

Управление на инциденти със сигурността и ИТ активи в реално време

Веселн Янков
Novell България
VYANKOV@NOVELL.COM

Novell®

Законодателството:

НАРЕДБАТА ЗА ОБЩИТЕ ИЗИСКВАНИЯ ЗА ОПЕРАТИВНА СЪВМЕСТИМОСТ И ИНФОРМАЦИОННА СИГУРНОСТ, в сила от 25.11.2008 г. Приета с ПМС № 279 от 17.11.2008 г., обн. ДВ. бр.101 от 25 Ноември 2008, урежда общите изисквания за оперативна съвместимост и мрежова и информационна сигурност за нуждите на предоставянето на вътрешни електронни административни услуги и обмена на електронни документи между администрациите, 1 това число изисква решаване на следните казуси в системата на държавната администрация на Република България:

В наредбата се казва:

Чл. 27. (1) Ръководителите на администрациите осигуряват сертификация на вътрешните правила като "Система за управление на информационната сигурност" по смисъла на ISO 27001:2005 от оправомощена за това организация.

Стандарта ISO 27001:2005 засяга и управлението на активите, като изисква:

- *Категоризиране / класифициране/ на информационните активи*
- *Създаване и актуализиране на детайлизирани оценки*
- *Периодично инвентаризиране*

Novell®

Фундамента :

Q: Какво стои в основата на информационната сигурност ?

A: Възможността перманентно, динамично да “виждаме” и контролираме всички ИТ активи

Решение: ZEN Asset Management от Novell

Възможности за:

- Инвентаризация на активите • Управление на активите

– Хардуерна инвентаризация

- > Пълна системна информация

– Софтуерна инвентаризация

- > Патентована технология за разпознаване
- > Месечни ъпдейти

– Изследване на мрежата

- > Идентифициране на устройствата закачени в мрежата
- > Използване на SNMP/WMI
- > Откриване на устройства с/без ZAM клиент



– Използваемост на софтуера

- > Сведения за локално инсталирани и сървърно базирани приложения
- > Кои продукти се използват и кои не и от кого

– Управление на софтуера

- > Картина на съответствие – закупени лицензи с инсталиран софтуер
- > Проследвяване на лицензите – въвеждане на данни при покупка

– Управление на договори

- > Договори за хардуер и софтуер
- > Поддръжка, наем, гаранция, ключови дати и срокове
- > Прикрепяне на документи за поддръжка

Основни характеристики

- Сканиране и откриване на софтуерни продукти, сървъри, персонални компютри, мрежови устройства
- Използва разширена база “знания” - над 70 хил продукта
- Разширяема архитектура
- Конфигурации - проследяване на историята им
- Разширяема база справки - потребителят определя полетата
- Сканиране по запитване (on demand)
- Web-базиран достъп
- Известяване при „инцидент“

Благодарение на ZEN Asset Management
ще знаете с какво разполагате, къде и
в какво състояние се намира, как се
ползва

Инвентаризация на активите

Дефинирана База знания

Базирана на простия въпрос: От каква информация се нуждаят ИТ мениджърите и как ще я използват?

- Съгласуване на ниво данни и приложения
- Нормализиране на описанието на продукта
 - Производител, Име на продукта
 - Версия, Език и Patch level (SP, SR, и т.н.)
- Детайлизирана информация за продукта
 - Свързаност на дефинираните компоненти пакет/ пакет
 - Класификация на типа продукти, например Comm Software/Chat Software, System, Monitor
 - Кодирани лицензни данни за софтуера
- Възможност за създаване на софтуерни дефиниции за продукти и софтуерните пакети според нуждите на клиента
- Месечни ъпдейти, поставени на web-сайт(PRUs)

Достоверна информация „on demand“

Novell® патентова технология за разпознаване, която доставя описателен и четлив резултат за приложенията.

Manufacturer	Product	Version	Installations	History
Microsoft	Visio 2000	6.0 SR-1 Pro	<u>2</u>	View
Microsoft	Visio 2000	6.0 SR-1 Tech	<u>1</u>	View
Microsoft	Visio Professional 2003	11.0 SP1	<u>2</u>	View
Microsoft	Visio Professional 2003	11.0 SP2	<u>3</u>	View
Microsoft	Visio Viewer 2002	10.0	<u>4</u>	View
Microsoft	Visio Viewer 2003	11.0	<u>3</u>	View
Microsoft	Visual Basic	6.0 SP-6	<u>1</u>	View
Microsoft	Visual Basic	6.0	<u>2</u>	View
Microsoft	Visual Basic .NET Standard 2003	7.1	<u>2</u>	View
Microsoft	Visual Basic Enterprise Edition	6.0 SP-6	<u>1</u>	View
Microsoft	Visual C++	6.0 SP-6	<u>1</u>	View
Microsoft	Visual C++	6.0 SP-4	<u>2</u>	View
Microsoft	Visual C++	6.0 SP-3	<u>1</u>	View
Microsoft	Visual C++	6.0	<u>2</u>	View

Незабавно постигане на целта



Бърз достъп до данните!



Нормализирана информация



Справки, отчети, аргументи, контрол =
управленски решения

Вече знаете кои активи как и доколко се
използват

Използване на софтуера

- Проследяване използването SW за:
 - Локални и сървърно базирани приложения
 - Приложения, стартирани чрез браузър
 - Приложения, обслужвани от Citrix и Windows Terminal Server
- Преглед на всички приложения, включително дефинирани от потребителя
- Измерване както на общото време за работа, така и на това за което приложението е било активно в прозорец
- Анализи на атрибути по работна станция и по потребител

Ефективност на инвестициите

- Колко бихте спестили от цената на лицензи, ако копувате само това, което наистина се използва?
- Колко бихте спестили при договориране с продавачите, ако знаете колко лиценза реално са ви необходими?



