Корпорация ЮНИ

# Обнаружение атак и угроз. IPS-1

*13 ноября 2007*

Игорь Левен

Директор учебного центра

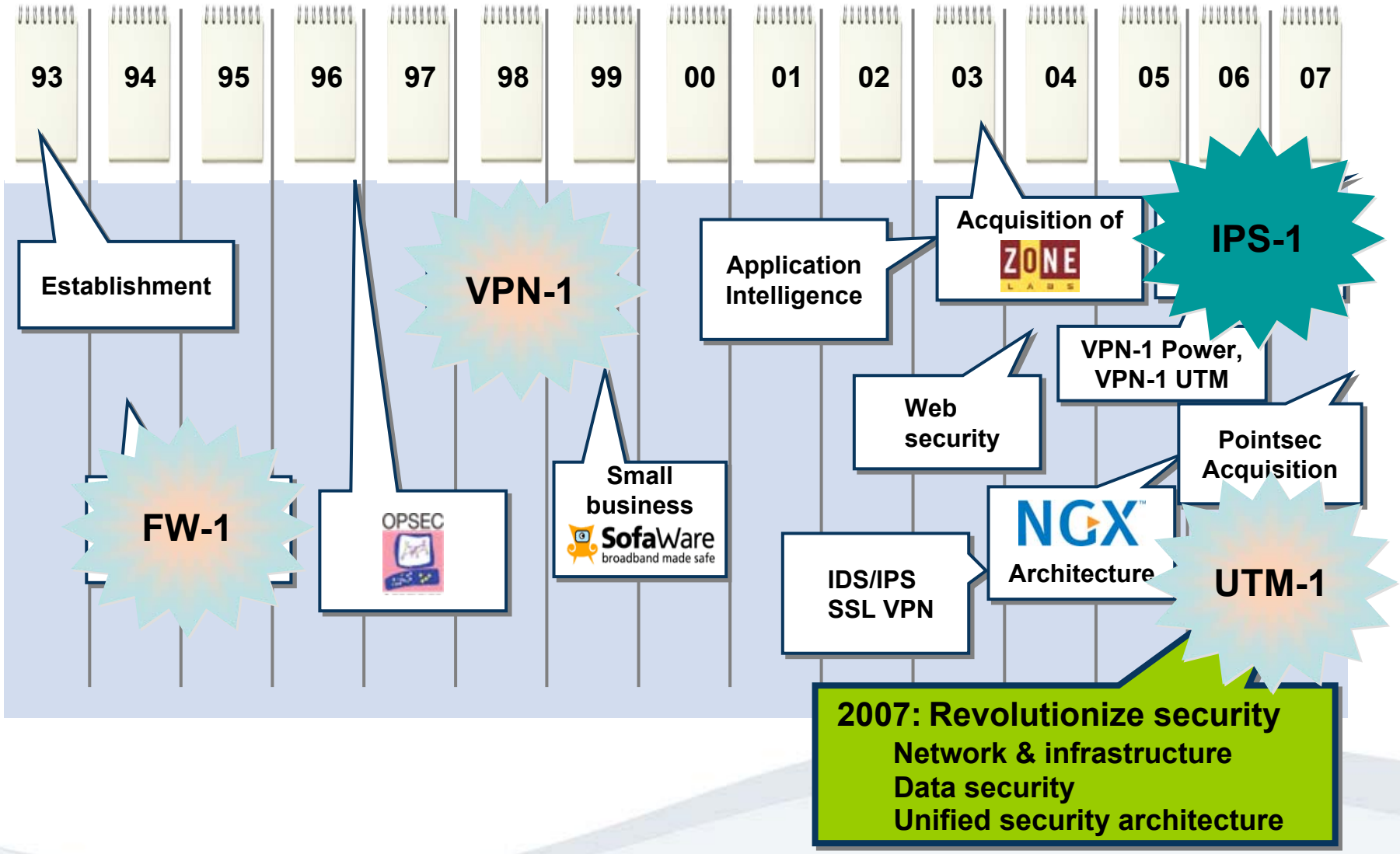
iloewen@ntc.ru

+7 (495) 580 9902

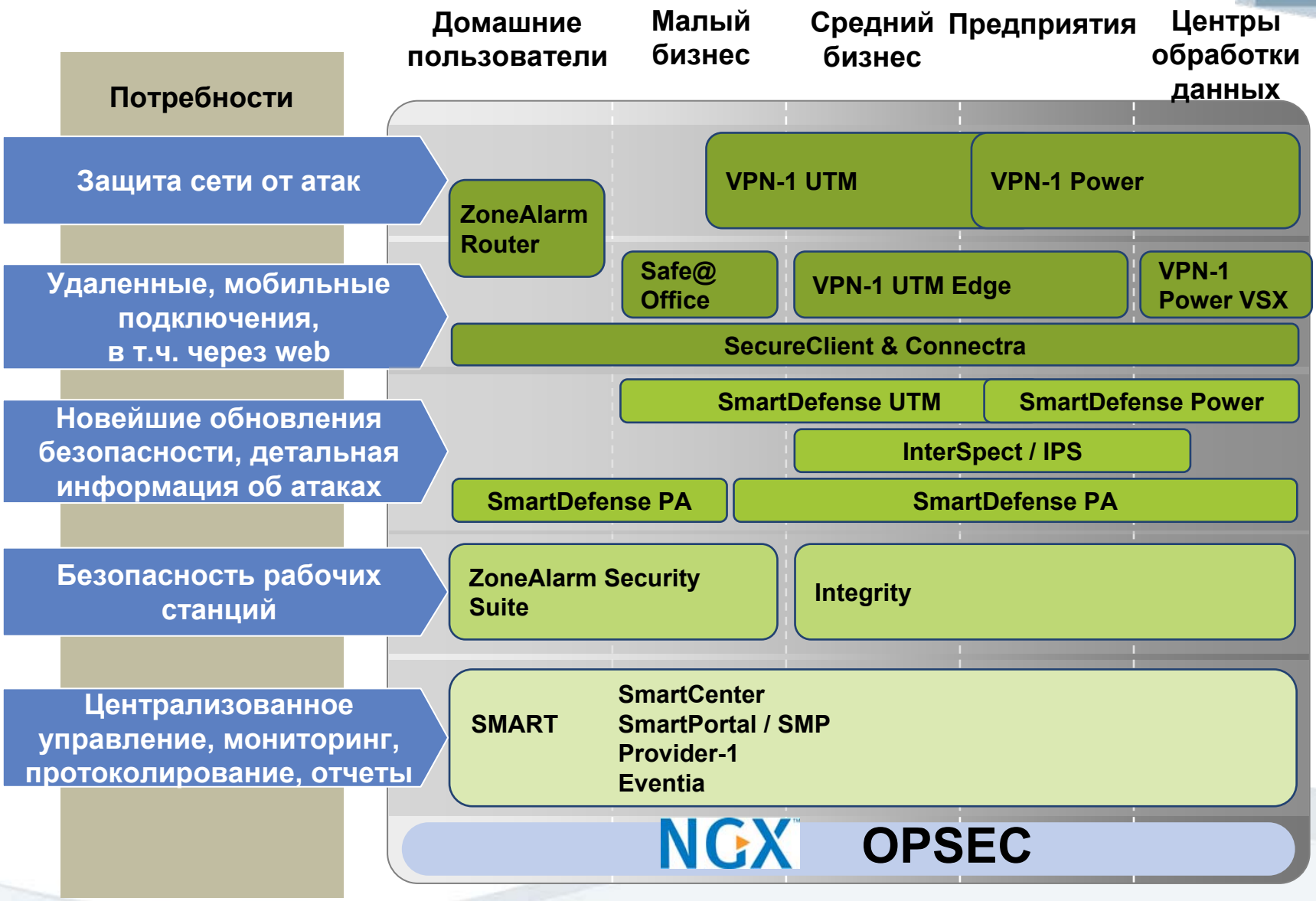
# Повестка дня

- **Состояние рынка систем IPS**
- Решение IPS-1 от Check Point
  - Архитектура
  - Функциональные возможности
  - Линейка продуктов и характеристики
  - Цены и лицензирование
  - Преимущества по сравнению с конкурентами
- Стратегия Check Point в отношении IPS-1
- Заключение
- Вопросы

