Эволюция SIEM

Artyom Medvedev
HP Enterprise Security
Russia&CIS
artyom.medvedev@hp.com

Agenda

Почему компании до сих пор не защищены?

Решение HP Arcsight

Подход HP?

Ландшафт угроз

Больше угроз + продвинутые злоумышленники = больше атак

Новые технологии

Cloud

SDN

Mobile/BYOD

	Zappos.com	RSA SECURITY	TJX	SONY	Heartland PAYMENT SYSTEMS
Attacks	24 Millions	40 Millions	95 Millions	101 Millions	130 Millions

Киберпреступность

Anonymous

State funded

LulzSec

Новые задачи – новые методы решения

Cloud

SDN

Physical

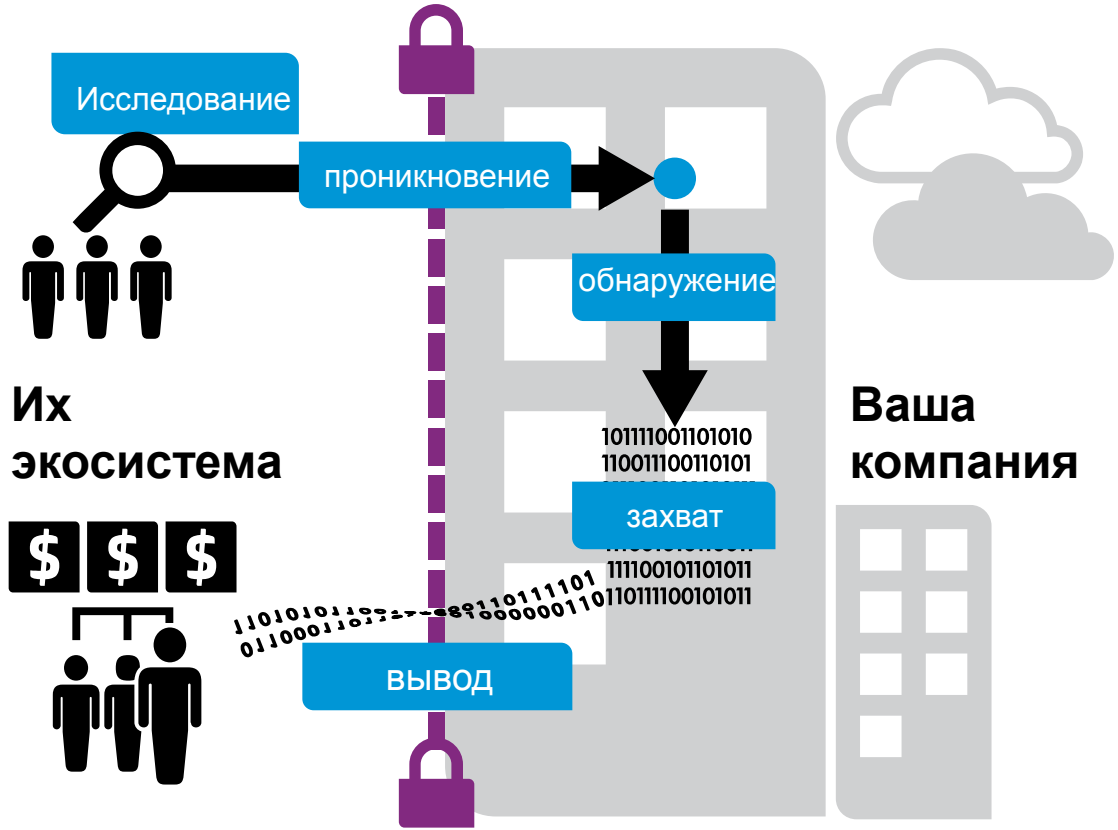
Слишком много данных

Слишком много средств защиты

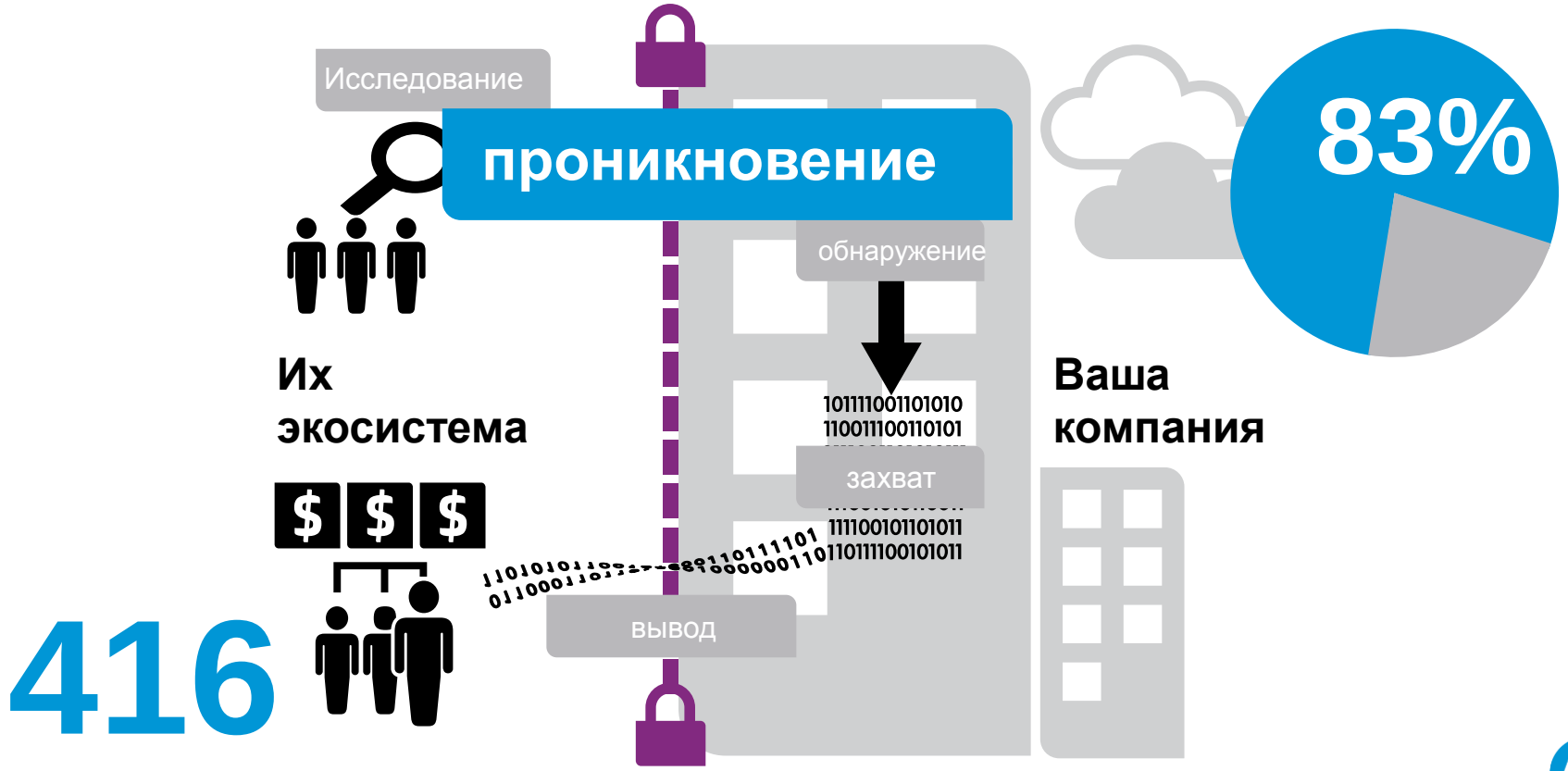
Нет единой аналитики

1000+ Security Vendors

Экосистема злоумышленников



Куда вкладывать ресурсы?



Agenda

Почему компании до сих пор не защищены?

