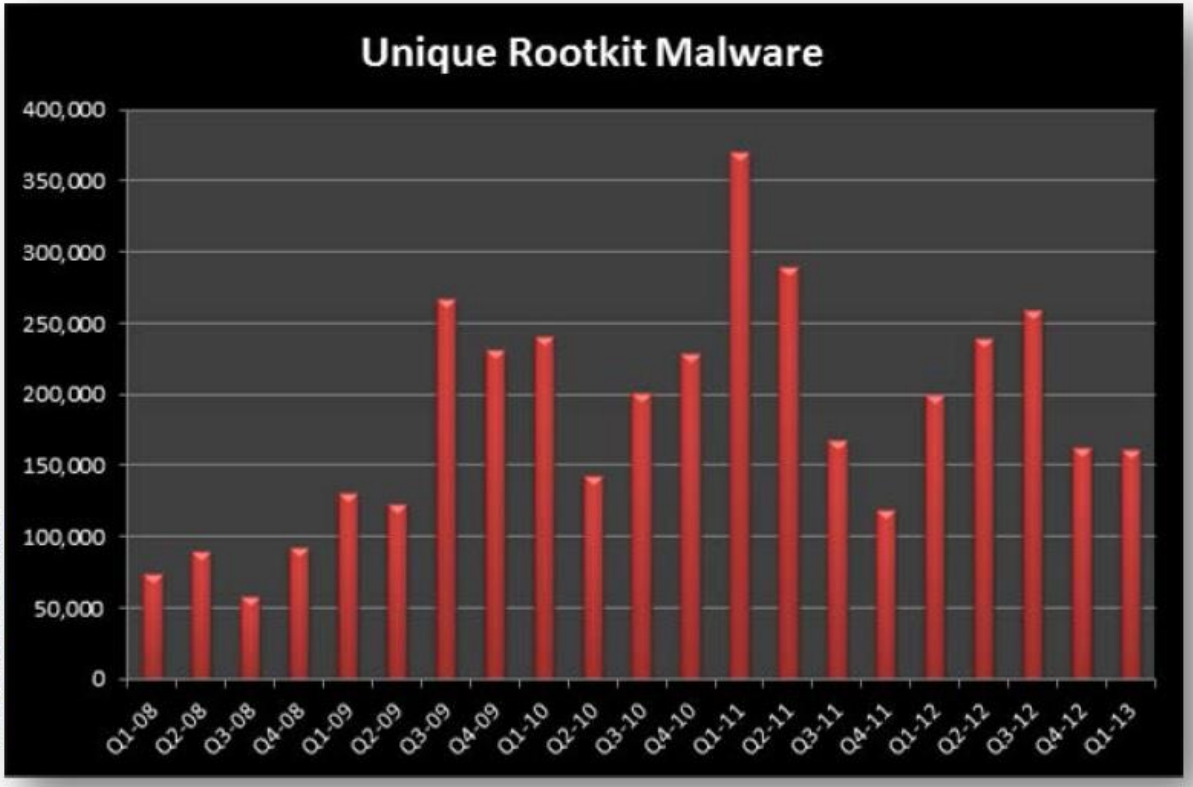
Доверенные вычислительные платформы.
Мифы и реальность