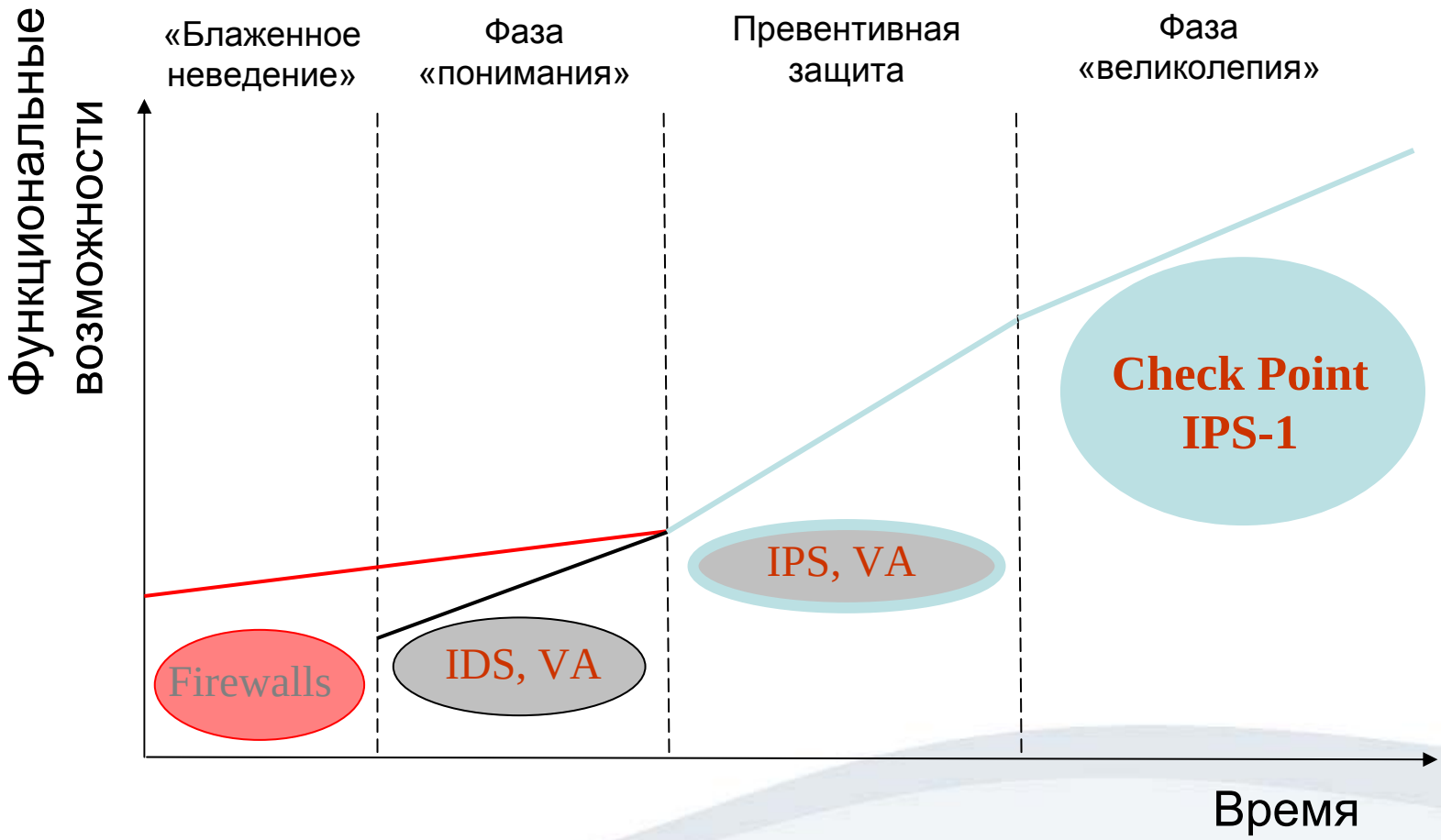
# Check Point – 14 лет лидерства на рынке информационной безопасности