Цялата картина:
Лицензи + Използване + Инвентаризация

Contract Management - ползи

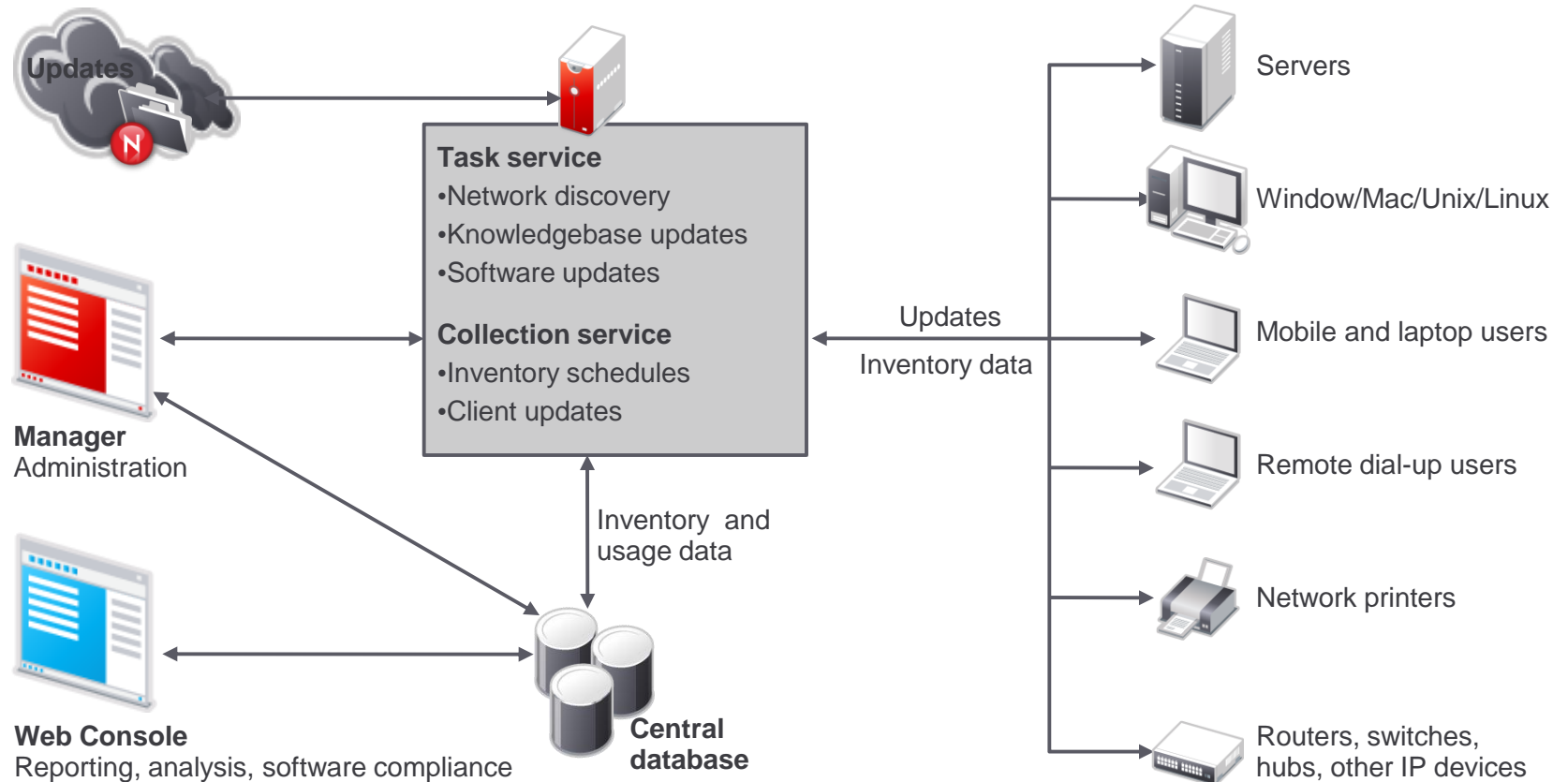
- Увеличена видимост и яснота
 - Намалява риска от неспазване на срокове и условия
 - Подобрява позицията пред производителя при договаряне
 - Дава ясна картина на какво има право maintenance/support
- Намаляване на цената
 - Елиминира закъсняване на вноски след връщане на оборудване под наем
 - Намалява разходите свързани с липсващи подновявания на лицензи
 - Намалява времето за откриване/управляване на договорните документи
 - Намалява времето за локализиране на активите свързани с договорите

Contract Management възможности

- Запис и управление на всички типове ИТ договори
 - Maintenance, наем, гаранция, сервис
- Ключови дати за проследяване
 - В сила, на прекратяване, на подновяване
- . Прикрепяне на документи
- . Записване на ключови срокове и условия
- . Свързаност на активи, потребители, отдели, лицензи
- . Проследяване историята на подновяване на лицензи
- . Добавяне на атрибути с полета дефинирани от потребителя

Architecture

ZENworks® Asset Management





ZENworks Asset Management demo

Access to ZENworks Asset Management demo.

<http://www.novell.com/solutions/resourcemanagement/assetmanagement/demo.html>

Username = zamdemo

Password = novell

SIEM или Log Management ?

Изборът:

- управление на инциденти в реално време -
real time SIEM

или

- контрол и разследване при необходимост - **Log Management**

... се определя от нуждите и целите/задачите които вашата организация си поставя.

Задължителните общи законодателни изисквания (compliance) се покриват и от двата продукта.

И все пак ... SIEM или Log Management



Log Management

- Troubleshooting
- Контрол върху „поведението“ на потребителите
- Съответствие със стандартите
- Разследване за неправомерни/криминални действия
- Контрол върху функционирането/състоянието на системите (health monitoring)

SIEM

- Детайлна корелация на събитията
- Разрешаване на проблемите в реално време
- Задълбочени разследвания за неправомерни действия или закононарушения
- Съответствие със стандартте

Защо организациите ползват LM / SIEM

анкета на SANS Institute (www.sans.org)



Първите 5 от 10 формулирани причини:

1. Проследяване на неправомерни действия и мониторинг на действията на потребителите
2. Текуща администрация и Process Control Compliance
3. Разследване и анализ на престъпни действия
4. Доказване на съответствие със стандартите и наредбите
5. Управление на сигурността на мрежите

Предизвикателствата и в двата случая са сериозни !

- Log retention and Compliance
- Performance
- Reporting
- Secure log transfer and management



Предизвикателствата... Log retention and storage, performance



- корпоративните ИТ системи генерират неимоверни количество Log-ове
- Стандартите изискват архивиране за срок от 1 год. (PCI) до **7 год. за Basel II**
- предвиждаме ли средства за филтриране и запис само на необходимите/задължителни събития
- решаваме ли проблема с унификацията и стандартизацията на Log-овете (parsing & standartizing)
- производителност: какво значи EPS (events per second) в нашия конкретен случай ? Къде е „тавана“ на предлаганото решение? Как се измерва ?

Предизвикателствата.... searching and reporting, secure log transfer

- какви средства за търсене и анализ се предлагат. Бърздействие и ефективност?
- Колко и какви „готови“ рапорти се предлагат. Възможна ли е кustomизация за конкретните ви специфични нужди?
- колко е сигурен механизма на събиране, трансфер и архивиране? Можете ли да представите доказателства, че информацията е автентична и не е била обект на допълнително човешко въздействие?



Novell Sentinel 6.1 SIEM

The slide features a solid blue background. In the center, the text 'Novell Sentinel 6.1 SIEM' is displayed in a white, sans-serif font. At the bottom of the slide, there are several horizontal white lines of varying thickness and opacity, creating a decorative effect.

Функционалност

Събира информация от компонентите на ИТ системата:

network devices – routers, firewalls

security devices - intrusion detection/prevention systems

operating systems

applications – anti-virus, ERP

databases



Функционалност

Събитията се:

- събират от всички или от определени системи/компоненти
- Парсинг и нормализация (parsed and normalized)
- корелация с цел разкриване на потенциален инцидент
- всеки инцидент се “присвоява на отговорното лице за разрешаване (e-mail, alerts)
- всичко се архивира в базата но е достъпно при необходимост за анализи
- процеса протича в реално време
- предвидена/възможна е интеграция с решението за управление на идентичностите/достъпа (identity, asset management)

Гъвкава архитектура

Скалируем дизайн -
distributed approach
using iScale message
bus

Разработен за внедряване в
“разпределени” системи
(multi-site scenarios)

Позволява дублиране на
компонентите на Sentinel за
постигане на висока
производителност (higher
event rates)