Ренат Юсупов, старший вице-президент

kraftway®
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Москва, 2014

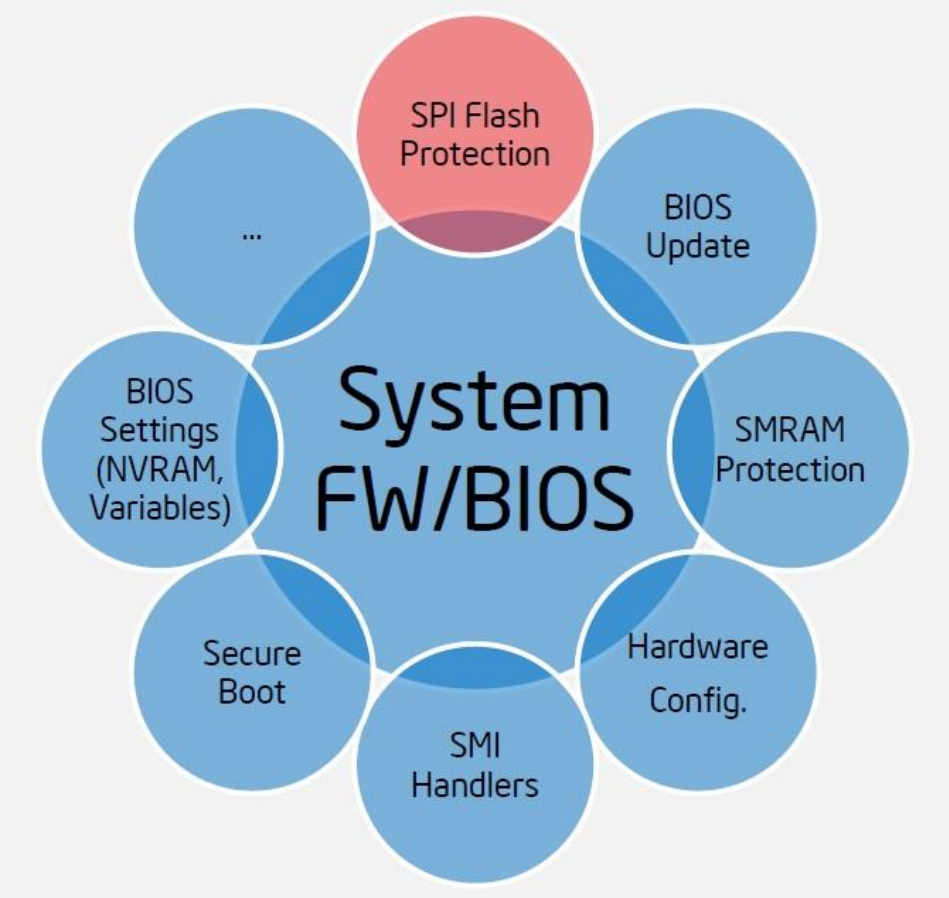
ОЦЕНКА УРОВНЯ УГРОЗ. MCAFEE



Source: McAfee

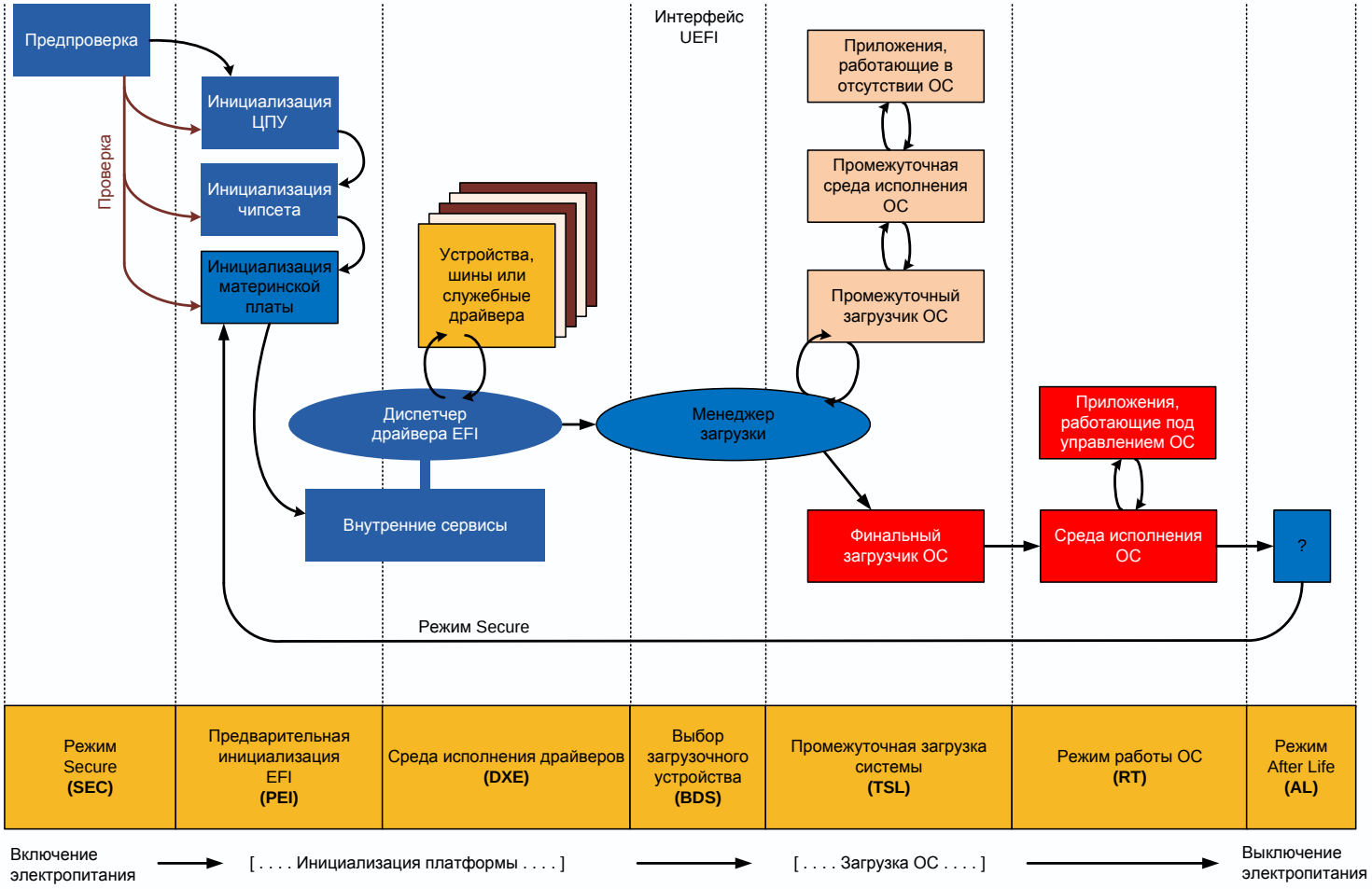
Rootkit Family	Binaries	%
Koutodoor	452,042	21%
TDSS	389,216	18%
Farfli	167,895	8%
MBR	162,605	8%
Caxnet	106,860	5%
Prosti	80,887	4%
DNS Changer	74,010	3%
Cutwail	32,560	2%
LDPinch	18,590	1%
Other rootkit samples	635,040	30%
Total	**2,119,705**	**100%**