Решение HP Arcsight

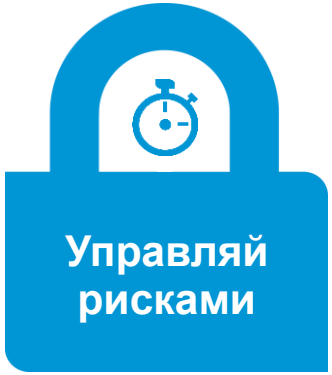
Подход HP

HP ArcSight and HP ESP

Поймать нарушителей, управлять рисками, расширить возможности

- Выявляет внутренних и внешних нарушителей
- Обнаруживает угрозы в реальном времени
- Репутационные базы

Security



- Быстрая реакция на инциденты ИБ
- Улучшает управление рисками
- Знание локальных и глобальных законодательных актов и требований

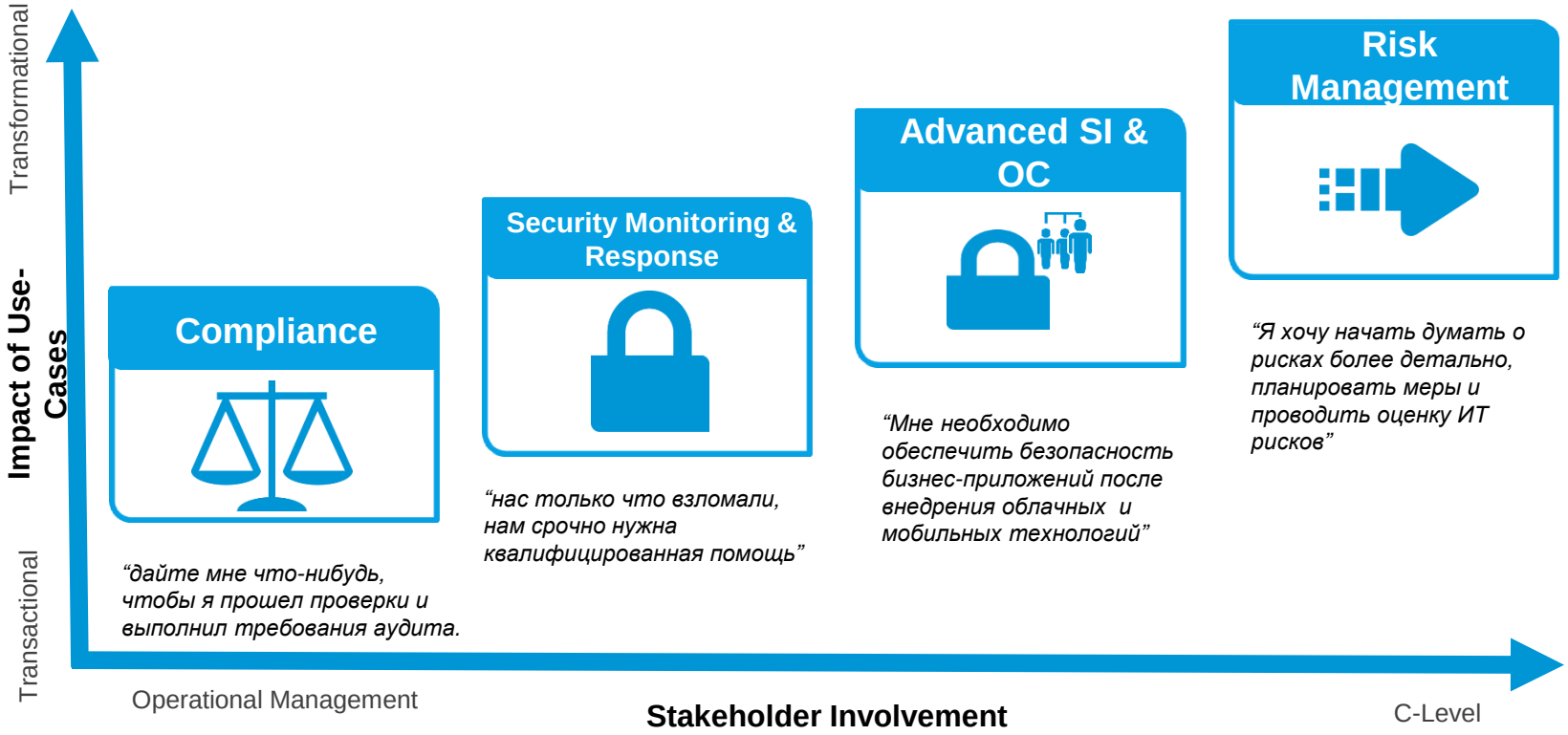
Risk & Compliance

- Меньше затраты и сложность
- Опыт более 5000 сотрудников HP в области ИБ
- От оценки защищенности до аутсорсинга всей инфраструктуры ИБ

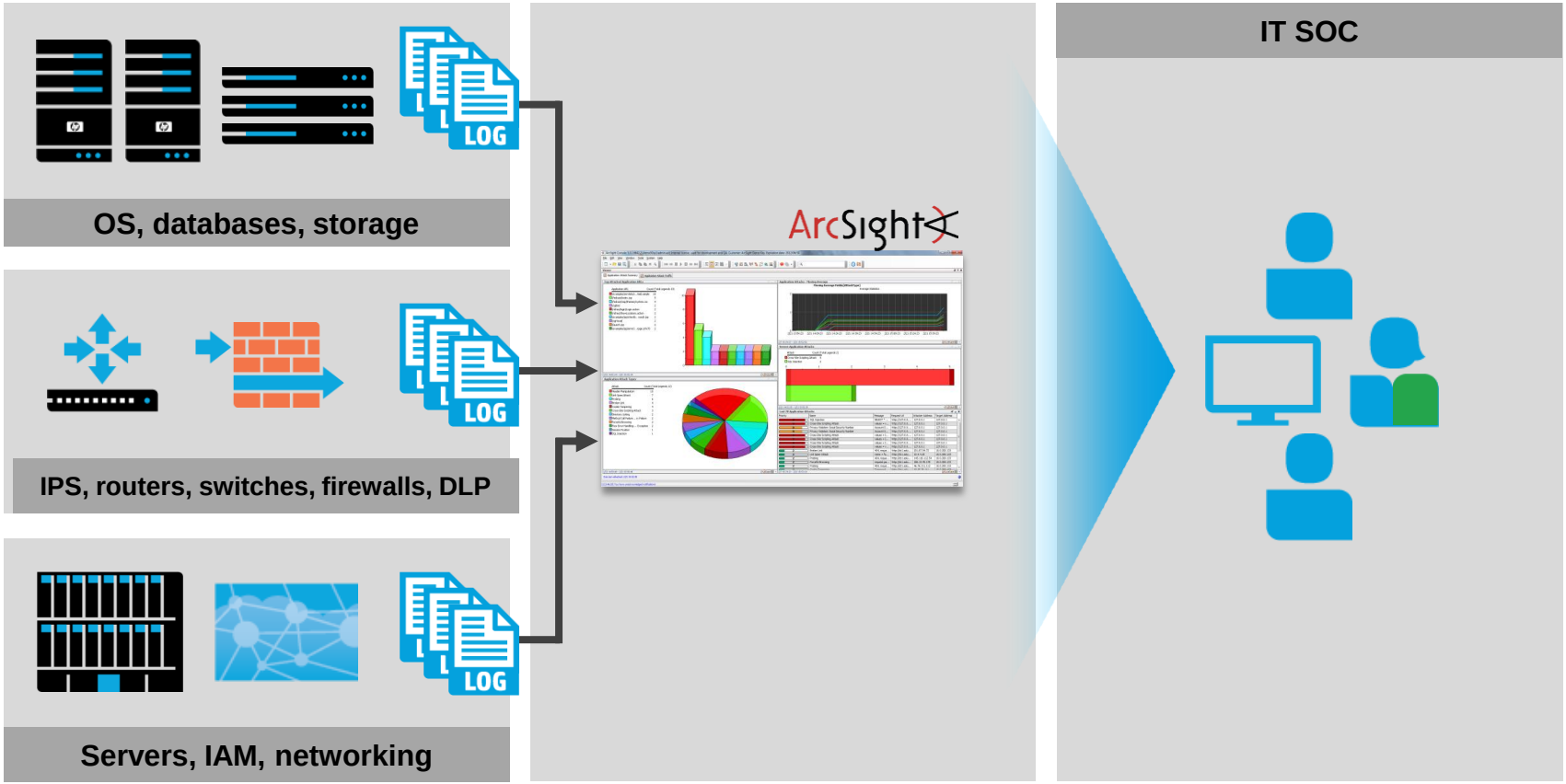
SOC Services

HP ArcSight Use Cases

мы можем покрыть любой спектр задач



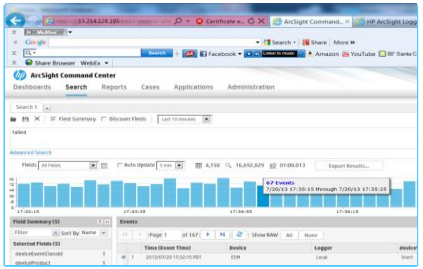
HP ArcSight: Сбор, Обнаружение, Реакция



HP ArcSight ESM 6.5

Новая версия SIEM с встроенным контекстным поиском в 30 раз быстрее с CORRe

Search



- Поиск в ESM как в Logger
- Быстрое расследование
- Текстовый поиск как в Logger