специализирани Collector
Managers

ефективни корелационни схеми

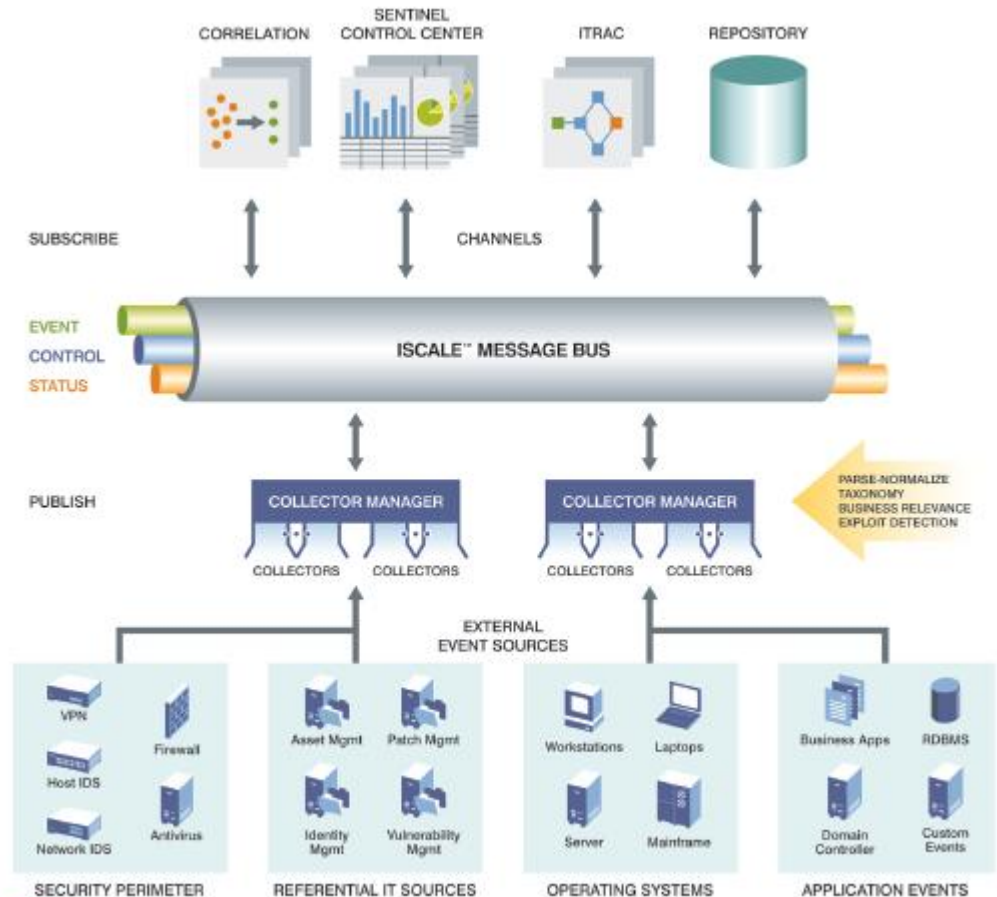
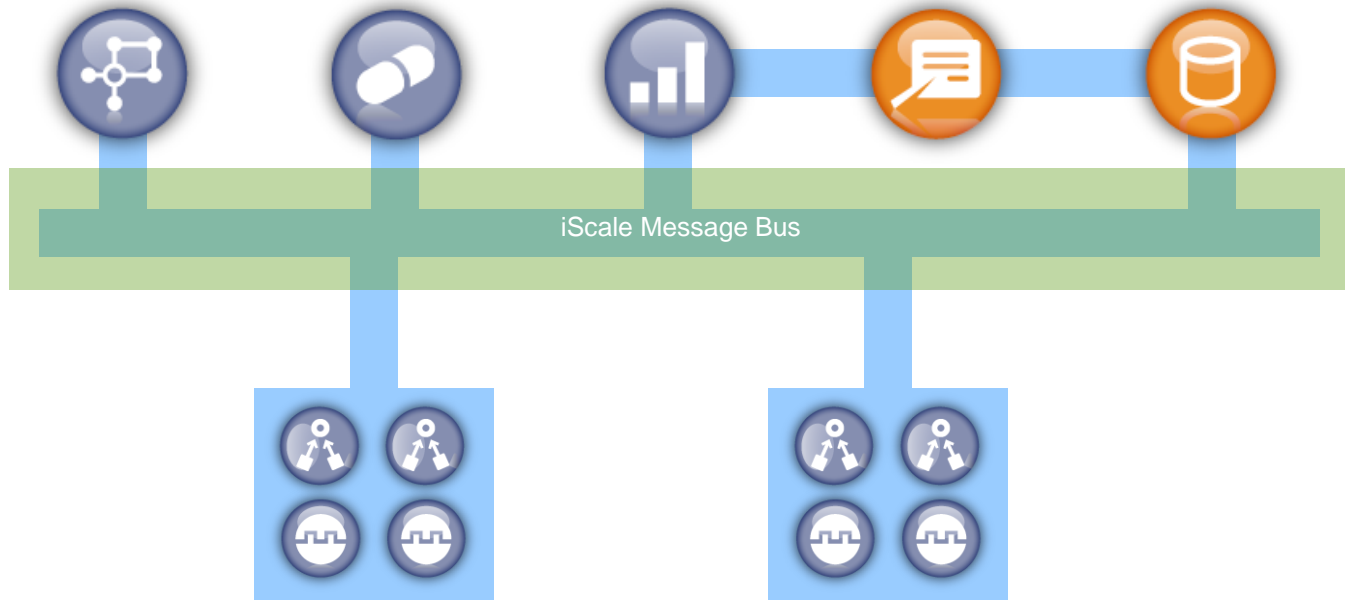
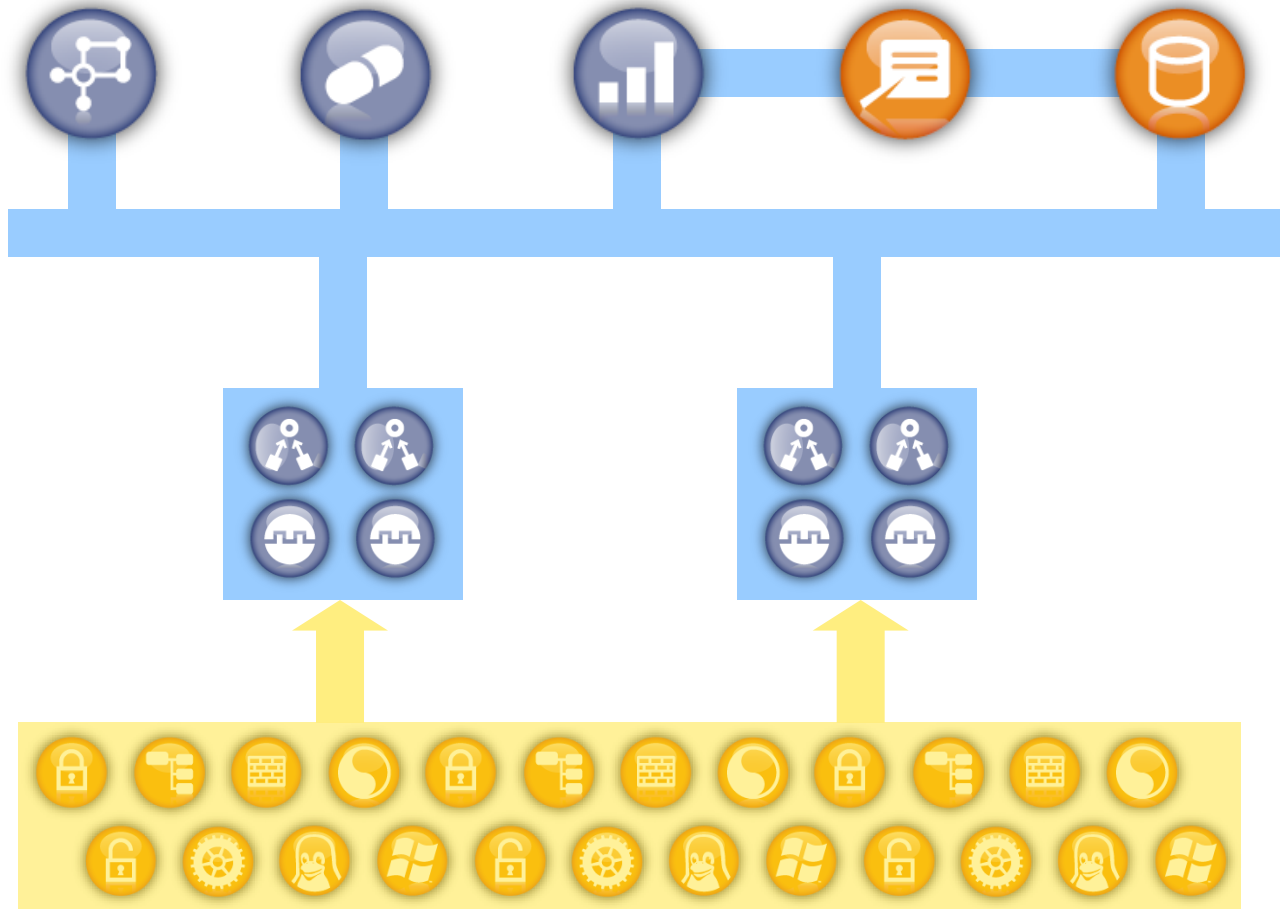