# Check Point защищает все уровни сети, для любого типа пользователей

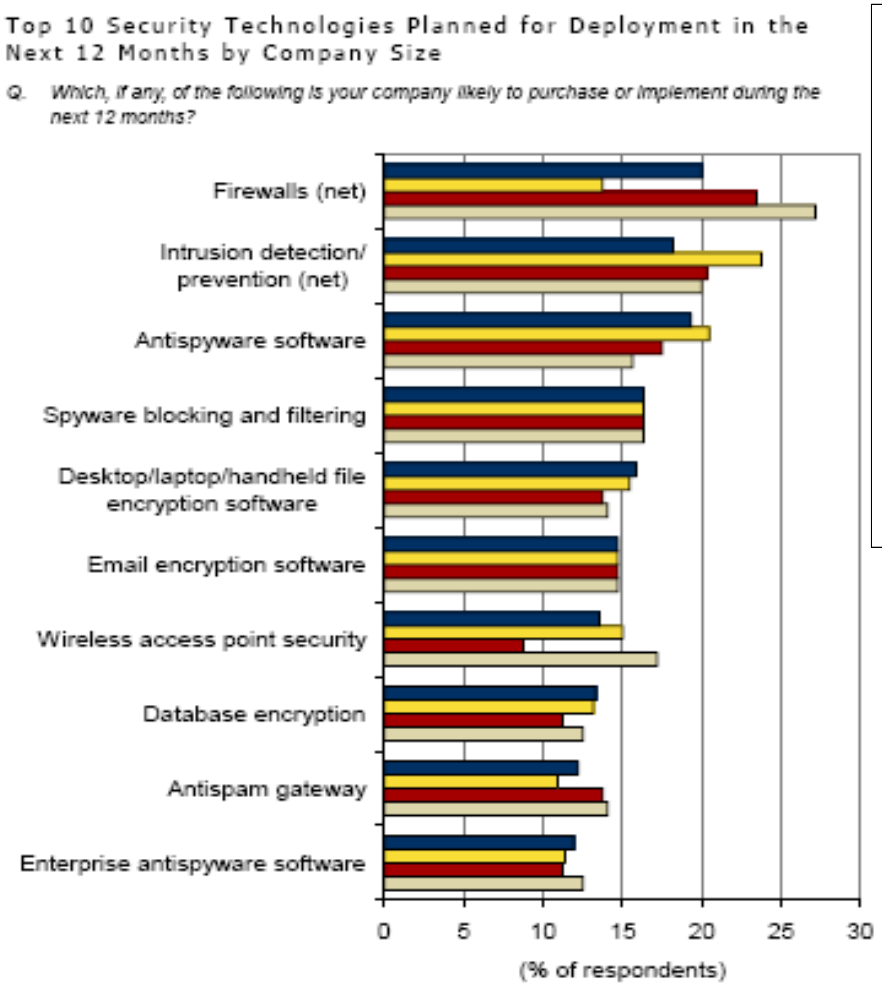


# Развитие систем IDS/IPS

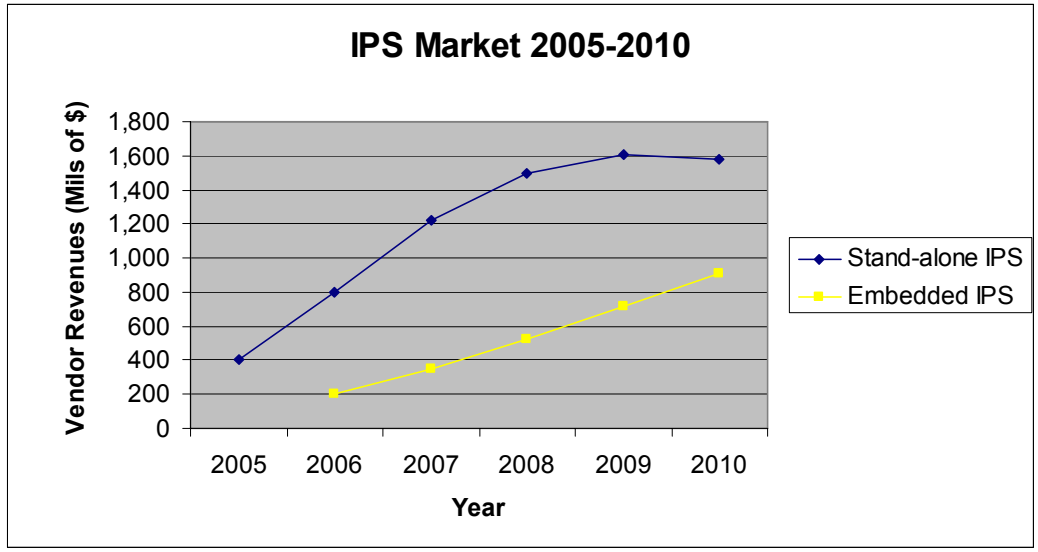


# Состояние и перспективы рынка систем IPS

**IDC: Ежегодый обзор рынка средств ИБ**




**Масштабы рынка систем IDS/IPS**




- Рынок средств IPS 2007
  - Выделенные IPS - $1.2 Billion
  - Интегрированные IPS - $400 Million
- Развитие и рост рынка средств IPS
- Check Point представлен в каждом из сегментов рынка средств IPS