Цели низкоуровневых атак



По материалам Intel Security на Devcon 2014

ЛОГИЧЕСКАЯ СХЕМА ЦИКЛА ИСПОЛЬЗОВАНИЯ ПК

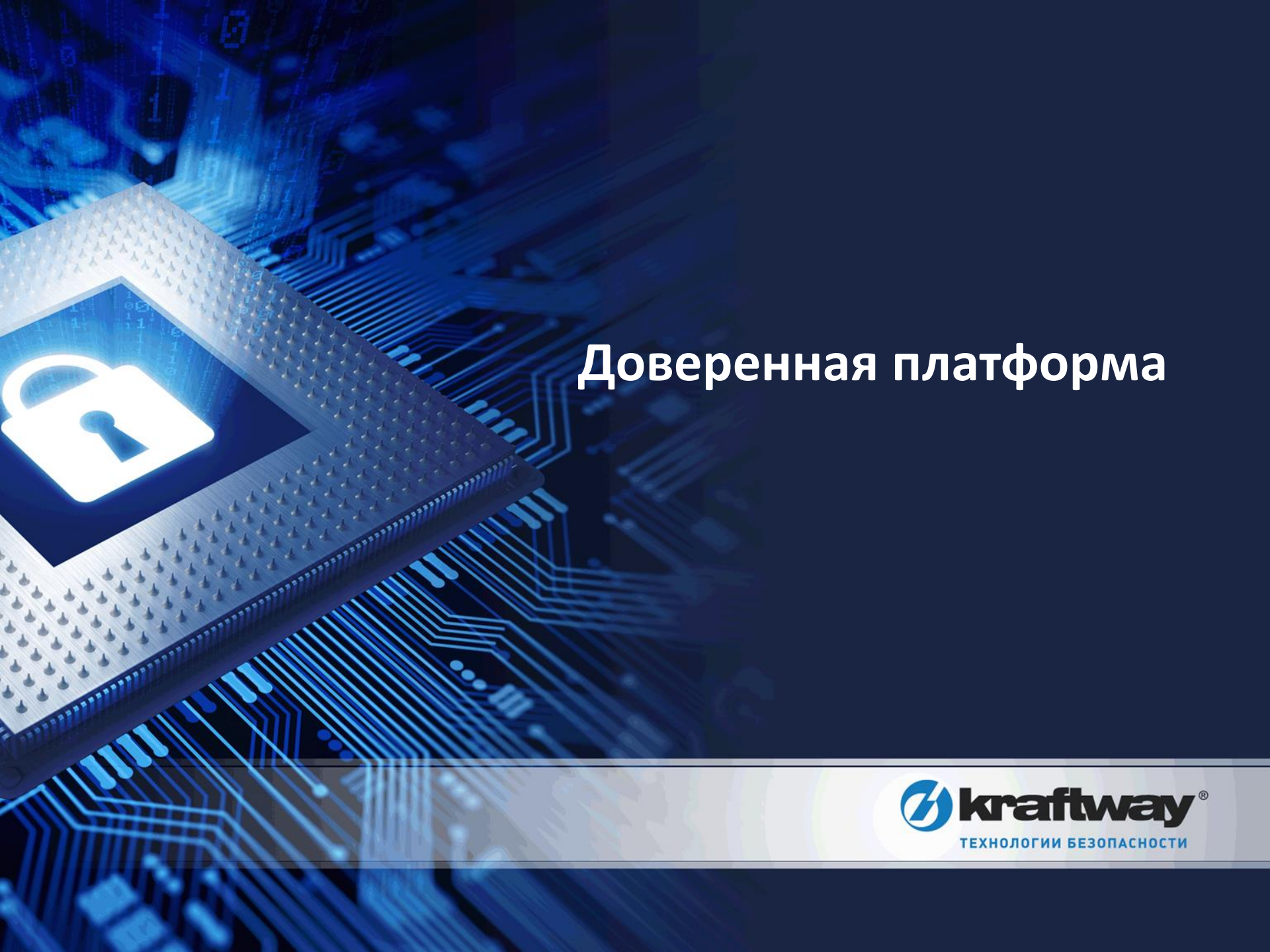


kraftway ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Использование НДВ в BIOS

Утилиты из каталога АНБ сезона 2008-2009

- IRATEMONK – модифицированная прошивка MBR для запуска программы кражи данных;
- SWAP – перепрошивка модифицированными версиями BIOS и HPA HDD для получения удалённого доступа;