Figure 1. Sentinel Architecture

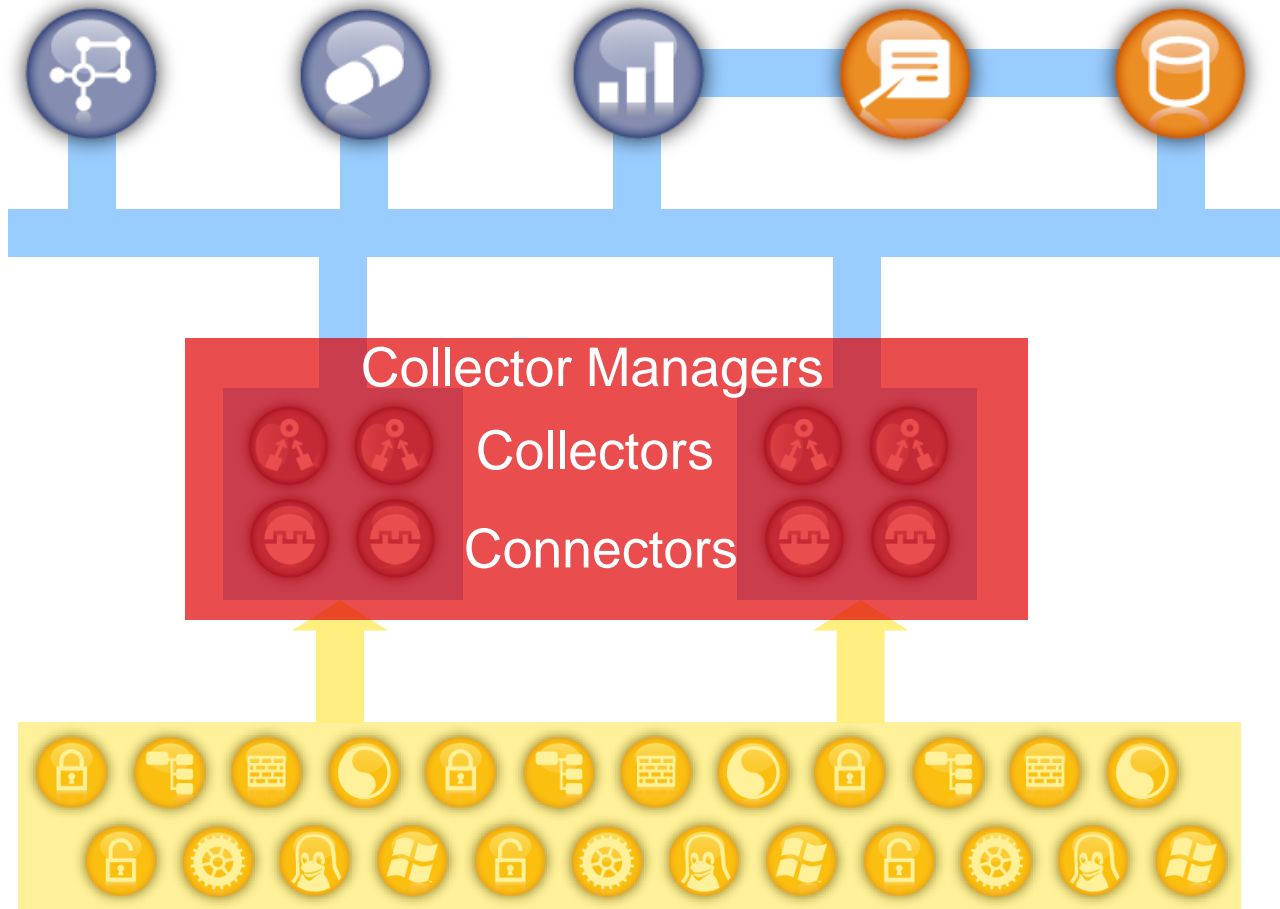
Architecture



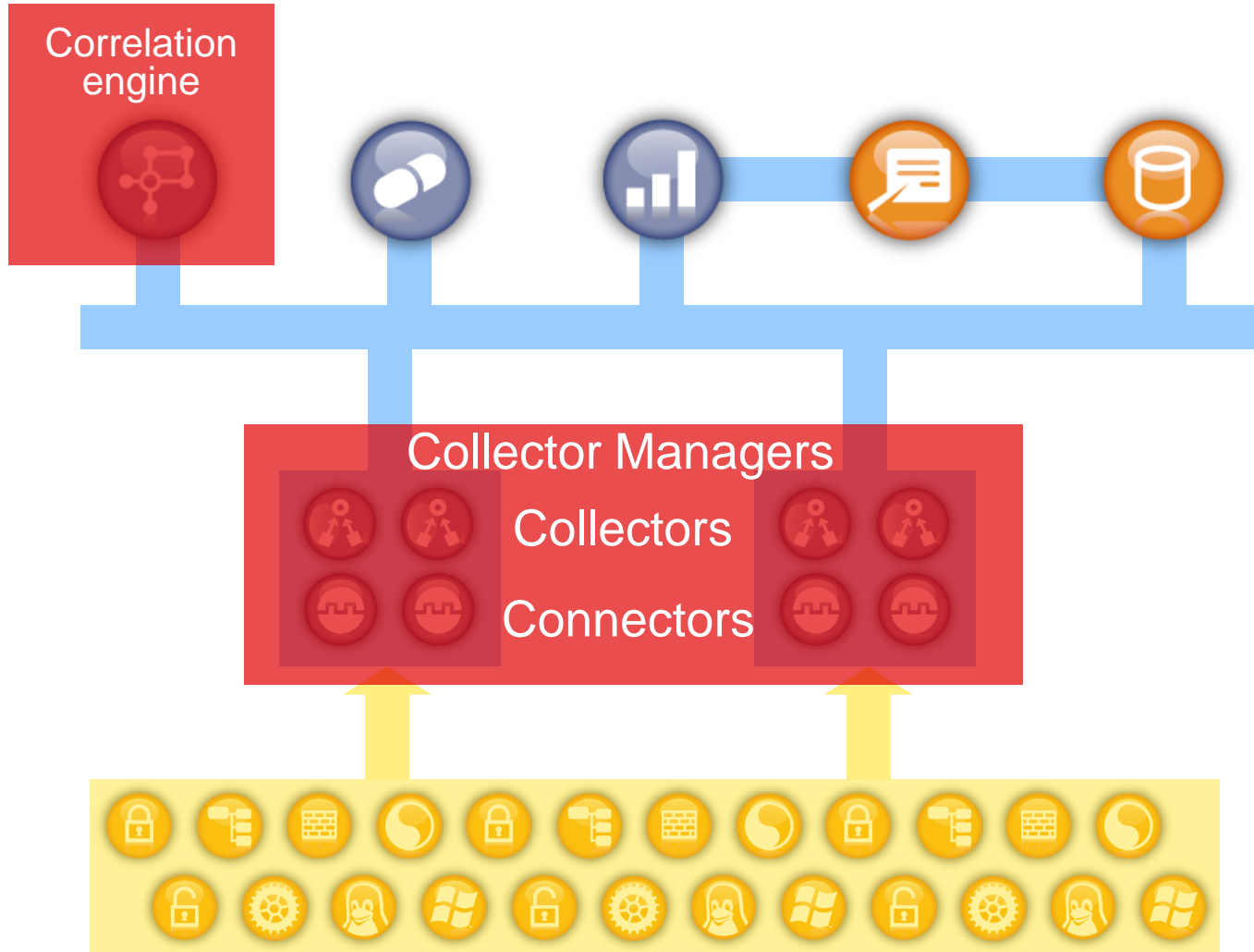
Architecture



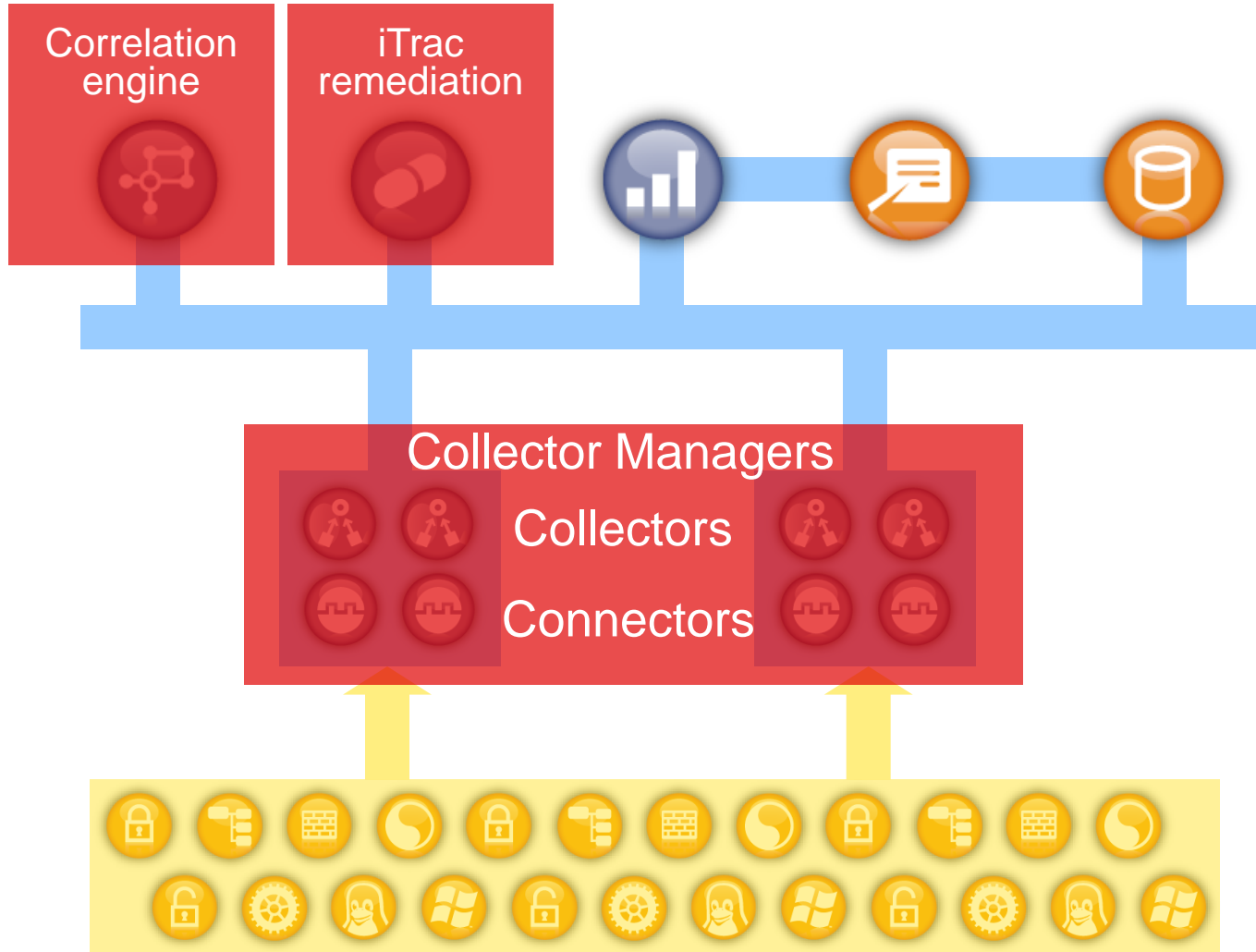
Architecture