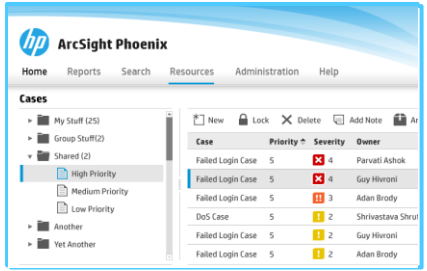
Log Management

hadoop

Integration

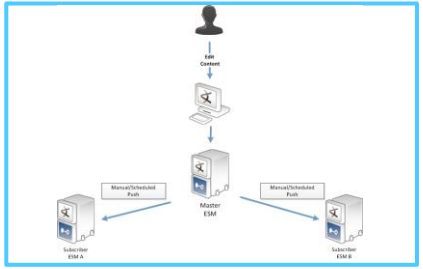
- Эффективное хранение логов
- Интеграция с open source
- 5oe поколение CORRe – в30х раз быстрее

Web 2.0 interface



- Упрощенная веб-консоль
- Поиск, отчетность, администрирование и оценка рисков из одной консоли

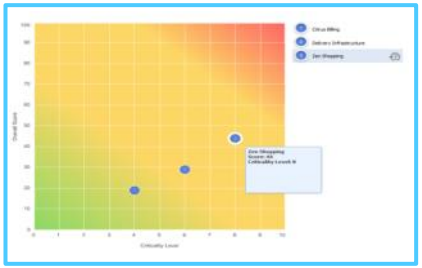
Content Sync



- Централизованное управление настройками и правилами
- Импор и экспорт контента
- Контент для контроля приложений AppView

HP ArcSight Risk Insight

Карта рисков



- Настраиваемая приоритезация
- Карта рисков дя бизнес-сервисов
- Управление рисками через скоринг

Схема активов

- Дополнительные бизнес уровни для модели активов
- Интеграция с uCMDB
- Контроль уязвимостей и анализ их влияния на риски

Текущие риски

- Агрегация нескольких источников рисков
- Оповещения о возникших рисках
- Отслеживание трендов и отчетность при изменении

Контроль соответствия

- Контроль соответствия всем типам требований регуляторов и законодательных актов

HP ArcSight Application View

Прозрачность активности приложений

Выборочное логирование

Доступы пользователей

Отслеживание источника

Ошибки приложения

Функции

- Полная прозрачность активности любых .NET и Java приложений
- Контроль авторизации пользователей и доступа к данным
- Использование корреляционных правил для определения мощеннических действий пользователей приложений

Задача решена

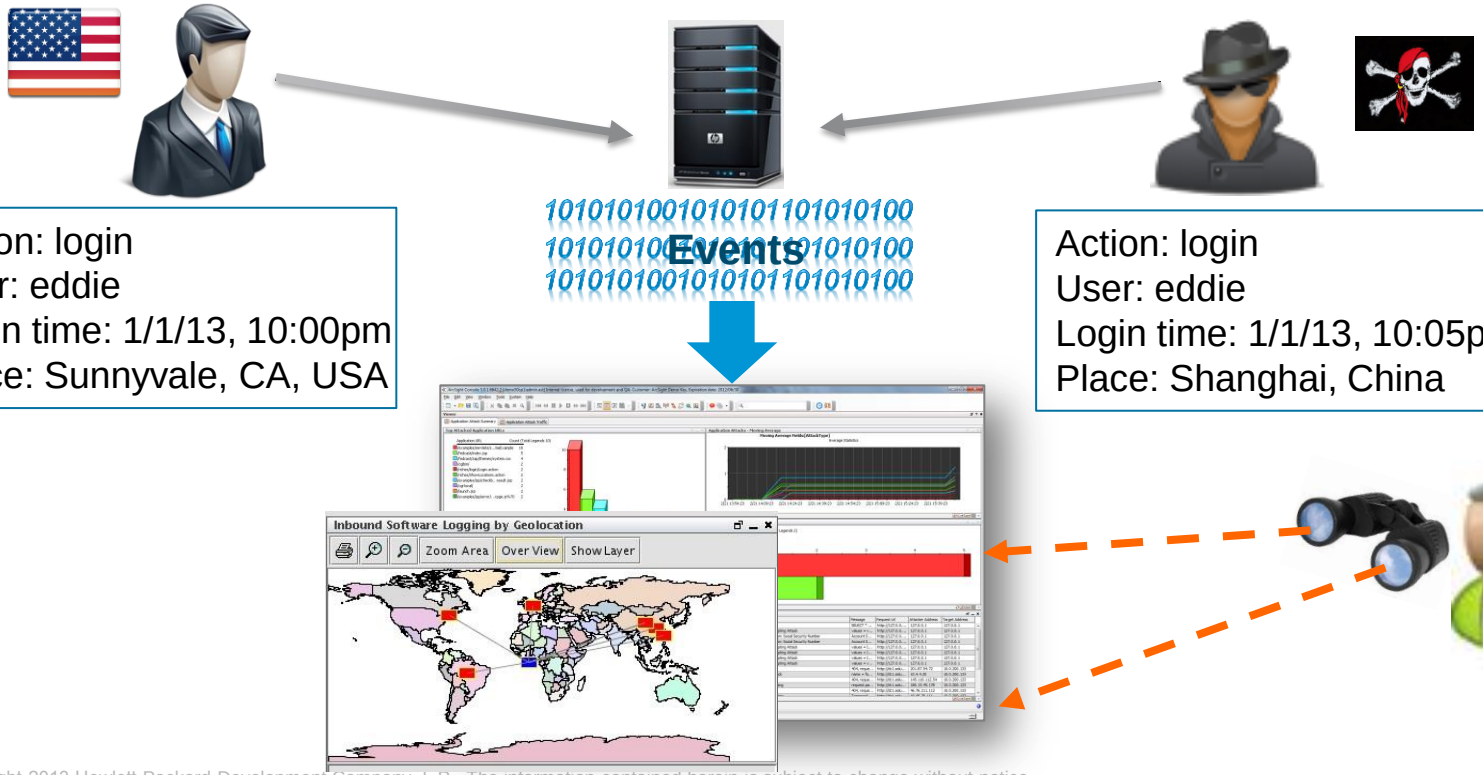
AppView помогает коррелировать действия пользователя с активностью приложения для определения и анализа мошеннических действий

Преимущества для клиентов

- Анализ событий приложения помогает определить кто из пользователей пытался получить доступ к данным
- Журналирование действий в любых приложениях
- Расследование атак на уровне приложения

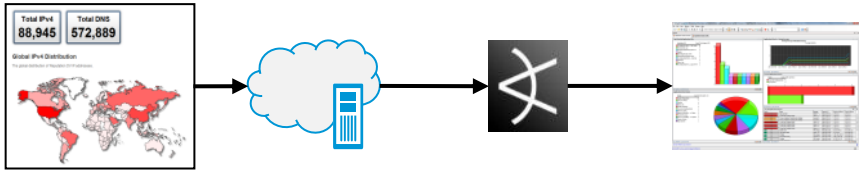
HP ArcSight Application View

Пример сценария: Geo-location



Reputation Security Monitor (RepSM)

Новый репутационный движок



HP DVlabs reputation research | HP RepSM web service | HP RepSM Model Import Connector | HP RepSM content for ESM

Функции

- Выявление угроз на ранних этапах, и приоритизация операций по устранению угроз на основе результатов их анализа
- Учет уникального опыта каждого клиента
- Анализ угроз в peer-to-peer сетях, выявление фишинга
- Интеграция с HP ThreatDetector и HP TippingPoint IPS для выявления 0-day атак и паттернов, с дальнейшей возможностью блокировки

Зачем это нужно?

RepSM сочетает анализ угроз на основе репутации с корреляционными возможностями SIEM в режиме реального времени. Позволяет выявлять, анализировать, приоритезировать и реагировать на современные угрозы.

