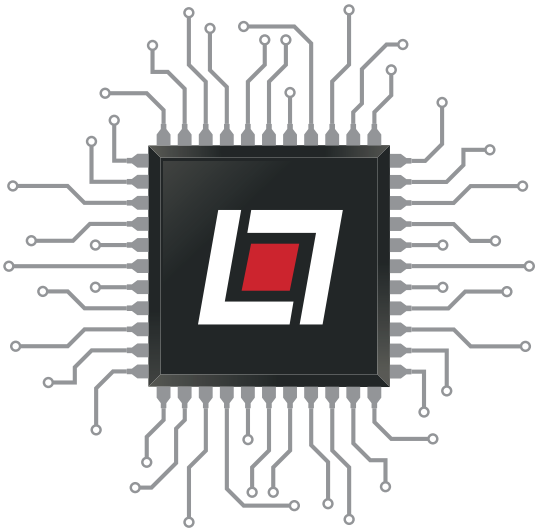


ALTELL TRUST

Новое поколение средств доверенной загрузки

ALTELL TRUST — модуль доверенной загрузки нового поколения, реализованный на уровне UEFI BIOS. В отличие от своих аналогов он обладает уникальными характеристиками: неизвлекаем, может управляться удаленно, поддерживает ролевую модель доступа и многофакторную аутентификацию на удаленных AD/LDAP-серверах, а также обеспечивает контроль целостности BIOS. Благодаря наличию полнофункционального стека сетевых протоколов ALTELL TRUST может использоваться в качестве единственного программного обеспечения в тонких клиентах, что позволяет организовать безопасную работу с VDI-инфраструктурами и терминальными сервисами (например, по протоколу RDP/RemoteFX).

Возможности ALTELL TRUST

Доверенная загрузка:

- контроль целостности BIOS и объектов файловой системы;
- возможность полномасштабного контроля аутентичности и целостности программно-аппаратного обеспечения на основе цифровых подписей;
- журналирование всех этапов работы BIOS.

Контроль доступа пользователей:

- обеспечение мандатного принципа контроля доступа;
- обеспечение ролевой модели доступа и возможности разграничения прав системных администраторов и офицеров безопасности;
- идентификация и авторизация пользователей до начала работы с виртуальным рабочим столом и привязка пользователя к компьютеру;
- поддержка USB-идентификаторов (eToken PRO, eToken PRO (Java) и Rutoken ЭЦП), а также смарт-карт eToken PRO (поддержка CCID, PKCS#11, PKCS#15 для авторизации пользователей);
- поддержка LDAP/AD, X.509, TLS 1.0 (развитие протокола SSL).

Удаленное управление:

- удаленное управление пользователями, конфигурациями, группами устройств, загрузкой обновлений ПО;
- управление с помощью MS SCCM;
- поддержка Intel Active Management Technology (Intel AMT).

ПО тонкого клиента:

- не требуется никакого дополнительного программного обеспечения (в том числе встраиваемого) для работы тонкого клиента;
- поддержка полного стека сетевых протоколов;
- поддержка Microsoft Remote Desktop Protocol (RDP) и RemoteFX.

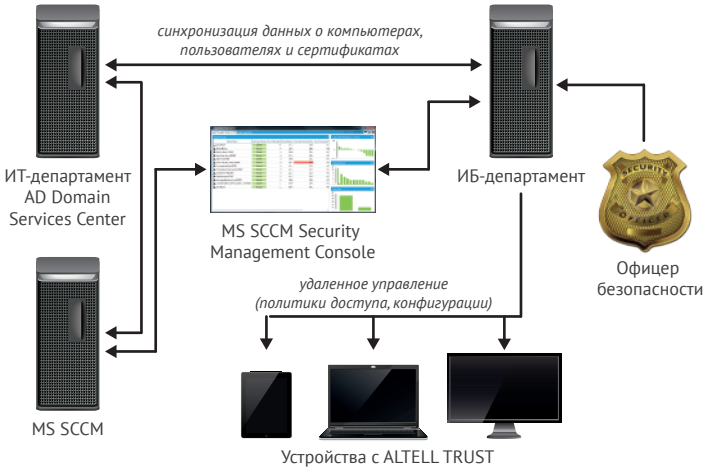
Защита виртуальных сред

- реализована возможность встраивания защищенного гипервизора в BIOS.