- IRONCHEF – SMI функция модифицированного BIOS для передачи информации через встроенную закладку – радиопередатчик;
- DEITYBOUNCE – SMI функция в модифицированном BIOS для удалённого доступа до загрузки ОС;
- JETPLOW, HALLUXWATER, FEEDTROUGH, SOUFFLETROUGH, GOURMETTROUGH – эксплойты в модифицированном BIOS для Cisco, Huawei, Juniper.



Доверенная платформа

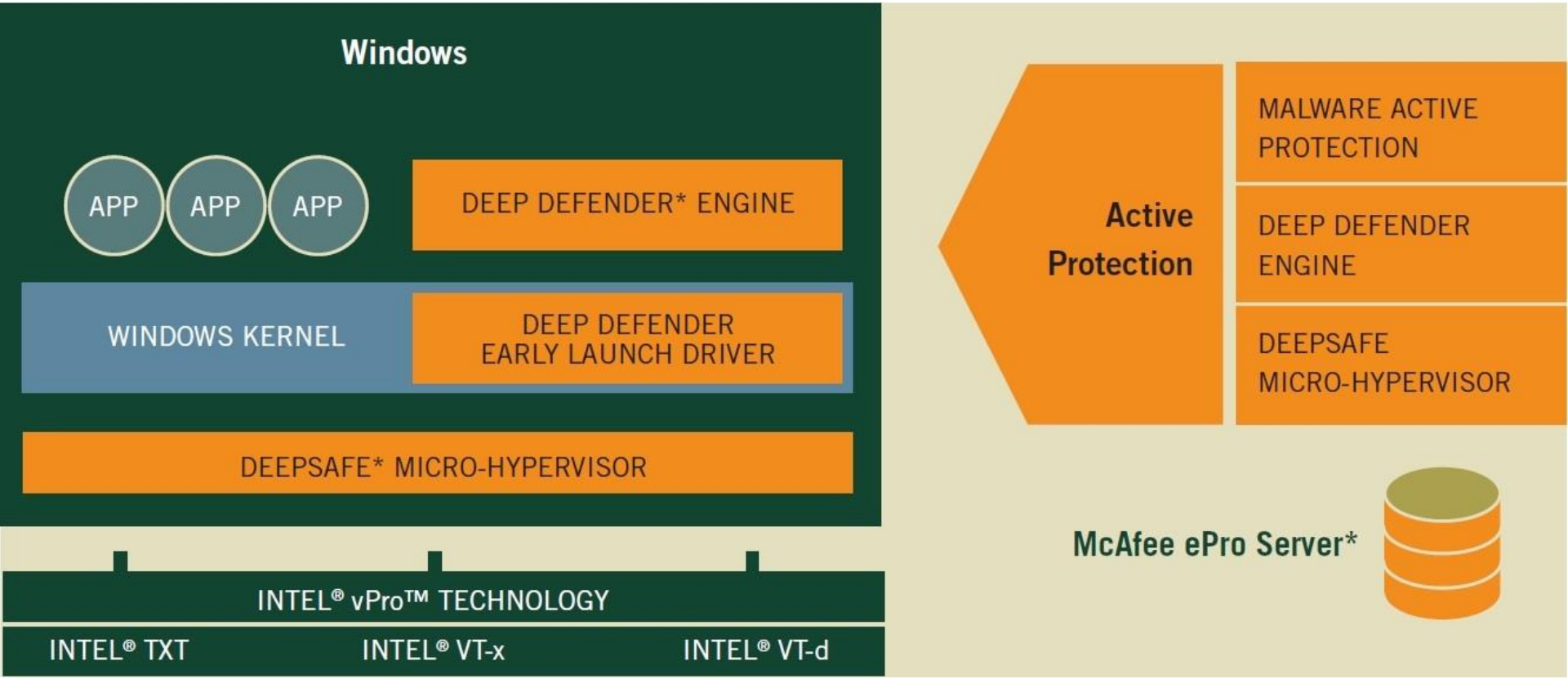
kraftway®
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