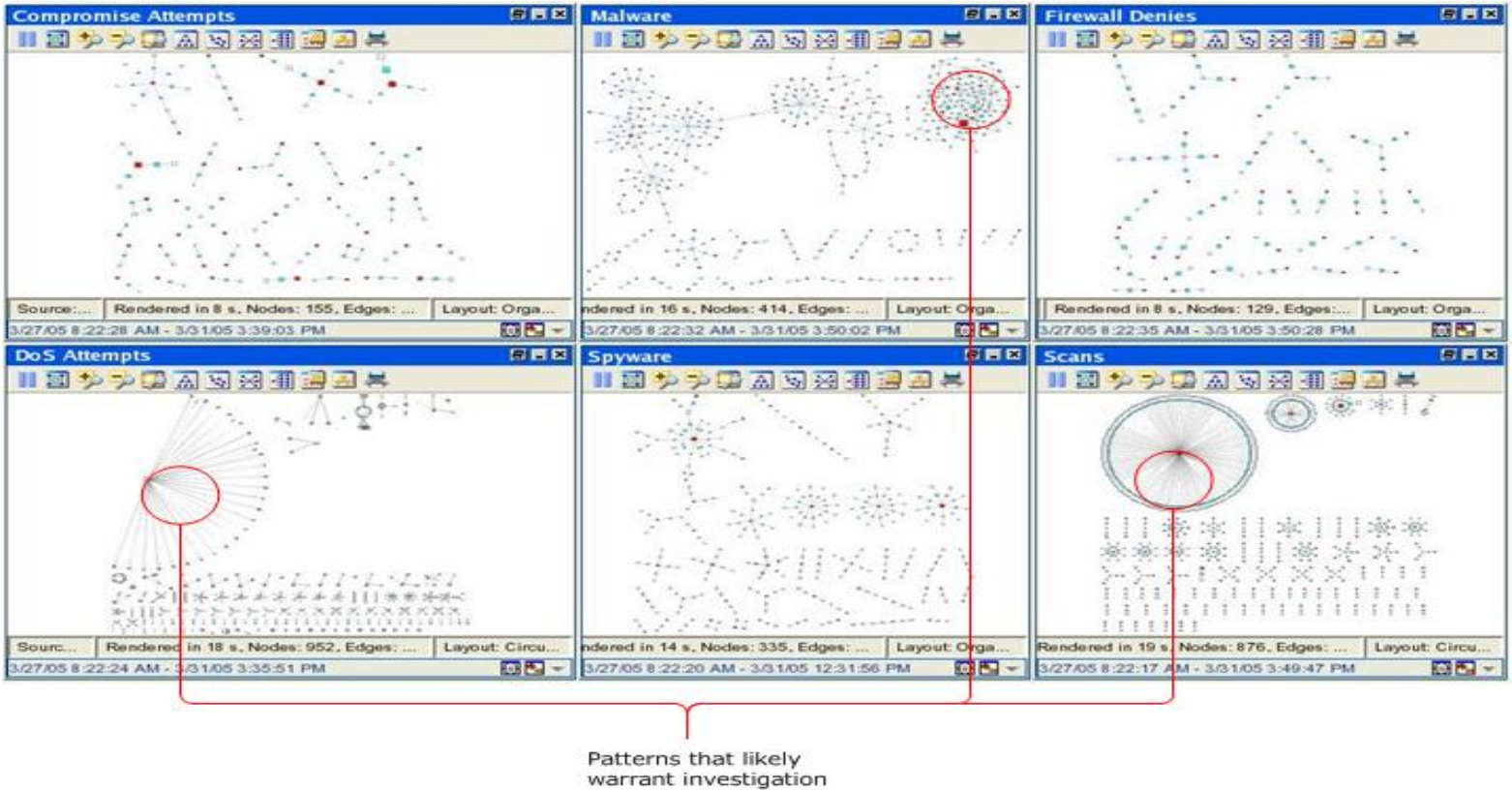
Преимущества

- Предотвращает распространение угроз
- Блокирует вывод важных данных
- Улучшает эффективность управления инцидентами

Почему HP?

- Репутационные базы от HP DVLabs
- Может обнаружить больше уязвимостей, чем 6 ближайших конкурентов вместе взятых

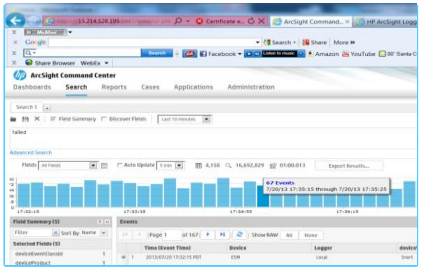
Обнаружение хакеров с помощью поведенческого анализа



HP ArcSight Management Center

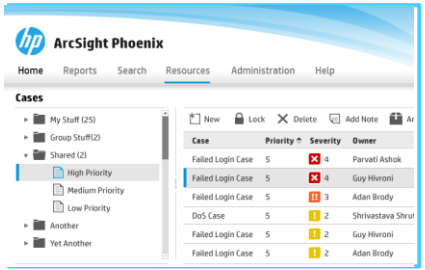
Универсальная консоль для настройки, внедрения и управления Arcsight

Централизация



- Единая консоль для управления безопасностью
- Логгер и конекторы из одного окна для удобства анализа

Масштабируемость



- Управление большими внедрениями
- Добавление новых компонент через единую консоль

Управление изменениями

- Контроль изменений конфигураций
- Удаленное обновление ПО

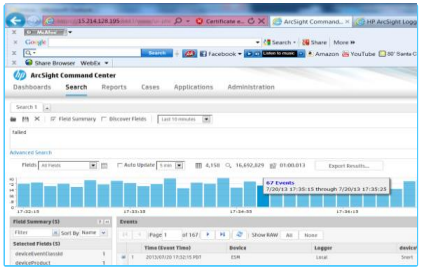
Меньше источников

- Фокус на соыбтиях и угрозах, не на продукте
- Требуется меньше времени операторов для анализа угроз

HP ArcSight Log Management Solution (Logger)

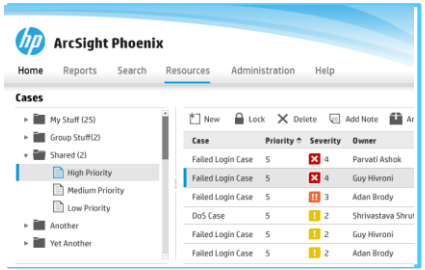
Унифицированная консоль для управления журналами событий

ArcMC



- Единая консоль для управления безопасностью
- Логгер и конекторы из одного окна для удобства анализа

Cloud Connector



- Собирает логи из облаков
- Собирает журналы из любых облачных приложений с помощью FlexConnector
- Box, Google, Salesforce, other SaaS providers

Hadoop

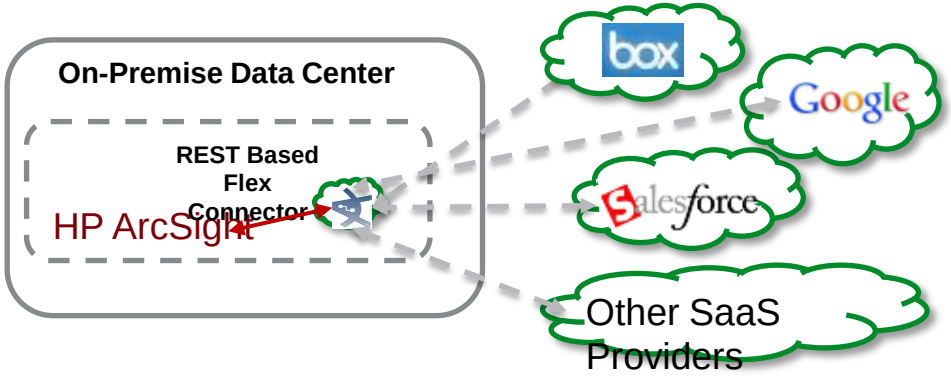
- Хранение всех логов длительное время
- Интеграция со средствами работы и анализа структурированных и неструктурированных данных огромных объёмов (Big Data)

Hyper-V &

- Теперь Логгер работает с Hyper-V и VMware ESX

Мониторинг облаков

ArcSight – индустриальный стандарт в области мониторинга SaaS



Функции

- Безопасный сбор событий от облачных приложений
- Использует стандартные протоколы – OAuth, REST, JSON
- Референсные заказчики - Google, Box and Salesforce
- Легко добавлять новые облачные приложения
- Поддерживает как онлайн, так и отложенный сбор событий

Преимущества

- Мониторинг угроз и активности пользователей облачных приложений в режиме реального времени
- Расширенные отчеты для облачных приложений
- Единая точка мониторинга событий из собственной инфраструктуры и из облачных приложений

Thank you

Agenda

Build to disrupt the adversary

Why are Companies still not secure?

The HP Arcsight Solution

Why HP?

HP ArcSight …

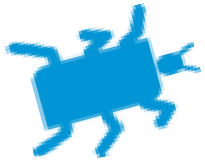
Global Presence

Security Professionals
5,000+

MQ Leader
10 Years

Built
30
SOCs

Devices under Management
90,000+



Vulnerability Intelligence
No. 1

HP Enterprise Security Momentum

HP Security Technology

#1
#2
In all markets we play in

HP Security SaaS

2.5B lines of code under SaaS subscription

HP ESP Customers

10000+ Customers

900+ Managed Security Services

New Products

35 Released in the last 12 months

---

9 out of 10	**9 out of 10**	**10 of 10**	**All Major Branches**
Major banks	Top software companies	Top telecoms	US Department of Defense