Сценарии применения

Аутентификация на удаленных серверах

После включения защищаемого устройства управление сразу передается ALTELL TRUST, который производит начальную инициализацию и проверку оборудования, самопроверку, а также проверку критических областей и файлов операционной системы. Далее запрашивается идентификационная информация пользователя на основе заданной в ALTELL TRUST конфигурации (либо обычный запрос логина/пароля, либо двухфакторная авторизация с использованием USB-токена или смарт-карты). Полученная идентификационная информация отправляется для проверки на серверы департамента ИБ. При этом данные о пользователях на этих серверах синхронизированы с данными ИТ-департамента. В случае положительных результатов проверки пользователю предоставляется доступ.

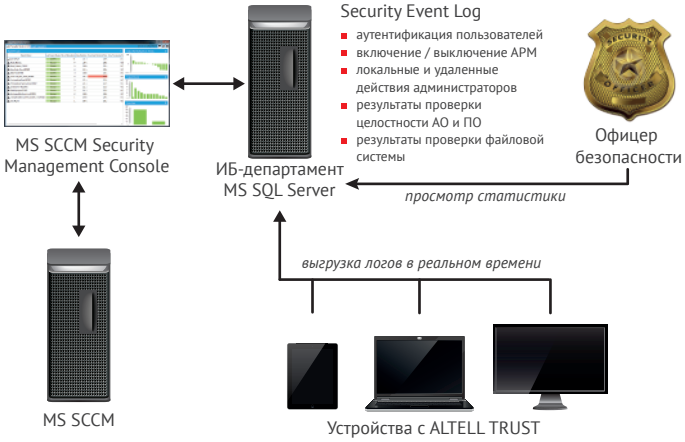


Удаленное управление устройствами

Удаленное управление ALTELL TRUST может осуществляться с помощью двух консолей: для системного администратора (посредством специального плагина, устанавливаемого в MS SCCM) и для офицера безопасности (с помощью АРМ офицера безопасности). При такой схеме работы офицер безопасности управляет правами пользователей и системных администраторов, сертификатами, журналами и аудитом, а системный администратор (если он обладает соответствующими правами) обновляет программное обеспечение и выполняет другие присущие ему функции. Такая схема работы позволяет соблюсти необходимый уровень информационной безопасности, одновременно снижая затраты на администрирование и изменение инфраструктуры.

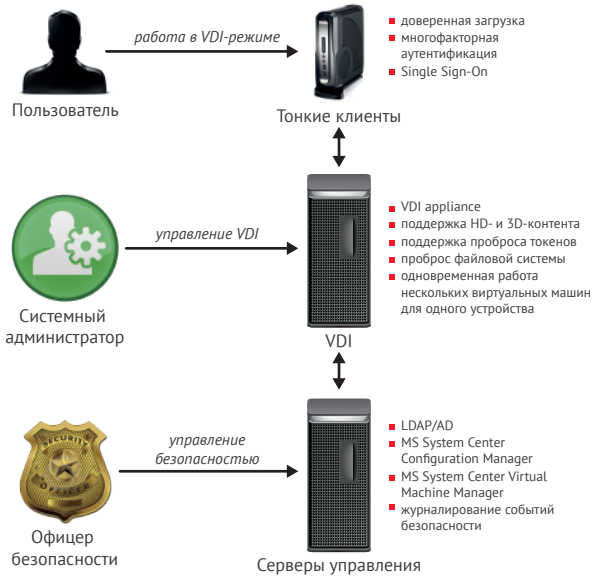
Ведение журнала событий

ALTELL TRUST позволяет выгружать логи из защищаемых устройств в режиме реального времени и импортировать их в другую систему, например, в СУБД Microsoft SQL Server. В журнал записываются факты аутентификации пользователей, включения/выключения АРМ, история локальных и удаленных действий администраторов, а также результаты проверки целостности BIOS, файловой системы, аппаратного и программного обеспечения. Офицер безопасности может работать с базой событий с помощью специализированного рабочего места АРМ офицера безопасности.