КОНЦЕПЦИЯ ПОСТРОЕНИЯ ДОВЕРЕННЫХ ПЛАТФОРМ X86

1. Превентивная модель защиты:
   - непрерывный контроль ключевых объектов и функций,
   - аппаратно-программная изоляция устройств и сервисов.
2. Непрерывная модель безопасности:
   - использование принципа «цепочек доверия» (пример – «secure boot») в цикле работы и в жизненном цикле изделия.
3. Интеграция СЗИ в типовую функциональность платформ:
   - совместимость СЗИ и платформ на уровне проектирования;
   - динамическая настройка на актуальную модель угроз.
4. Разделение среды функционирования СЗИ и стандартных приложений
   - перенос части функций СЗИ и систем управления в BIOS и доверенные виртуальные машины.
   - Приоритет исполнения приложений безопасности над остальными функциями платформ

Доверенная платформа по версии Intel Security

Модель комплексной защиты по версии Intel Security



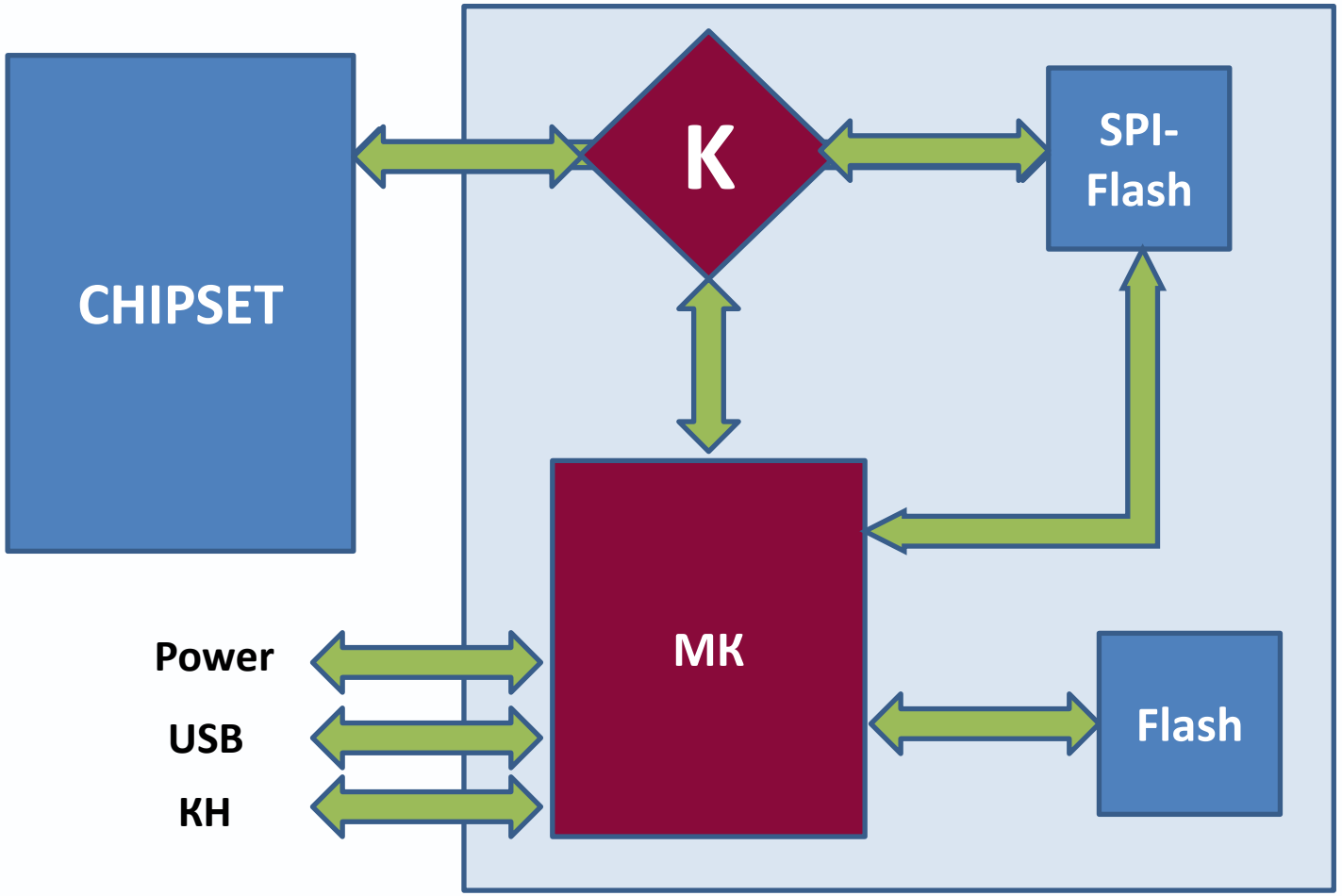
Реализация доверенной платформы

kraftway®