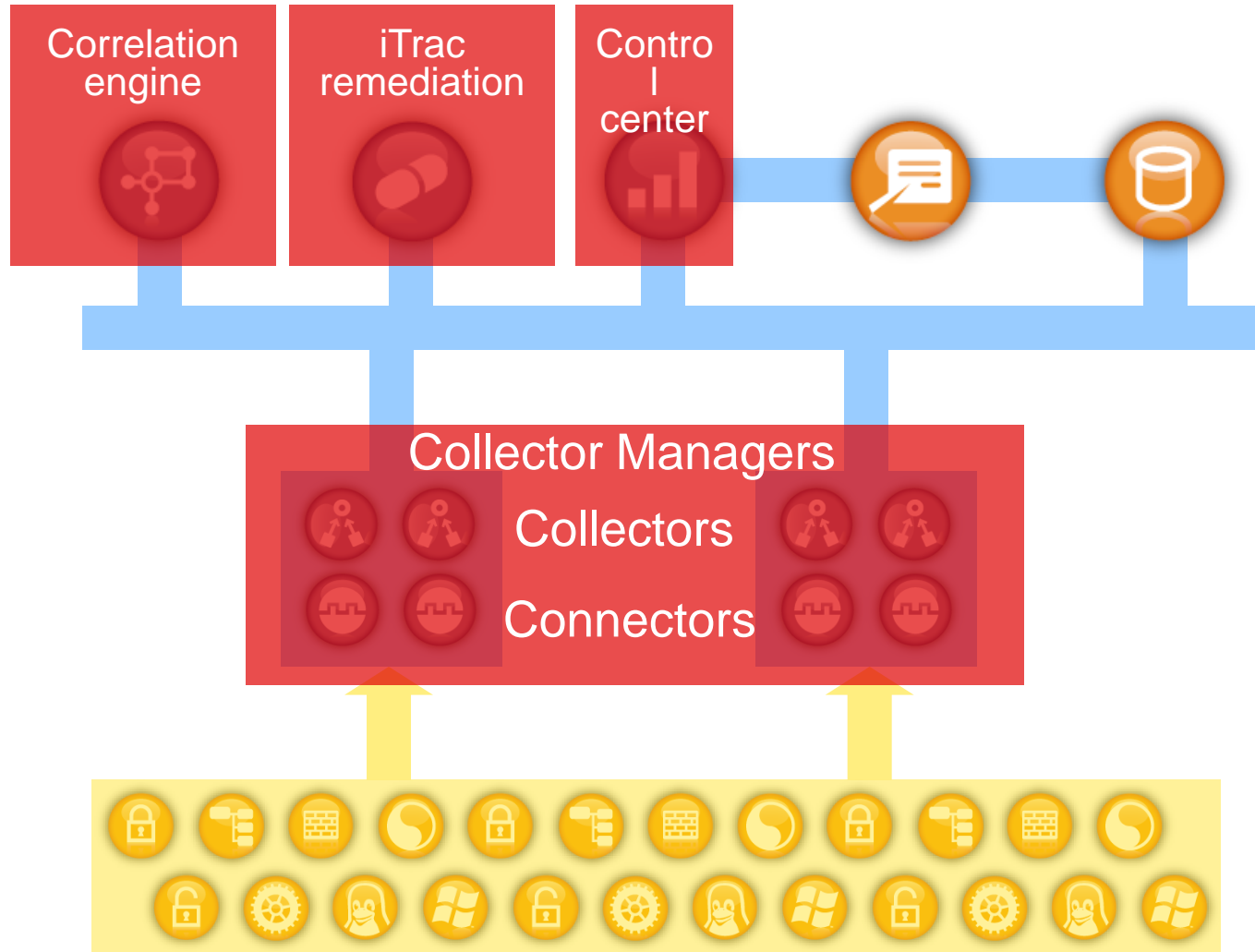
Architecture



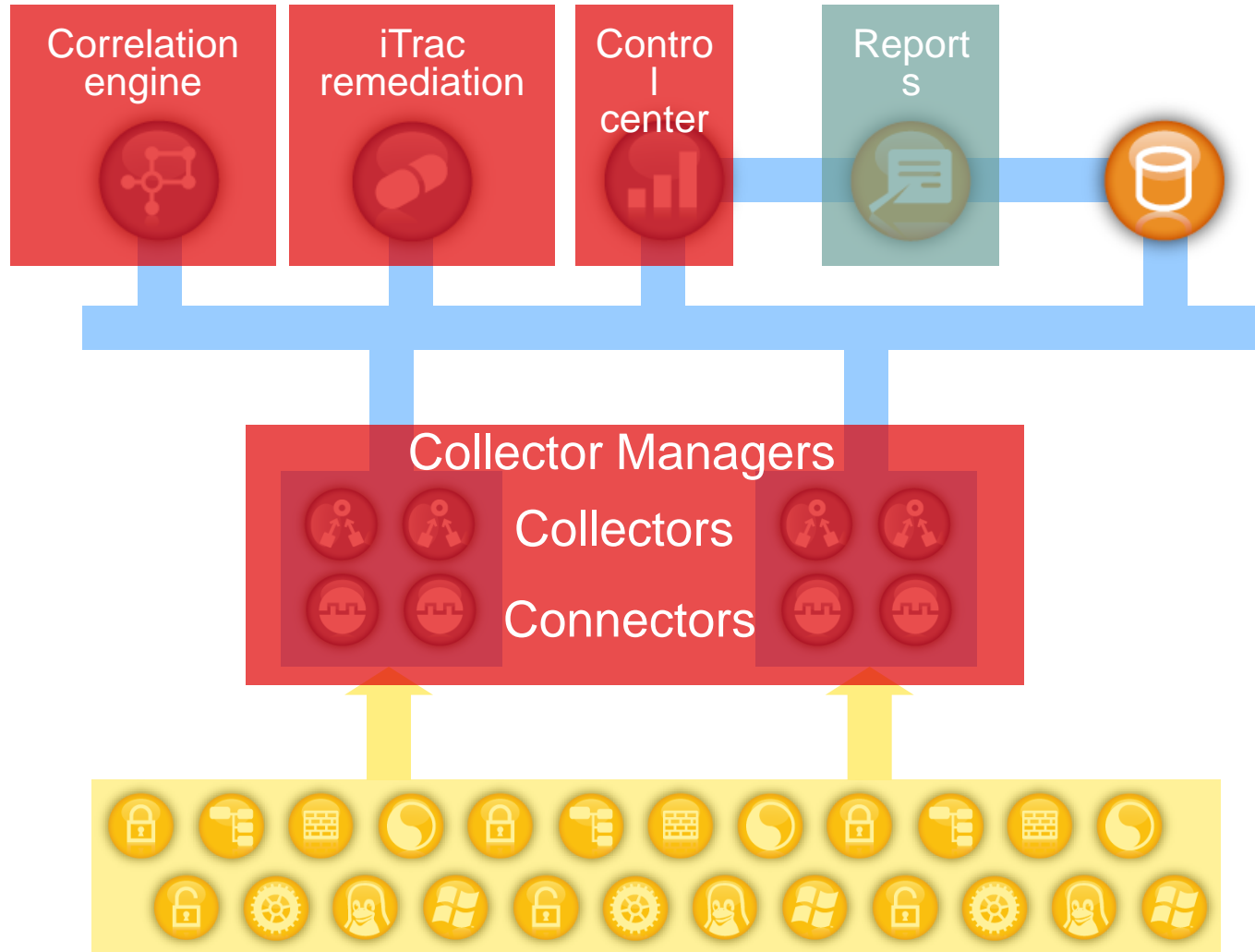
Architecture



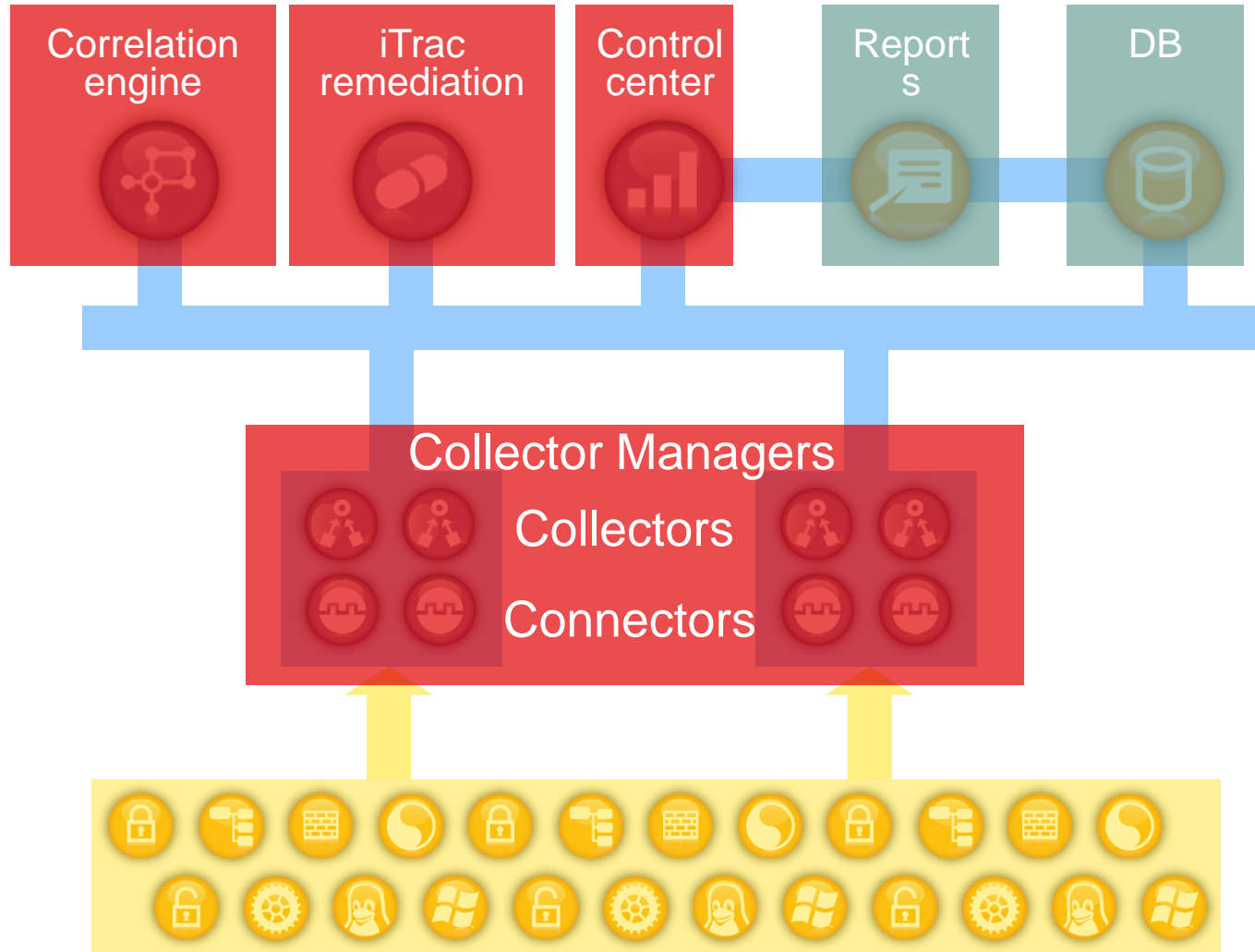
Architecture



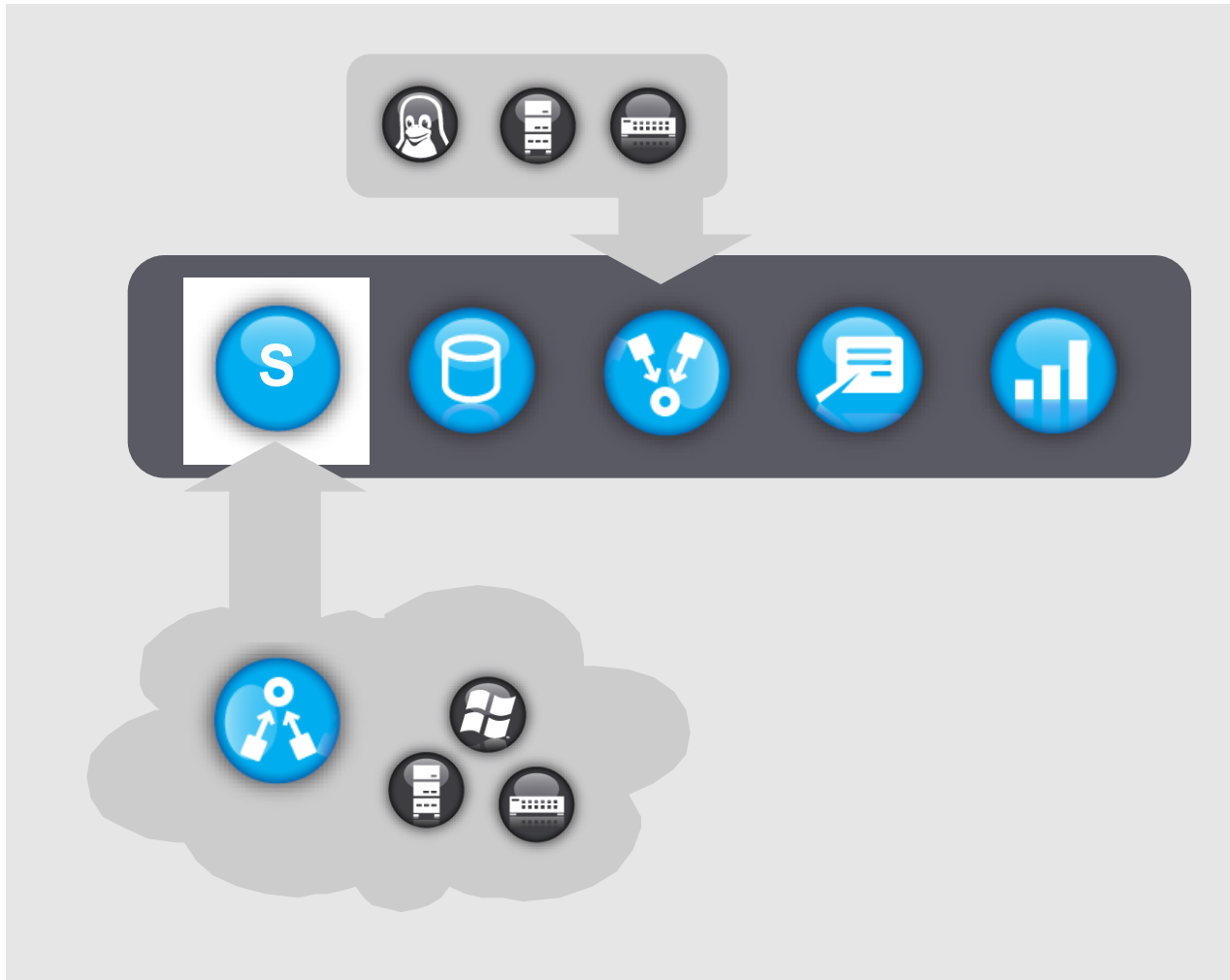