Customers of all sizes and industries

Healthcare

Finance

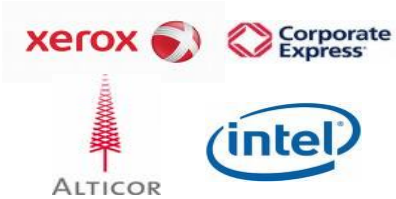
Education

Government

Energy

Telecommunications

Manufacturing



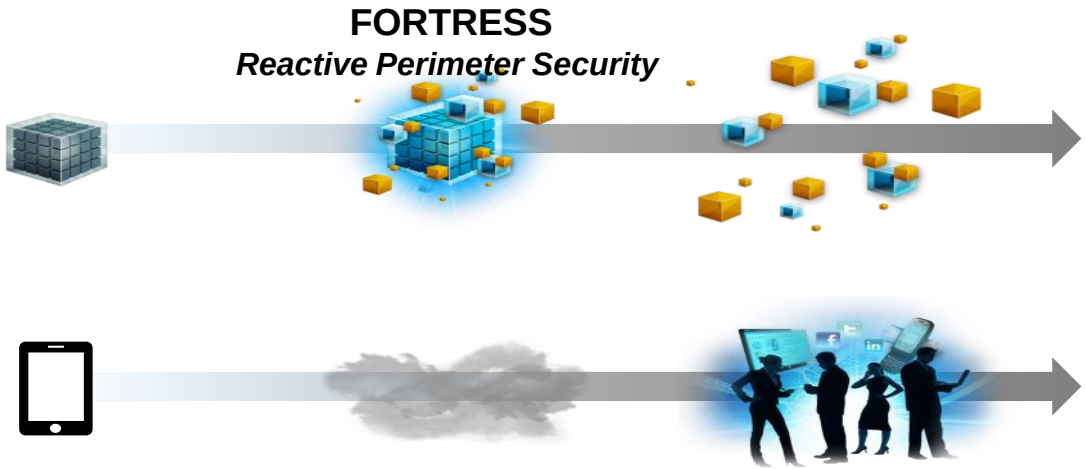
Retail

Appendix

Why security doesn't work today?