# Повестка дня

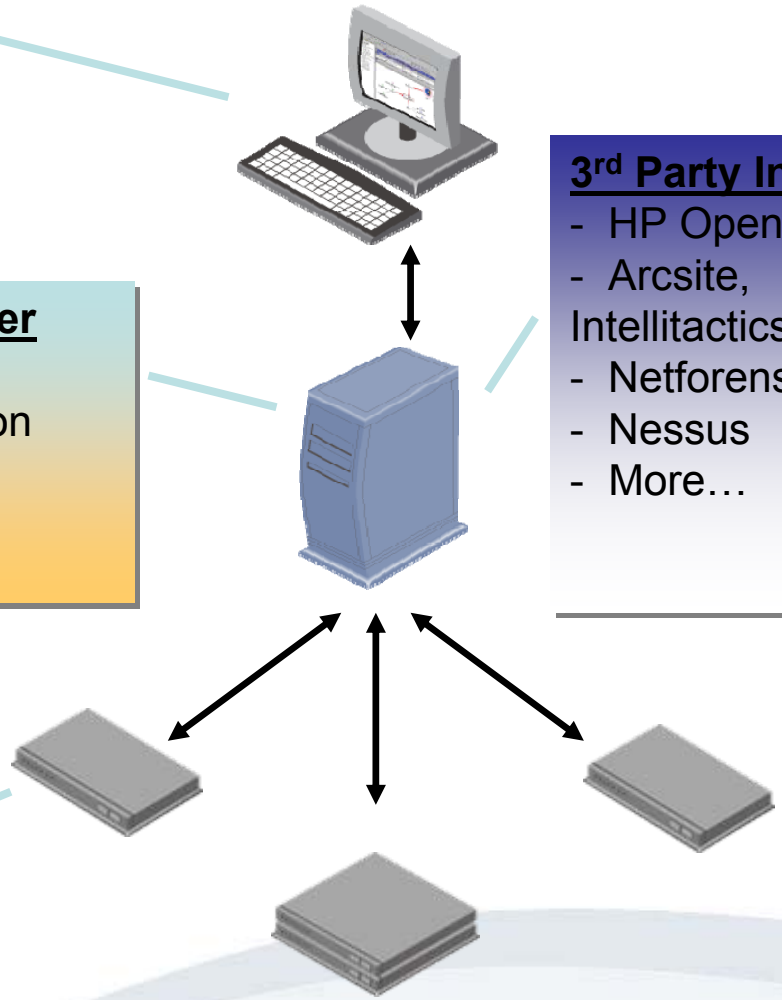
- Состояние рынка систем IPS
- **Решение IPS-1 от Check Point**
  - **Архитектура**
  - **Функциональные возможности**
  - **Линейка продуктов и характеристики**
  - **Цены и лицензирование**
  - **Преимущества по сравнению с конкурентами**
- Стратегия Check Point в отношении IPS-1
- Заключение
- Вопросы

# Архитектура Check Point IPS-1

**IPS-1 Management Dashboard**
- Centralized Management
- Real Time Views
- Advanced Forensics
- Reporting and Compliance