Architecture



Architecture



Distributed Deployment Scenario



Solution Packs

Solution Packs are targeted content packages that have prepackaged correlations, reports and processes

Identity Management Solution Pack

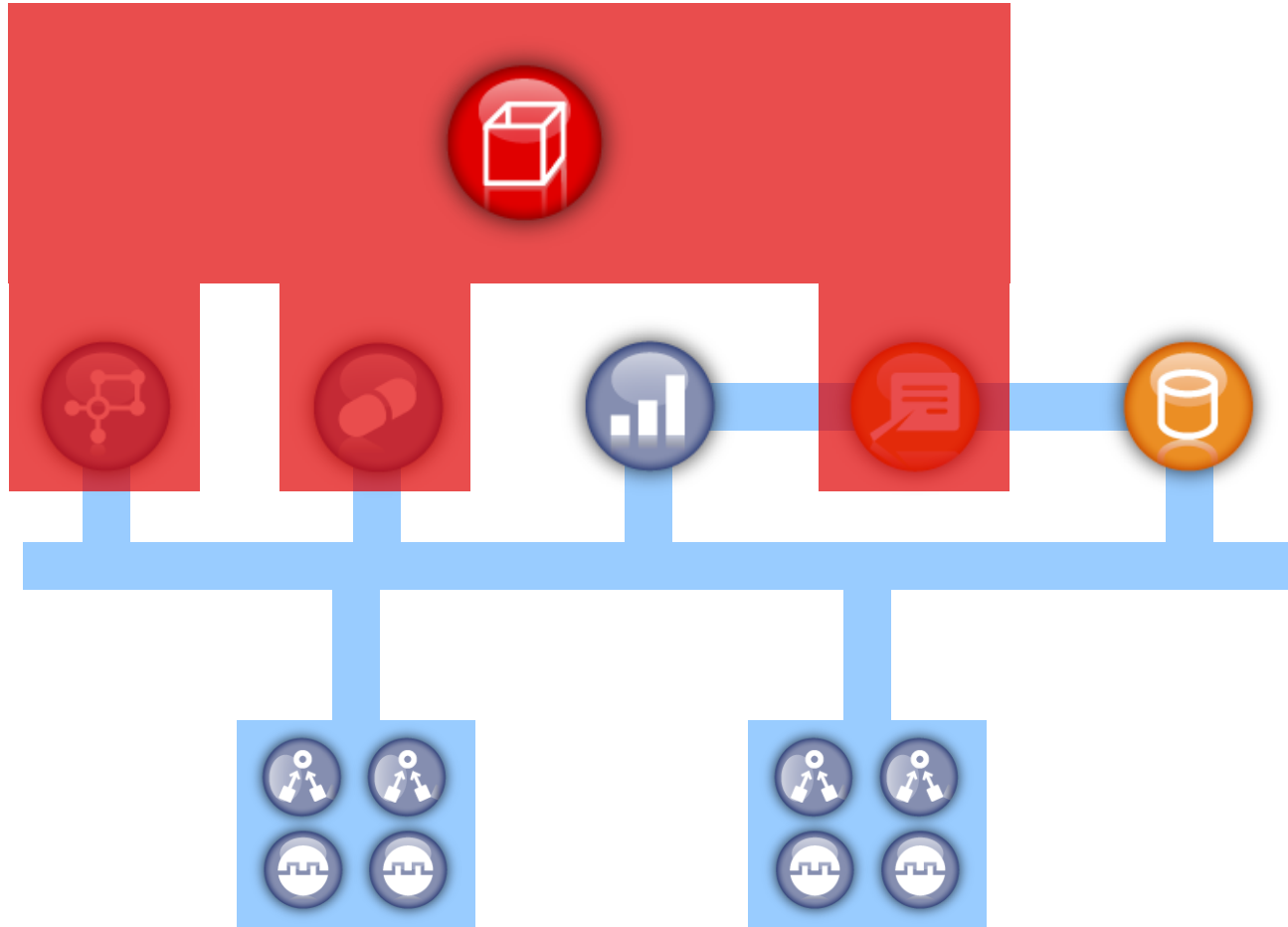
enables rogue administrator work-flows and other identity based processes with Novell Identity Manager - immediately reactive