COLLABORATIVE
OPEN & EXTENDED

DEVICES,DATA & INFRASTRUCTURE

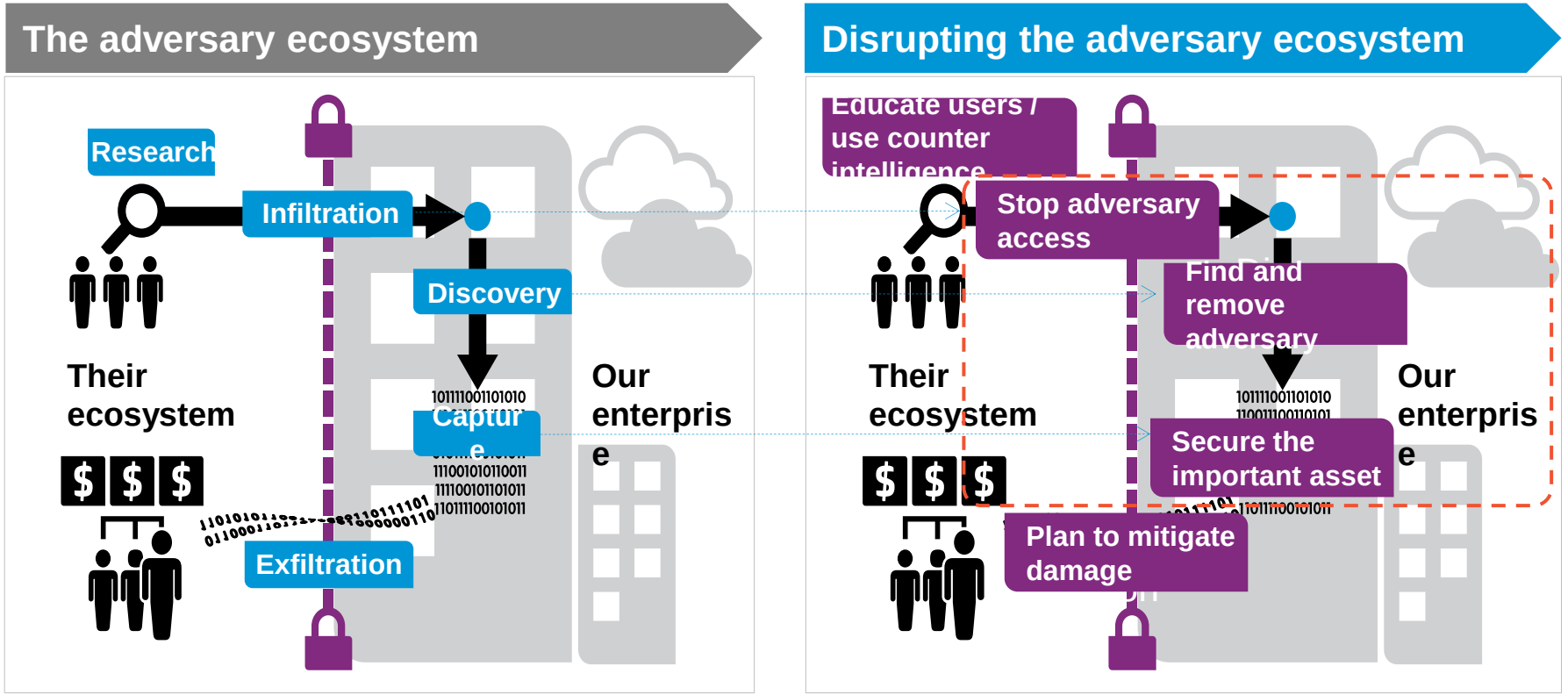


MOBILE
Data Everywhere

CLOUD
Public, Private, Hybrid

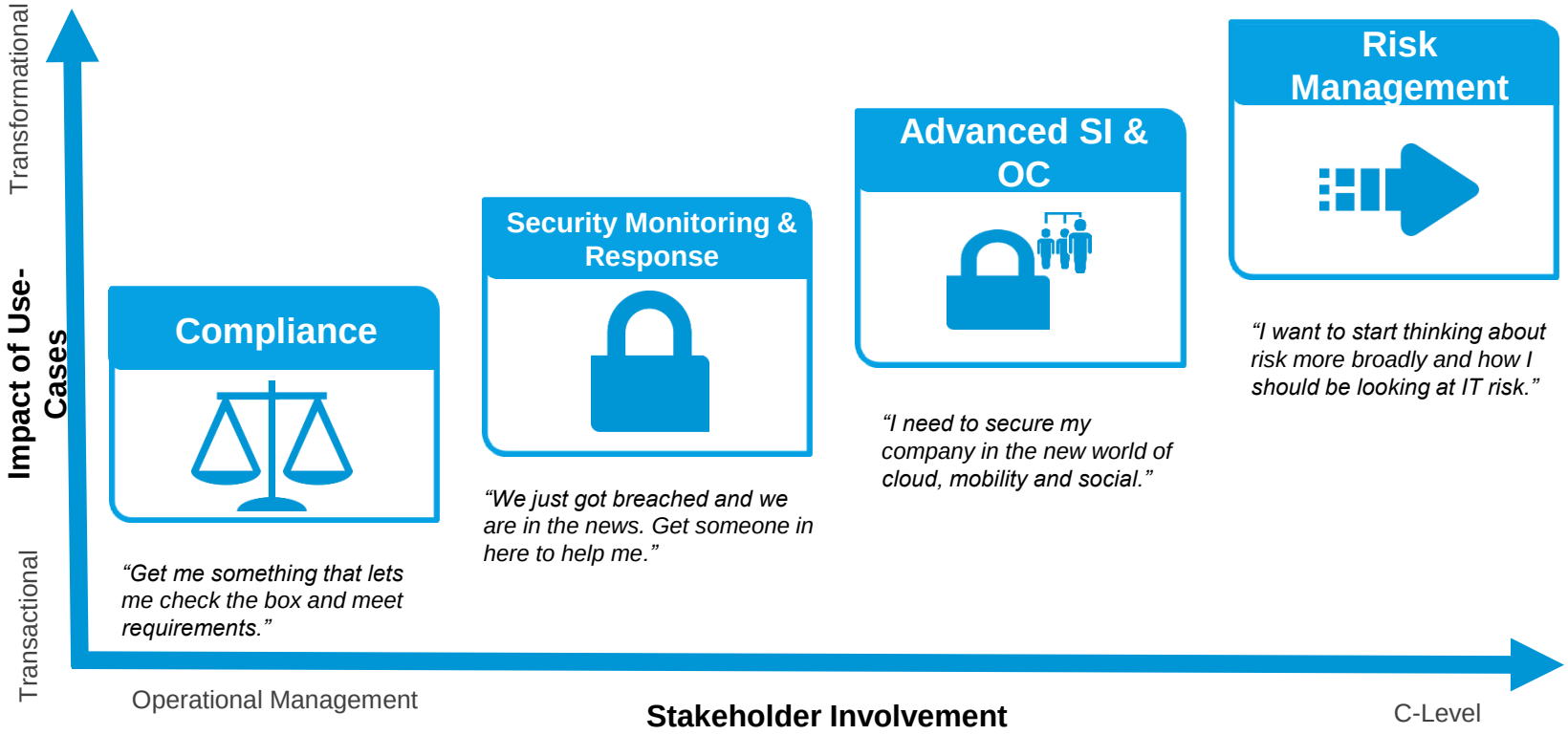
SOCIAL
Mobility, Device Networks

HP ArcSight : What we do

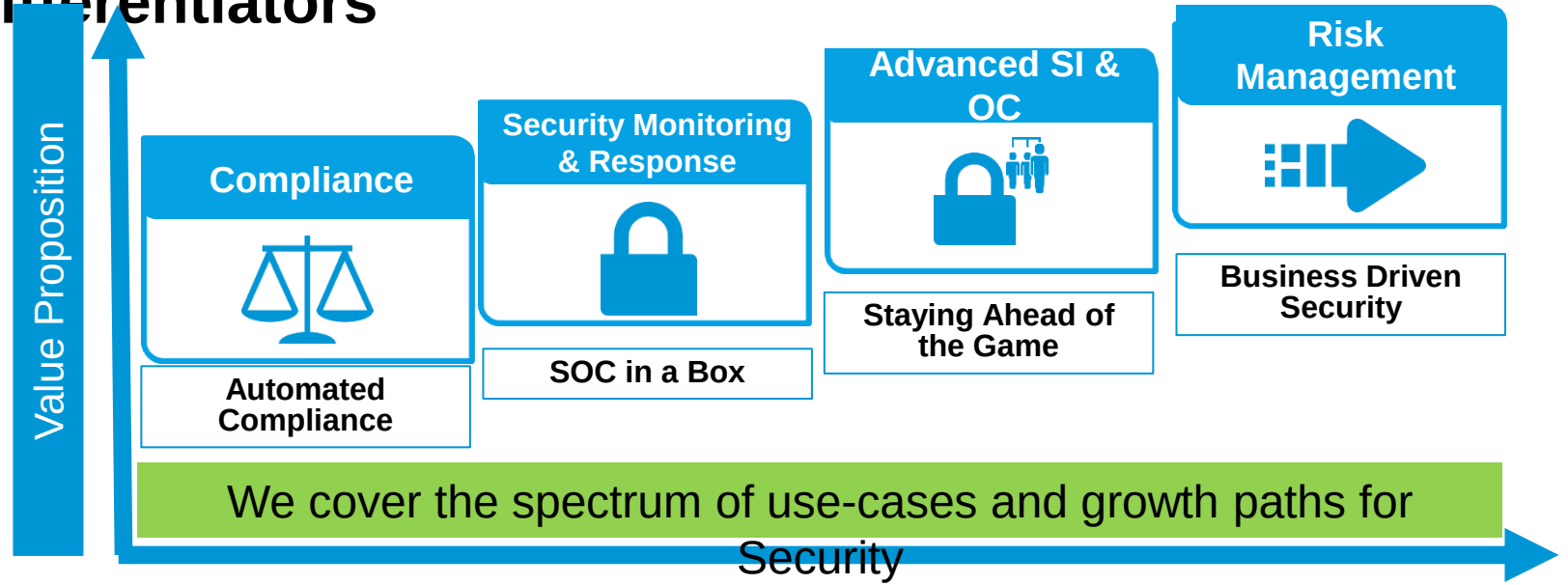


SIEM Maturity Model

We cover the spectrum of use-cases and growth paths for Security

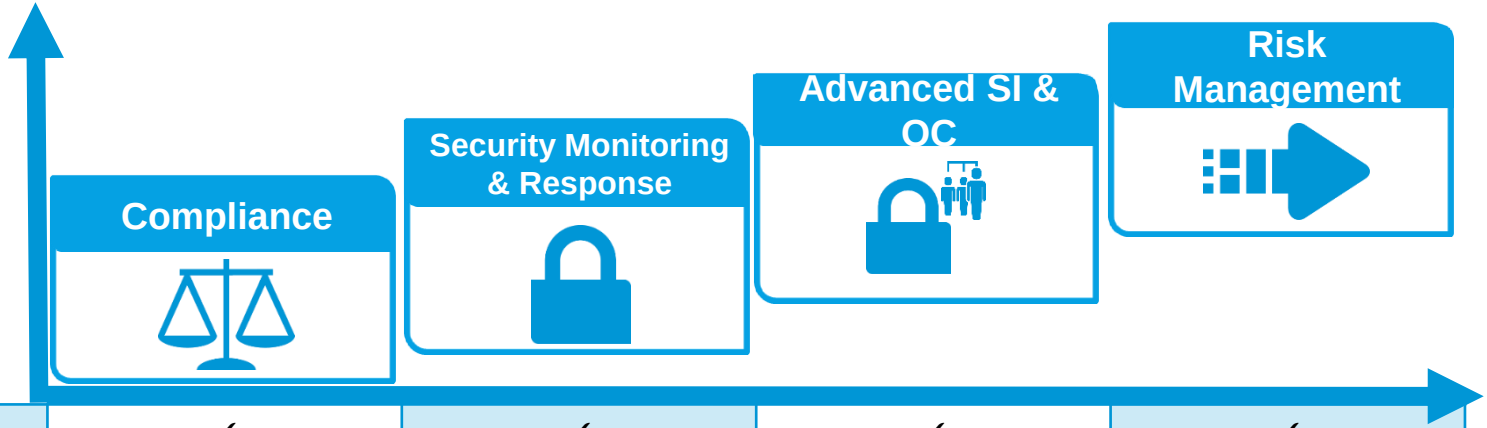


HP ArcSight Solutions - Value Proposition & Differentiators



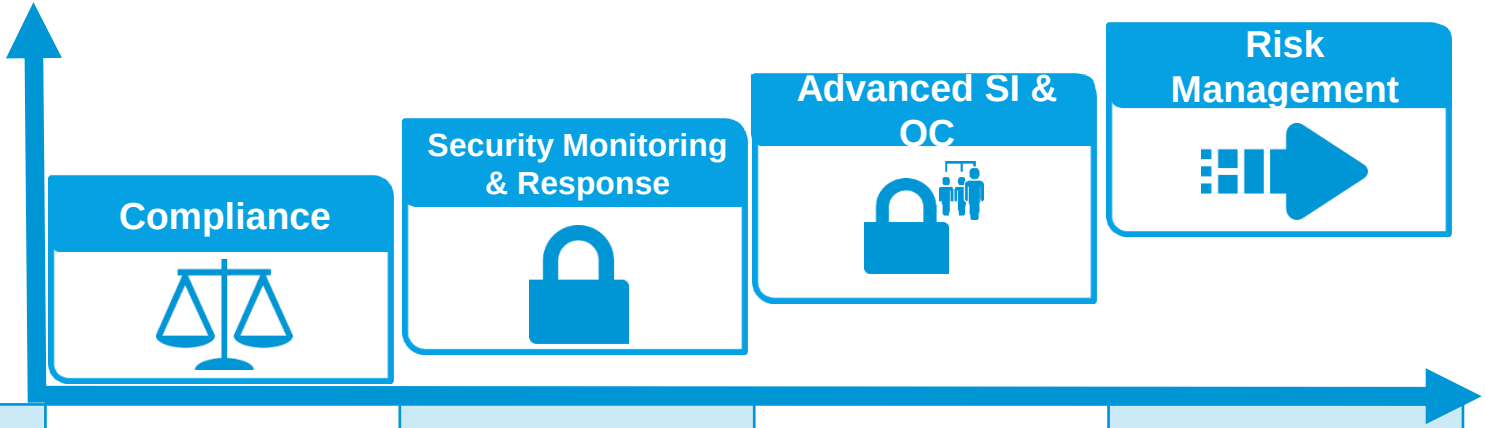
Differentiators			
Built-in Growth Path	Built-in Growth Path	Enterprise Scale Platform	First fully integrated Risk + SIEM
Best Practice	All in one Package	Built 30+ world-class SOCs	Business Centric Visualization
	Rapid Time to Value	HAVEn Architecture	Risk Modelling and What-if Capability

HP ArcSight Solutions – Product Mapping



Logger & CIPs	✓	✓	✓	✓
Express		✓	✓	✓
RepSM & Threat Detector		✓	✓	✓
ESM			✓	✓
Identity & Application View			✓	✓
PS for SI & OC			✓	✓
Enterprise View				✓

HP ArcSight Solutions – Services Mapping



Implementation & Training	✓	✓	✓	✓
Health Check Workshop	✓	✓	✓	✓
Use Case Workshop	✓		✓	✓
SOC Primer		✓	✓	✓
SOC Maturity Assessment			✓	✓
SOC Advisory Services	✓	✓	✓	✓
Content Development	✓		✓	✓
Risk Management				✓

What is CORRE?