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Платформы. Стандартная vs Доверенная. Часть 1

Защитные функции платформы	Стандартная платформа	Доверенная платформа
Контроль ключевых элементов защиты при запуске платформы	Самоконтроль процессора и чипсета	Контроль FW, BIOS и СЗИ до подачи питания на CPU и chipset. АПМДЗ + KSS
Автоматическое восстановление при запуске	-	Восстановление образов FW, BIOS и СЗИ из защищённого недоступного хранилища
Запуск СЗИ в BIOS	Secure Boot (только в UEFI режиме), либо АПМДЗ (только в CSM режиме)	Микроконтроллер, KSS + СЗИ, АПМДЗ (UEFI)
Низкоуровневый гипервизор	Deepsafe Micro-Hypervisor (Intel Security)	Kraftway Hypervisor + KSS

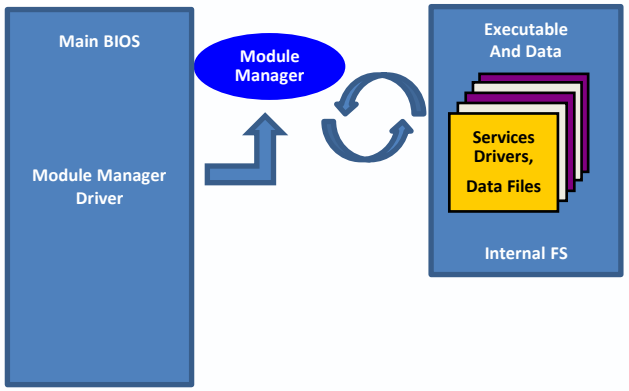
КОНТРОЛЬ И ВОССТАНОВЛЕНИЕ ПРИ ЗАПУСКЕ



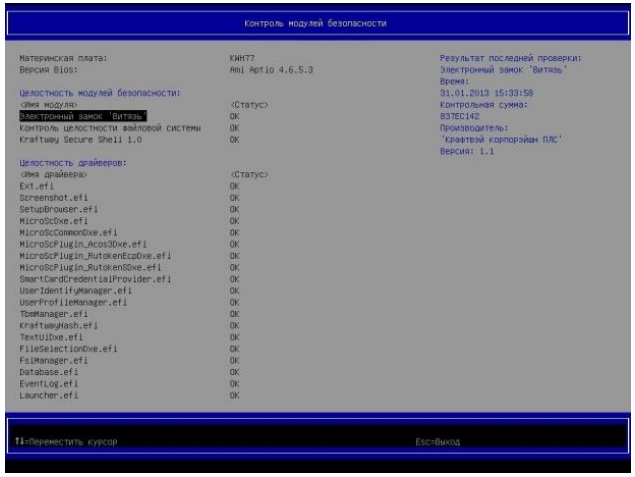
kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

ЗАПУСК СЗИ В BIOS. KRAFTWAY SECURE SHELL

KSS - интегрированная в UEFI среда гарантированного и защищенного исполнения модулей безопасности до загрузки операционной системы.