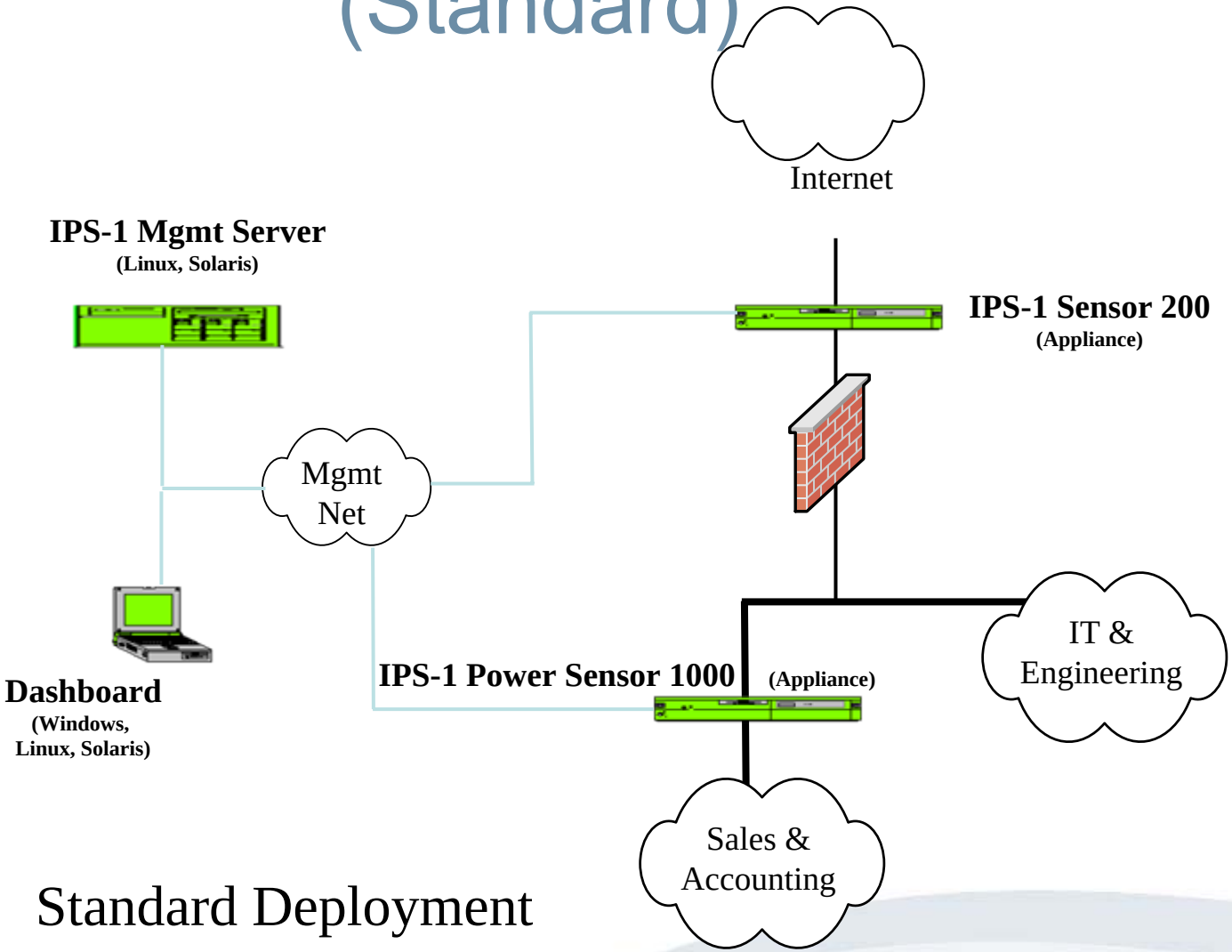
**IPS-1 Management Server**
- Optimized Data Store
- Multi-Element Correlation
- Dynamic Shielding

**IPS-1 Sensor**
- Hybrid Detection Engine
- Confidence Indexing
- Open signature language
- Multi-mode prevention appliance with Failover