The Correlation Optimized Retention and Retrieval - Engine

CORRE is our high-performance storage engine for ESM

Next generation of ArcSight patented data store

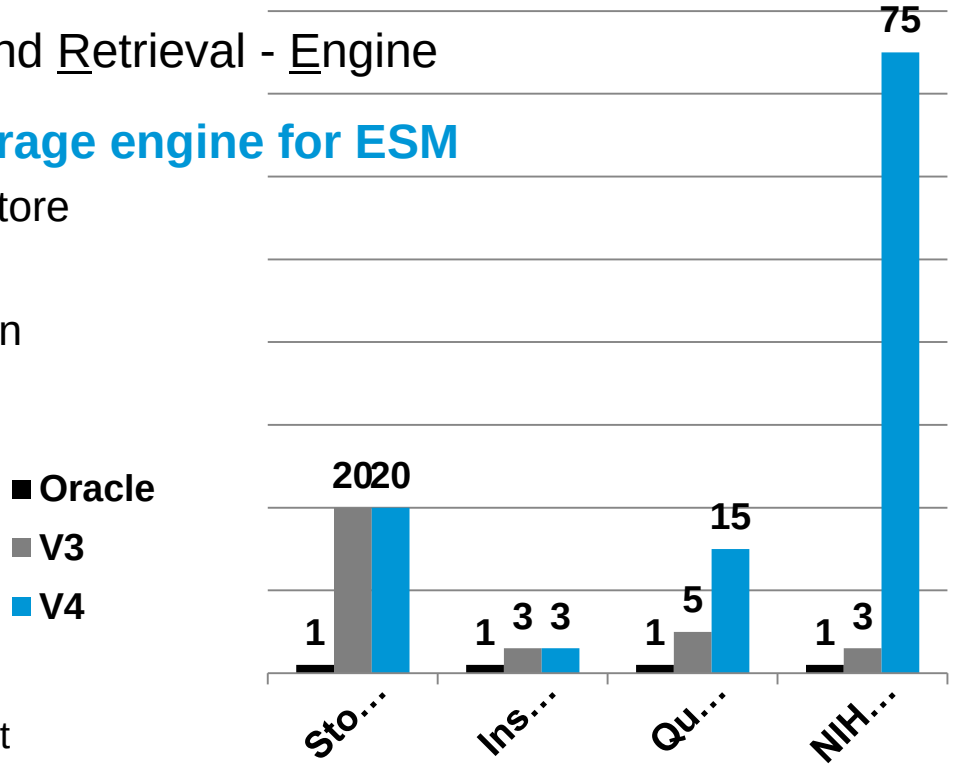
Replaces Oracle

Faster, Simpler and easy Install and maintain

Proven technology in Logger and Express

Optimized for:

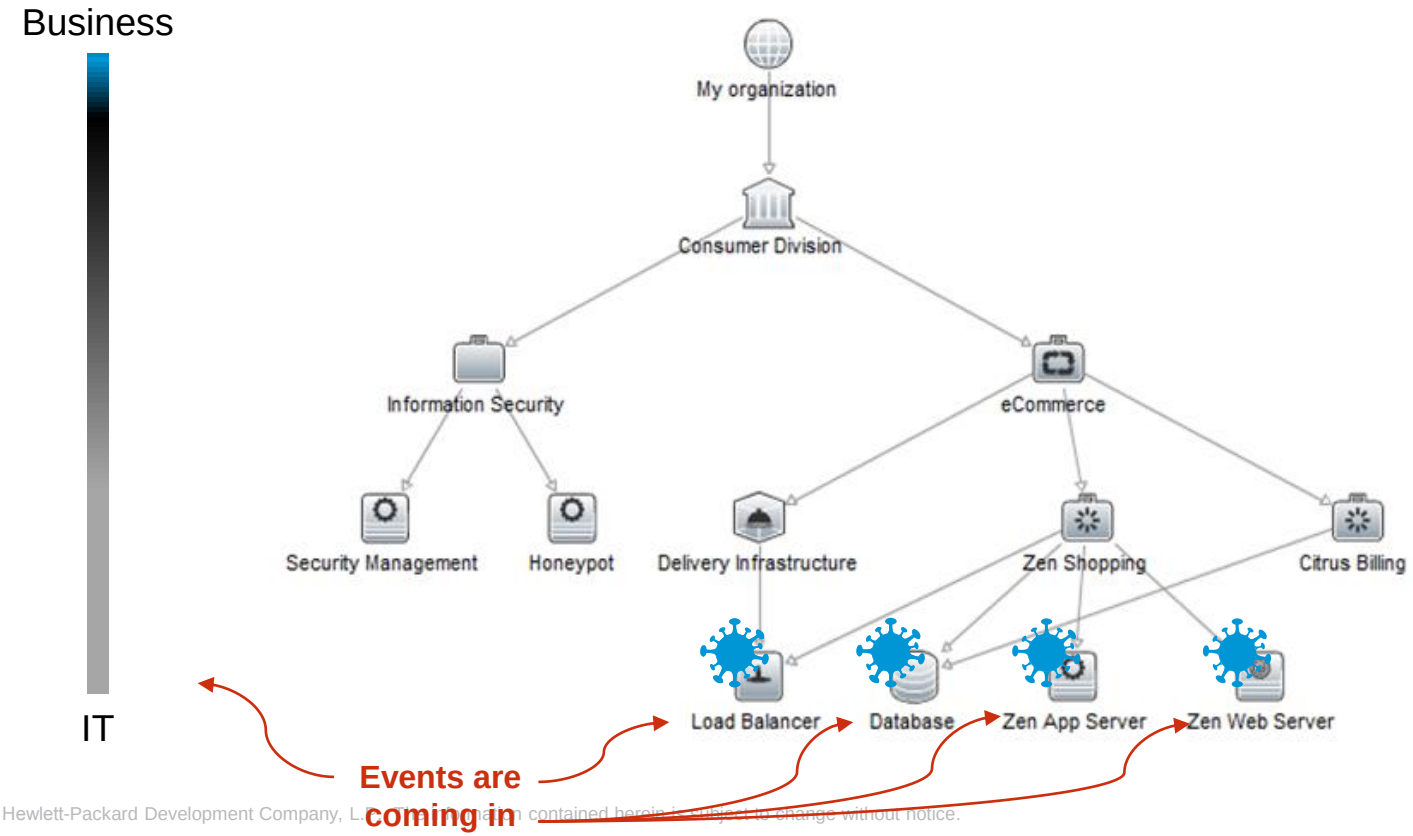
- Faster log insertion rates
- Faster query response times
- Greater storage efficiency
- Better user experience
- Simpler administration and storage management
- Cloud and virtualized deployments preparedness



Risk InSight

What do we now have with Risk Insight? (1)

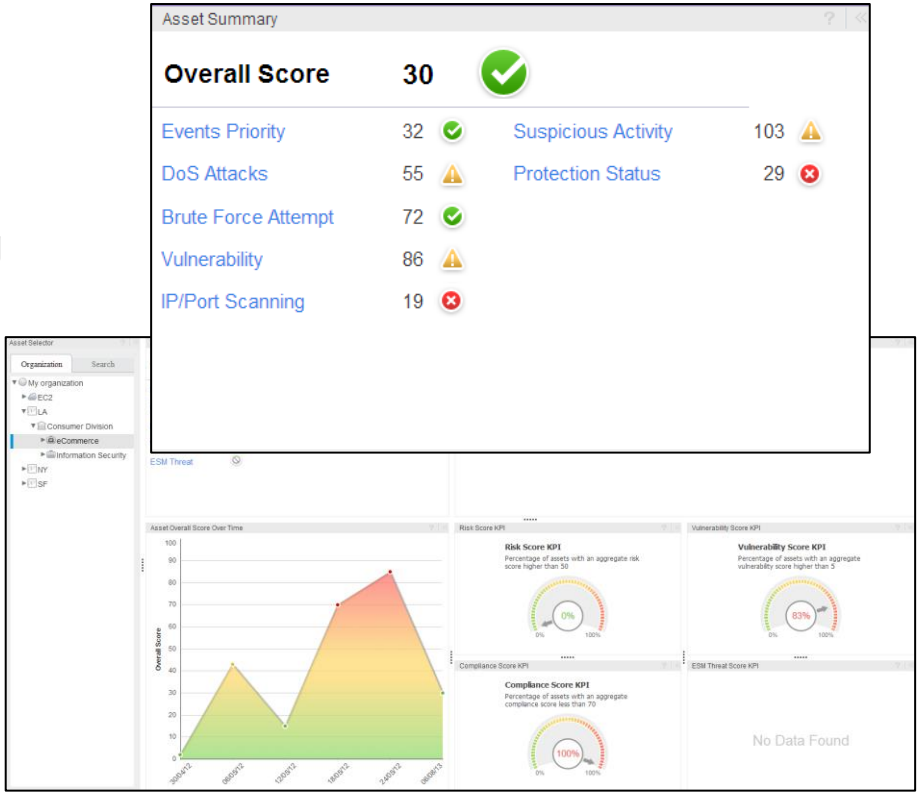
Business Context and aggregation



What do we have now with Risk Insight? (2)