ПО тонких клиентов

Наличие полнофункционального стека сетевых протоколов позволяет использовать ALTELL TRUST в качестве единственного ПО тонких клиентов («нулевой клиент»), организовав защищенную работу с удаленными рабочими столами (VDI). Перед подключением к виртуальному рабочему столу осуществляется многофакторная авторизация пользователей с использованием USB-токена и смарт-карты. Образы виртуальных рабочих столов хранятся на серверах и управляются централизованно, что позволяет осуществлять их быстрое клонирование, восстанавливать образы из резервного хранилища, а также сохранять или возвращать состояние такого образа в любой момент времени. Возможность переключаться между несколькими виртуальными машинами позволяет одновременно работать с информацией разного уровня секретности.



Сравнение с конкурентами *

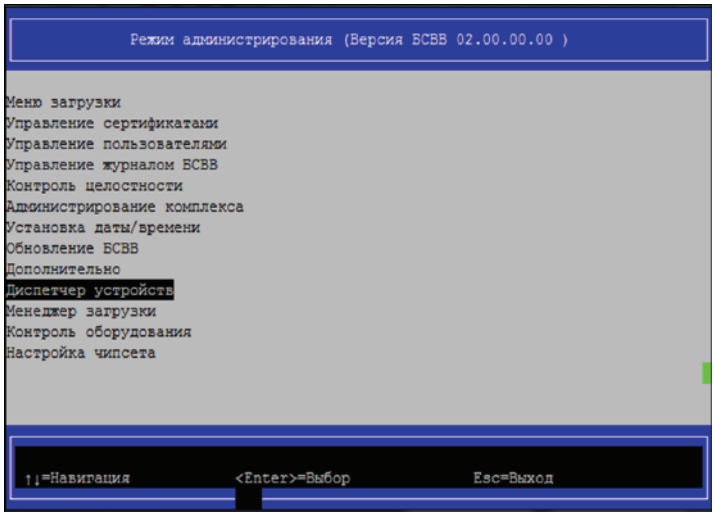
Традиционные аппаратно-программные модули доверенной загрузки не обладают возможностями, необходимыми на современном этапе развития информационных систем: у них отсутствуют функции мониторинга и удаленного управления парком защищаемых устройств, многофакторная аутентификация на удаленных серверах, ролевая модель доступа и ряд других функций:

Характеристика		ALTELL TRUST	Соболь	Аккорд
Варианты исполнения		UEFI BIOS	PCI, PCIe, Mini PCIe	PCI, PCIe, Mini PCIe, Mini PCIe half
Идентификаторы		eToken PRO (Java) + смарт-карты, Rutoken ЭЦП	iButton, eToken PRO (Java) и eToken PRO + смарт-карта, Rutoken + RF, iKey 2032	iButton, Шипка, eToken PRO
Поддержка операционных систем		любая, включая Windows, Astra Linux, ALT Linux , МСВС	Windows, МСВС, RHEL, Mandriva, ALT Linux, Debian	любая, при условии использования поддерживаемой файловой системы
Поддерживаемые файловые системы		FAT, NTFS, EXT2, EXT3, EXT4	FAT, NTFS, EXT2, EXT3, EXT4, UFS	FAT, NTFS, EXT2, EXT3, Sol86FS, QNXFS, MINIX
Контроль целостности	**UEFI BIOS**	+	−	−
	Оборудования	+	+	+
	Системных областей HDD	+	+	+
	Файлов и секторов HDD	+	+	+
	Реестра Windows	+	+	+
Блокировка загрузки с внешних носителей / загрузка с одного доверенного устройства		+	+	+
Сторожевой таймер		+	+	+
Датчик случайных чисел		+	+	+
Ведение журнала безопасности		+	+	+
Удаленный сбор логов/журналов		+	−	−
Программная инициализация комплекса		+	+	−
Возможность криптографической аутентификации		+	−	+
Неизвлекаемость из АРМ		+	−	−
Удаленное управление		+	−	−
Защита сетевых соединений		+	−	−
Управление доступом на основе ролей		+	−	−
Возможность реализации SSO		+	−	−
Поддержка инфраструктуры PKI		+	−	−
БД пользователей	**Энергонезависимая память**	+	+	+
	LDAP-сервер	+	−	−