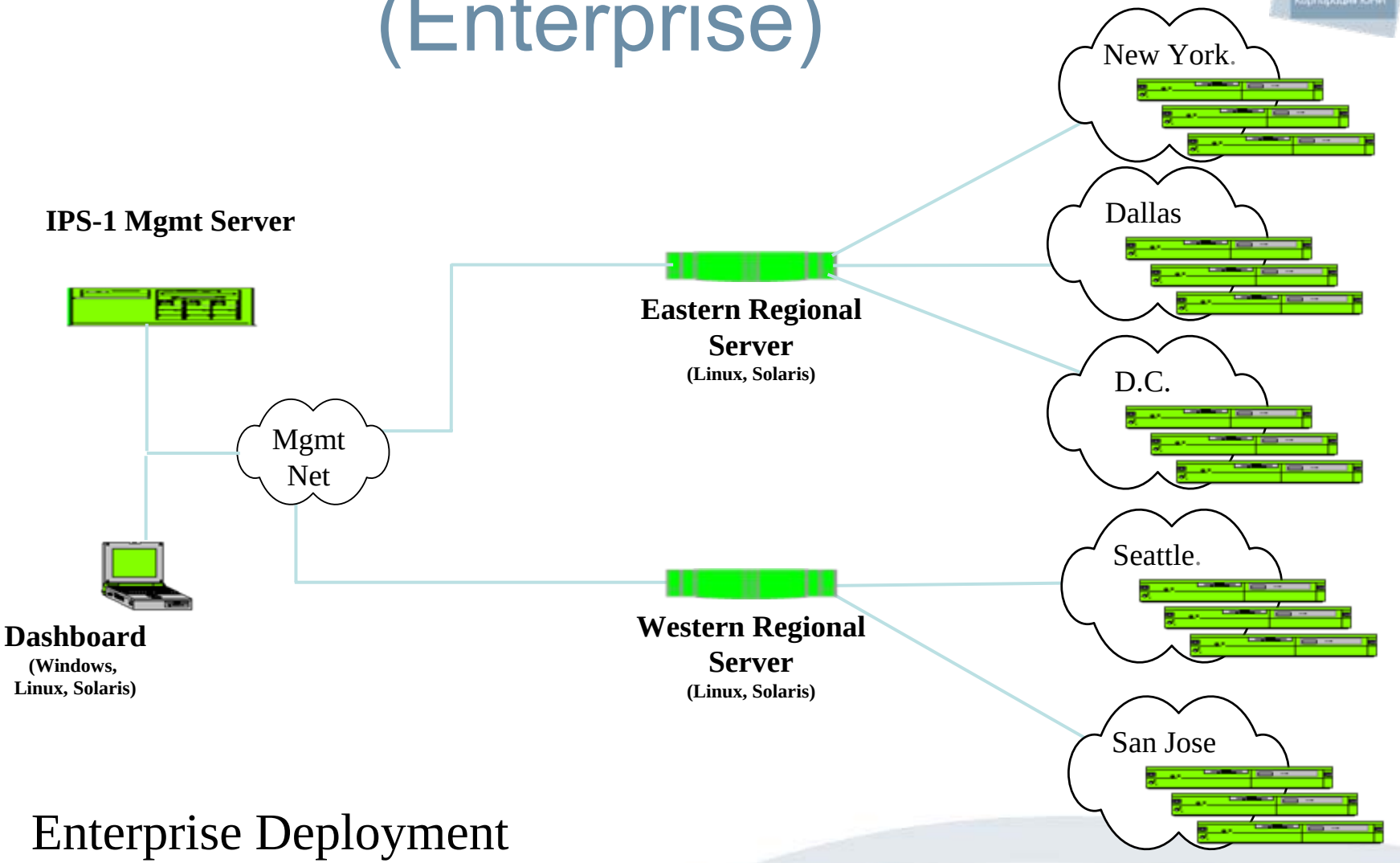
**3rd Party Integration**
- HP OpenView
- Arcsite, Intellitactics
- Netforensics
- Nessus
- More…