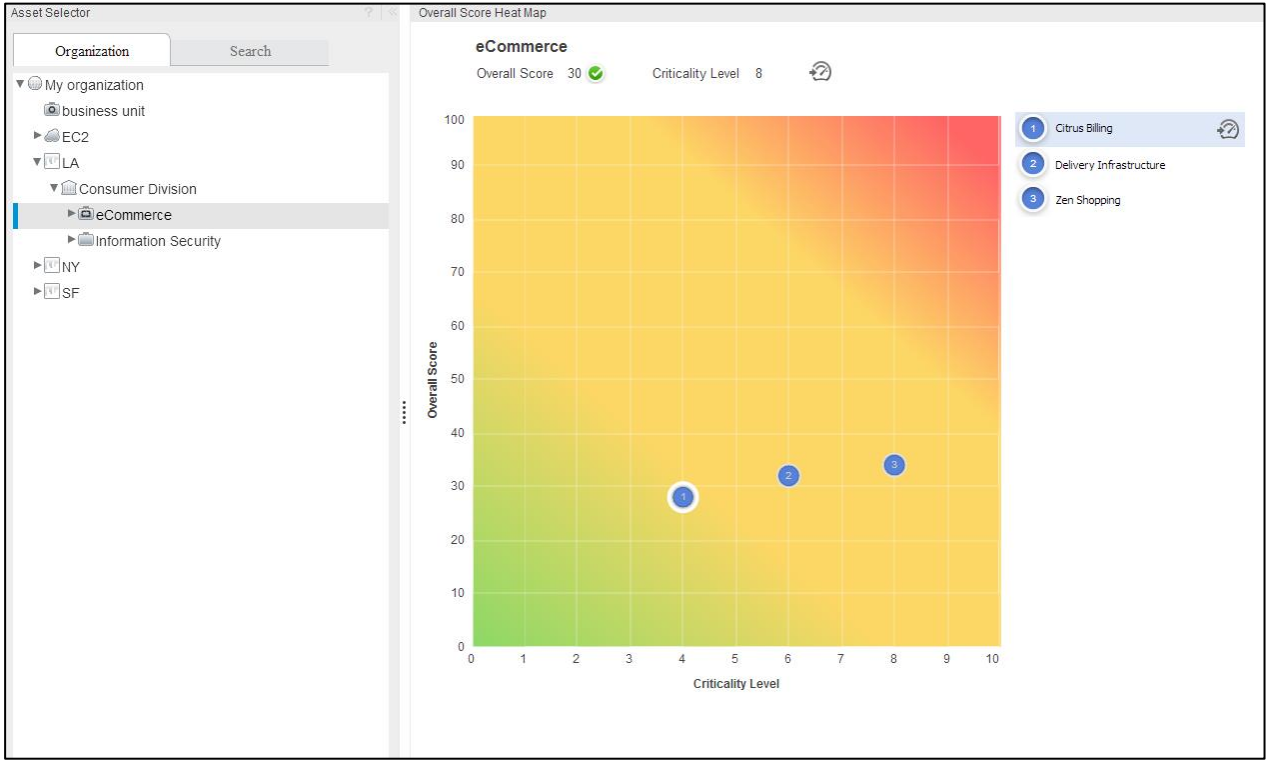
Business focused risk management

- Well defined risk factors to monitor built upon your existing ESM logic representing your overall risk score of an asset
- Long term trends
- Easy to define KPIs, Dashboards and reports

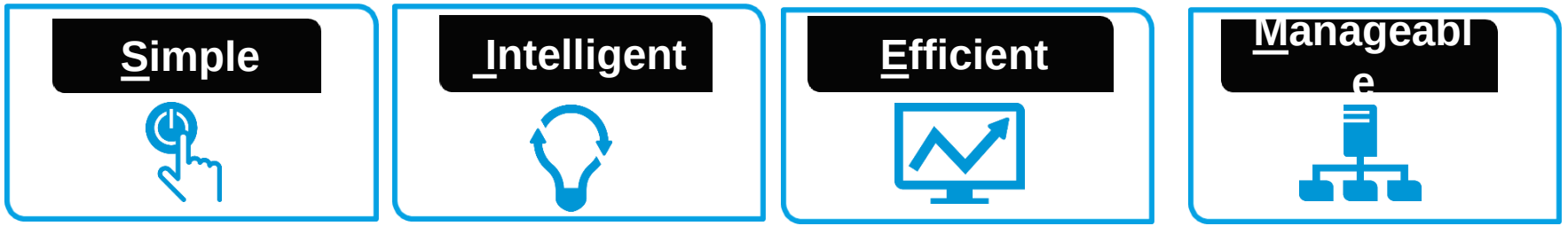


What do we have now with Risk Insight? (3)

Combine to get to a **Prioritized Risk Overview**



HP ArcSight redefines SIEM



Accelerated Time to Value

Simple to deploy, collect, integrate, use and operate. Out of the box content for quick ROI

Real-time Correlation and Analytics

Threat Analysis, Big data and complex event processing

Optimized engine for correlation and storage

Efficient data storage, Optimized retrieval performance

Enterprise scalability

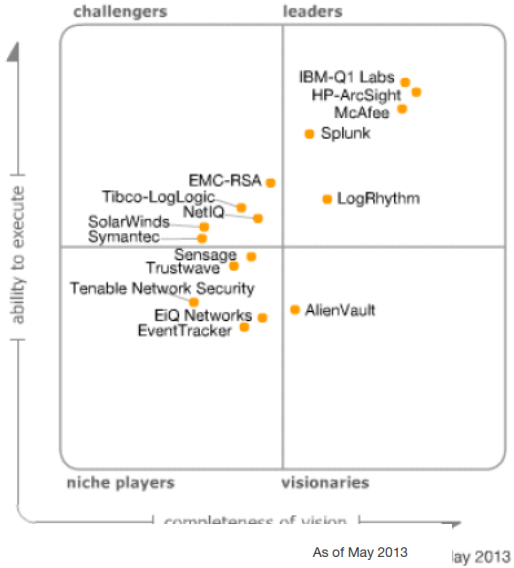
Centralized configuration, content, upgrade, license, user and role management

Gartner SIEM MQ 2013

- HP ArcSight has moved **UP and to the RIGHT**
- A **LEADER for 10 consecutive years,** while others have appeared and disappeared
- The **most visionary product** in the Gartner MQ
- We are **#1 in 4, #2 in 3** of the 8 categories in meeting customer's SIEM requirements

(no other vendor is #1 in more than 2 categories)

- HP ArcSight is the only vendor that is **#1 in all use cases** that matters most to your customers



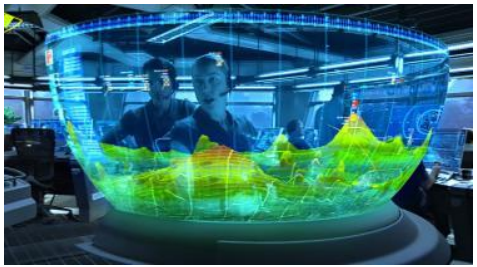
HP/ArcSight

#1	#2

Product Rating	AlienVault	EiQ Networks	EMC-RSA	HP-ArcSight	IBM-Q1 Labs	LogRhythm	McAfee ESM	NetIQ	Sensage	SolarWinds	Splunk	Symantec	Tibco-LogLogic
Real-Time Monitoring	2.80	3.2	2.8	4.1	3.9	3.53	3.55	3.90	2.6	3.03	3.0	3.40	2.85
Threat Intelligence	3.30	3.0	4.0	4.0	4.0	3.00	4.00	1.00	3.5	1.00	3.5	4.70	1.00
Behavior Profiling	3.50	3.3	3.0	3.8	4.5	3.50	3.25	3.50	3.3	2.00	3.3	2.00	3.40
Data and User Monitoring	2.60	3.0	3.2	4.2	3.5	3.58	3.54	3.08	3.6	3.06	3.1	2.92	2.79
Application Monitoring	3.17	3.0	3.3	4.1	3.5	3.58	3.83	2.40	3.7	3.00	3.7	3.08	2.42
Analytics	3.28	2.9	3.5	3.7	3.9	3.00	3.70	2.69	3.7	2.25	3.7	3.00	2.87
Log Management and Reporting	3.04	3.3	2.9	3.8	3.5	3.62	3.68	3.31	3.5	3.29	3.4	3.48	4.00
Deployment and Support Simplicity	3.53	3.2	2.5	3.3	4.0	4.00	3.50	3.80	2.3	5.00	2.9	3.00	3.85

HP ArcSight Value Prop

Situational



Adaptive Security

Keep Data

Predict

Correlate events from apps, network and sentiment analysis to determine where you are most likely to get targeted

Protect

Configure your defenses to secure your most important Assets

Prevent

HP ArcSight prevents your data from being stolen via Real-time event logging and threat response