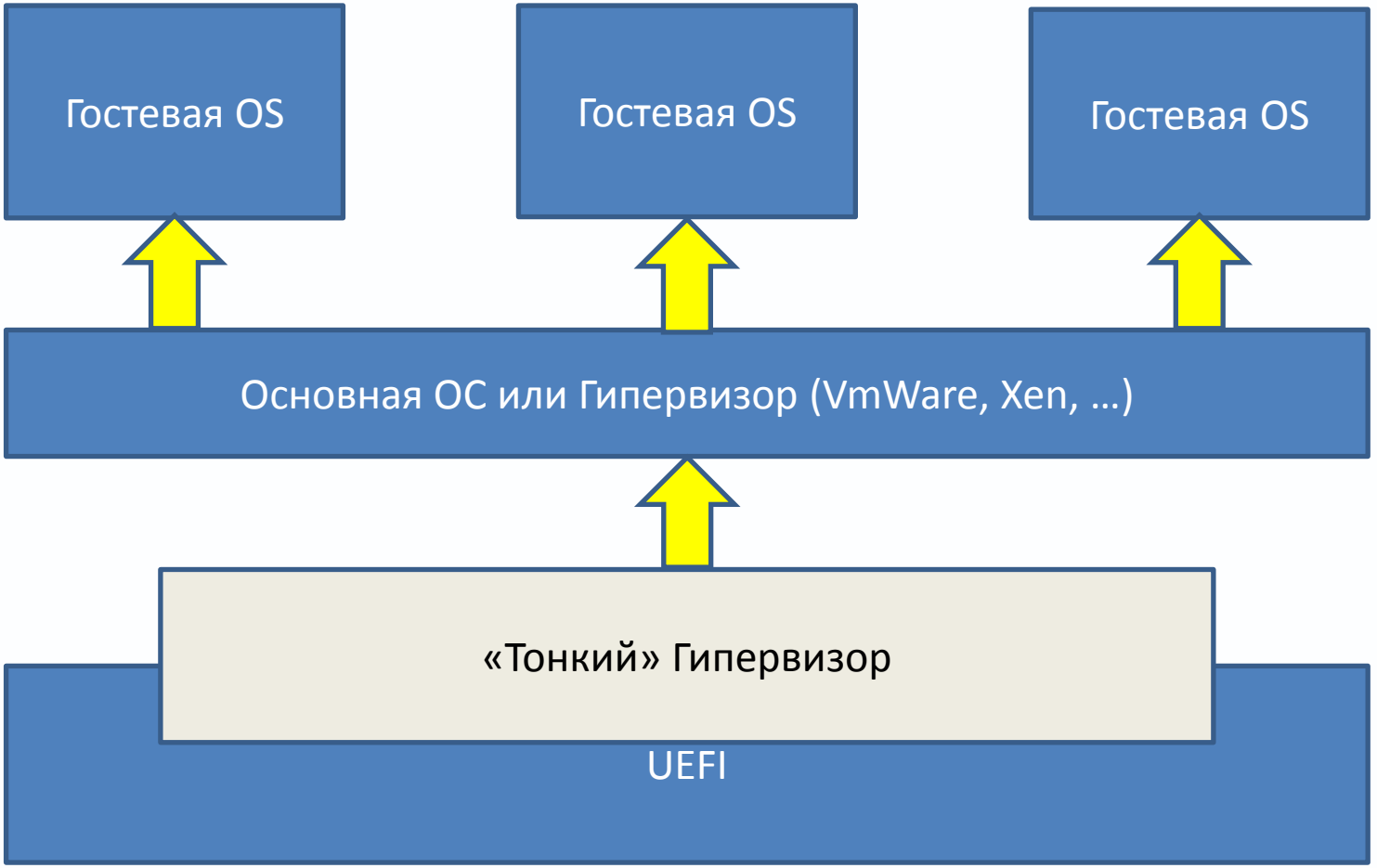


- Открытое API для интеграции модулей других производителей;
- Модули безопасности реализованы в виде Plug-In;
- Легко расширяется, легко портируется;
- Все данные и модели хранятся в защищенной встроенной файловой системе.
- Централизованный дистанционный мониторинг и и управление функциями безопасности через Kraftway Security Center