PCI-DSS Solution Pack

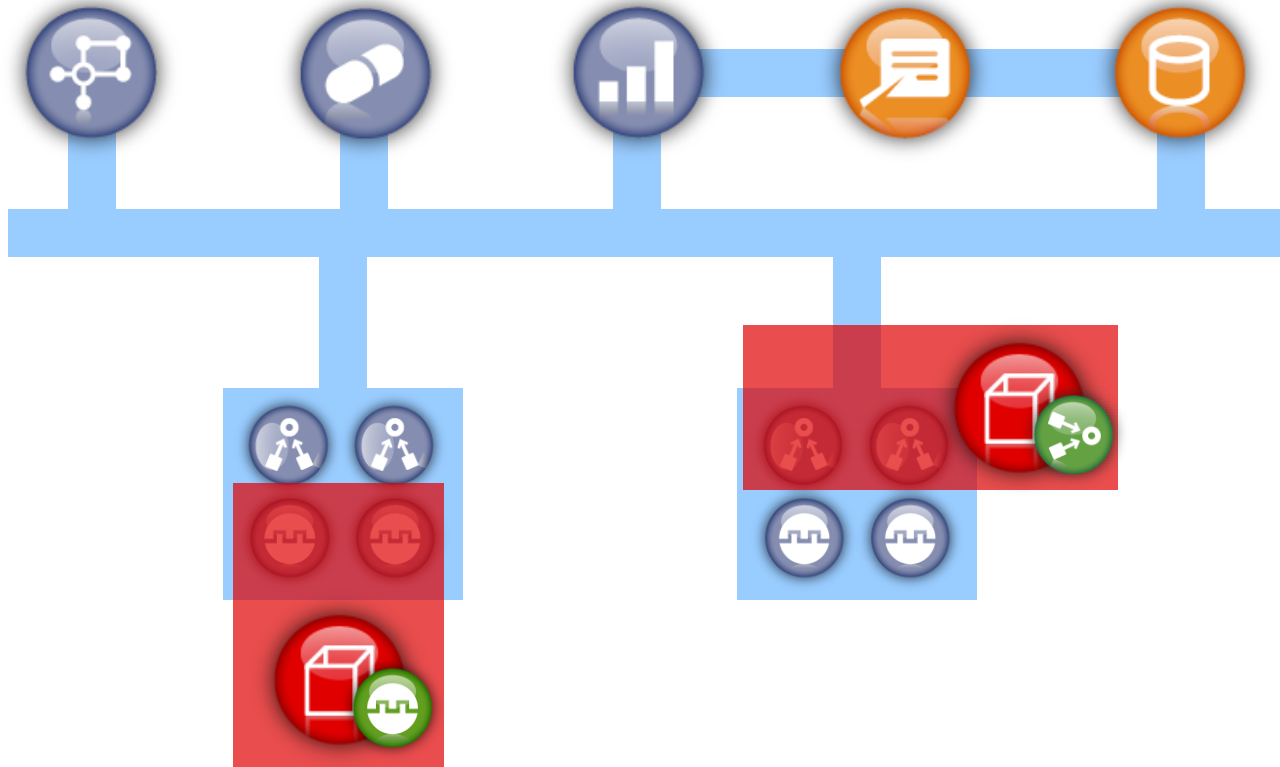
helps the enterprise wide adoption of PCI-DSS compliance controls

Collector and Connector packs are really just specialized Solution Packs

Solution Packs



Solution Packs - special editions



Sentinel Log Manager 1.0

The bottom of the slide features a series of horizontal lines in white and light blue, creating a decorative footer element.

SIEM или LM - различията

Sentinel 6.1 е Event Management system

и обработва събитията в реално време (real-time event management)

корелациите и отработката на инцидентите се отработват преди събитието да постъпи в базата данни

Sentinel Log Management, като алтернативно решение е организиран да:

- събира и записва в базата parsed and normalized logs и/или unknown logs
- постига производителност (event rates) по-висока от Sentinel
- значително по-опростен за конфигуриране и експлоатация

SIEM или LM - различията

Sentinel Log Management е разработен с цел анализи и вземане на решения “при необходимост”

- позволява филтриране и запазване само на целево необходима информация
- има изчерпателно развити възможности за анализи и репортинг, вкл. възможности за кustomизация според нуждите/особеностите
- гарантира оригиналния произход на информацията (digital signatures on event records)
- автоматизирано разпознаване на типа на източника (automatic device type recognition)
- обработва както parsed and standartized така и unknown лог-ове

Общото в технологиите им

Sentinel Log Management използва конекторите и колекторите създадени за Sentinel 6.1

Sentinel Log Management също така обработва входящите лог-ове (parses incoming log records) по същия начин както Sentinel

..... в резултат на което организациите които се нуждаят едновременно и от двете могат да ги интегрират

Интеграцията

Sentinel Log Management supports the new Sentinel Link feature

this allows Sentinel Log Management to act as a filtering forwarder for Sentinel

useful if you have requirements for storing logs for audit purposes

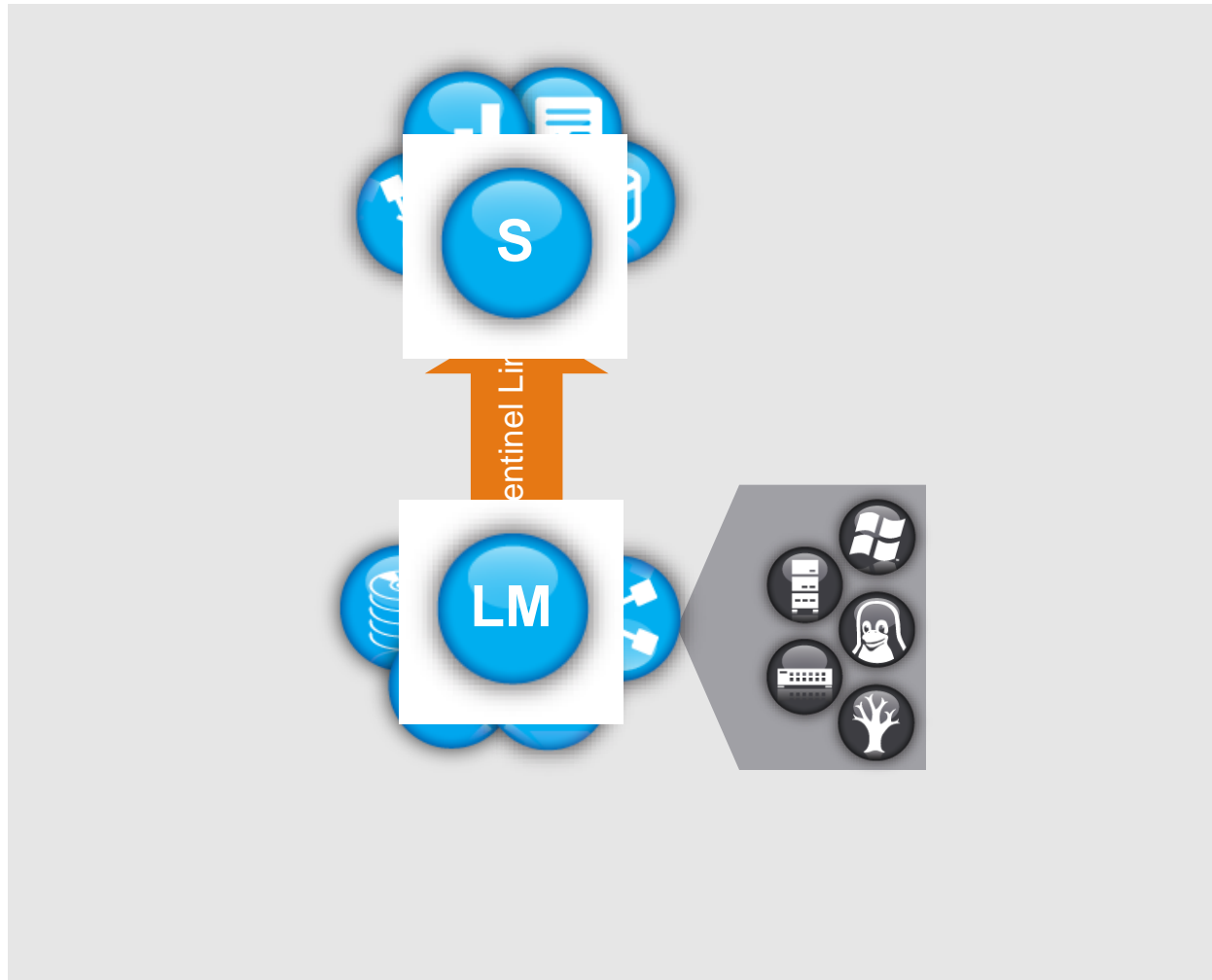
but only some of those events are important from a security perspective

multi-tier installations

full logs stored near the sources

response and remediation is centralized

Mixed Scenario



Questions & Answers

The bottom of the slide features a series of horizontal lines. There are two thin white lines, followed by a thicker light blue line, and another thin white line, all set against the blue background.

Novell®

Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. Novell, Inc. makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for Novell products remains at the sole discretion of Novell. Further, Novell, Inc. reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