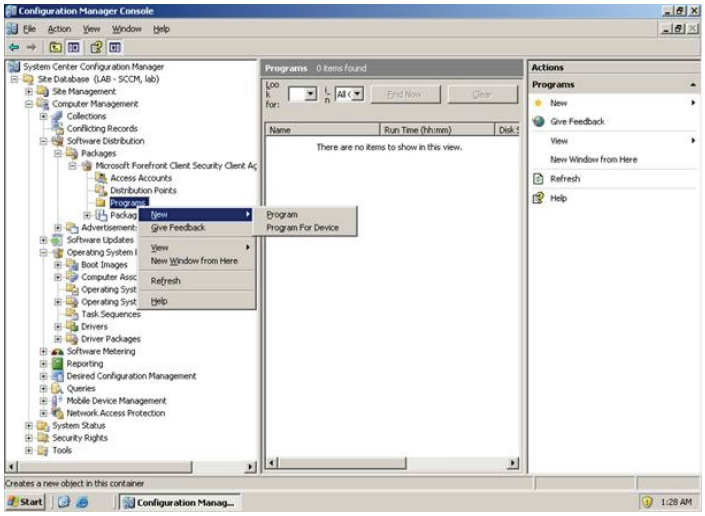
* Данные о характеристиках конкурирующих решений получены из открытых источников сети Интернет в марте 2014 года.

Управление

Администрирование ALTELL TRUST осуществляется через стандартные средства управления и не требует специальных знаний или дополнительного обучения. На рабочем месте администрирование осуществляется через стандартный интерфейс BIOS. Удаленное управление осуществляется с помощью консоли Microsoft System Center Configuration Manager. Для ИБ-специалиста создано специализированное АРМ офицера безопасности.



Консоль UEFI BIOS



Консоль Microsoft System Center Configuration Manager

Платформы

В настоящее время ALTELL TRUST поддерживает:

- моноблоки Lenono ThinkCentre M71z, M72z и M73z;
- ноутбуки Lenovo ThinkPad T520 и T530, Panasonic Toughbook CF-31, CF-53 и CF-AX3;
- планшеты Panasonic Toughpad FZ-G1;
- десктопы Lenono ThinkCentre M92p и M93p, ALTELL FORT 5, 6, 7 и 8;
- тонкие клиенты ALTELL FORT 1600.

В разработке:

- поддержка серверных плат на базе Intel Xeon E3/C2xx;
- поддержка плат для встраиваемых решений на базе Intel Atom N2600/D2550 и NM10, а также AMD G- и R-Series;

При наличии технической информации возможна поддержка большинства материнских плат на базе наборов системной логики Intel 5/6/7/8 Series.

Сертификаты

ALTELL TRUST передан на сертификацию в ФСТЭК и ФСБ России по следующим регулирующим документам:

- ФСТЭК — «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) — по 2 уровню контроля;
- ФСТЭК — «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013) —по 2 классу защиты;
- ФСТЭК — «Профиль защиты средств доверенной загрузки уровня базовой системы ввода-вывода второго класса защиты ИТ.СДЗ.УБ2.ПЗ»;
- ФСБ — «Требования к аппаратно-программным модулям доверенной загрузки» на класс 3Б.

Срок получения сертификатов — IV квартал 2014 года.

Контактная информация

ALTELL
IT Innovations & Security

Санкт-Петербург

ООО «АльтЭль»
Цветочная ул., д. 18, литера Б, офис 301,
БЦ «Бизнес-Парк», 196247
Тел.: +7 (812) 309-05-88
Факс: +7 (812) 677-34-71
e-mail: sales@altell.ru

Москва

ООО «АльтЭль»
2-я Звенигородская ул., д. 13,
стр. 43, офис 407, 123022
Тел.: +7 (495) 664-22-40
Факс: +7 (812) 677-34-71
e-mail: sales@altell.ru

Координаты партнера