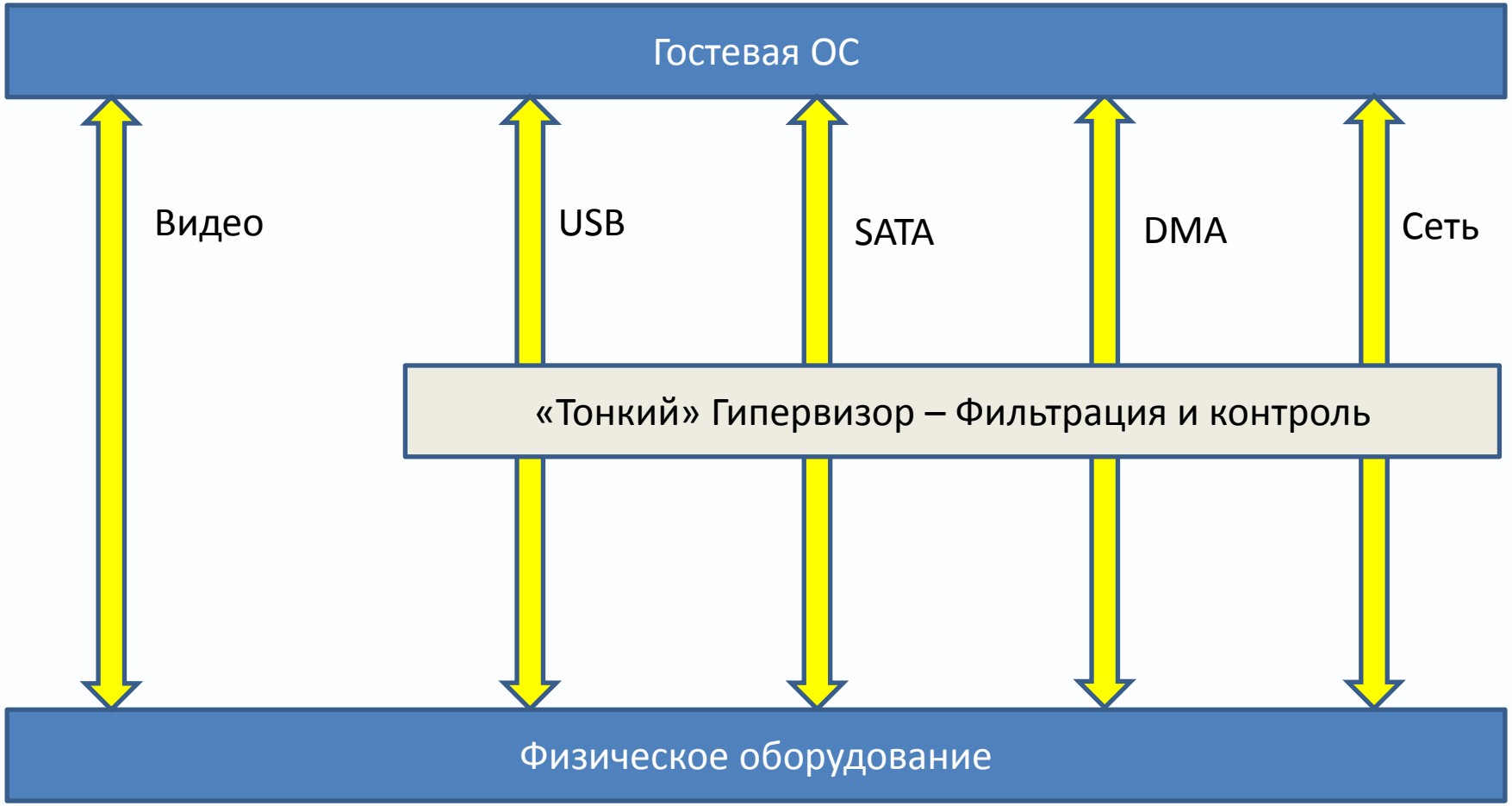


kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

«Тонкий» гипервизор KHV. Часть 1



«Тонкий» гипервизор KHV. Часть 2



kraftway
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ

Платформы. Стандартная vs Доверенная. Часть 2

Защитные функции платформы	Стандартная платформа	Доверенная платформа
SMI функции. Режим высоких привилегий	Без изменений	Адаптированный стек SMI функций, связанный с KSS
ME. Недекларированные возможности	Без изменений	Модифицированный
UEFI. Неконтролируемая сборка	Без изменений	Переработанный
Защита SPI, Boot, CMOS, EFI области. Защита от несанкционированных модификаций	Без изменений.	Недоступны из ОС

Доверенные платформы Kraftway.

- 2014 год
  - ПК
  - Тонкий клиент
- 2015 год
  - Сервер
  - Планшет
  - Моноблок
  - Маршрутизирующий коммутатор
  - Ноутбук

СПАСИБО ЗА ВНИМАНИЕ!

kraftway®
ТЕХНОЛОГИИ БЕЗОПАСНОСТИ