# Централизованное управление (Standard)



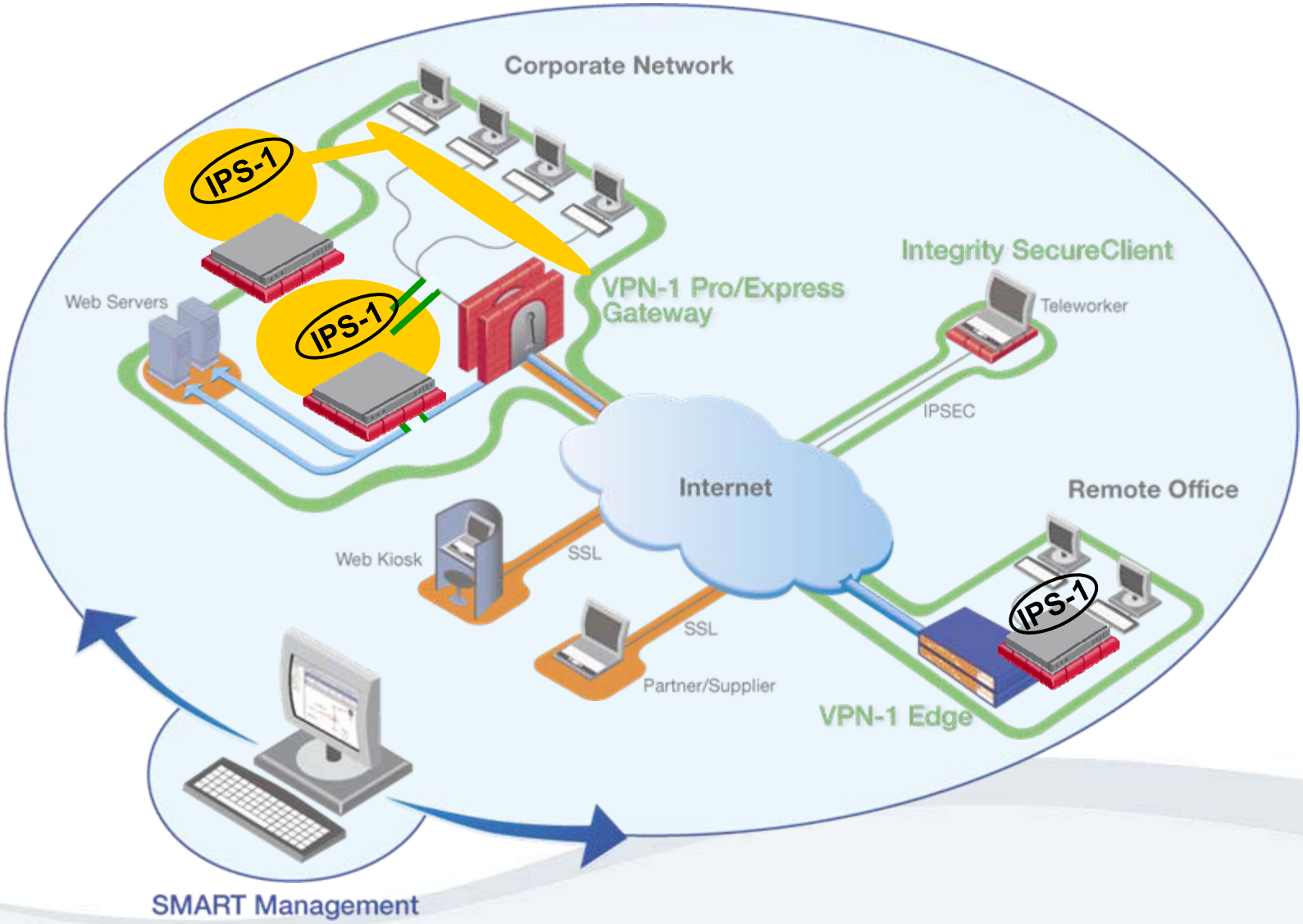

Standard Deployment

# Централизованное управление (Enterprise)




Enterprise Deployment

# Вариант реализации системы IPS-1



# Check Point IPS-1: IPS и даже больше

- **Защита критических ресурсов**
  - Система предотвращения атак в т.ч. на уровне приложений
    - “0-day” предотвращение атак для более чем 30 протоколов
    - Потрясающая точность, устойчивость к технологиям обмана IDS/IPS
    - Hybrid Detection Engine
  - Отличное соотношение цена/качество/производительность
  - Назначение: Чистота сети & Защита от червей

- **Активная динамическая защита сети (Active Dynamic Network Protection)**
  - Основной компонент стратегии Check Point’s в части IPS
  - Автоматический импорт, корреляция и адаптация к данным об уязвимостях
  - Точные и детальные отчеты о брешах и уязвимостях

- **Check Point IPS-1 SmartDefense Services**
  - Security Response Team ***(SRT)***: постоянно опережает конкурентов
  - Каждый пользователь IPS-1 имеет доступ к расширенной базе знаний SRT

# Check Point IPS-1: Централизованное управление

- **Установка за считанные минуты (а не часы или дни)**
  - “Lights-out” IPS-1 Smart Sensor appliances can be drop-shipped
  - НЕ требуется глубоких знаний по безопасности
- **Интуитивно-понятный, мощный интерфейс**
  - Разбор  инцидентов, настраиваемые режимы просмотра, корреляции
  - Отчеты
  - Скоро: Интеграция с Eventia
- **Централизованное управление в рамках всего предприятия**
  - Скоро: Интеграция с SmartCenter и Provider-1

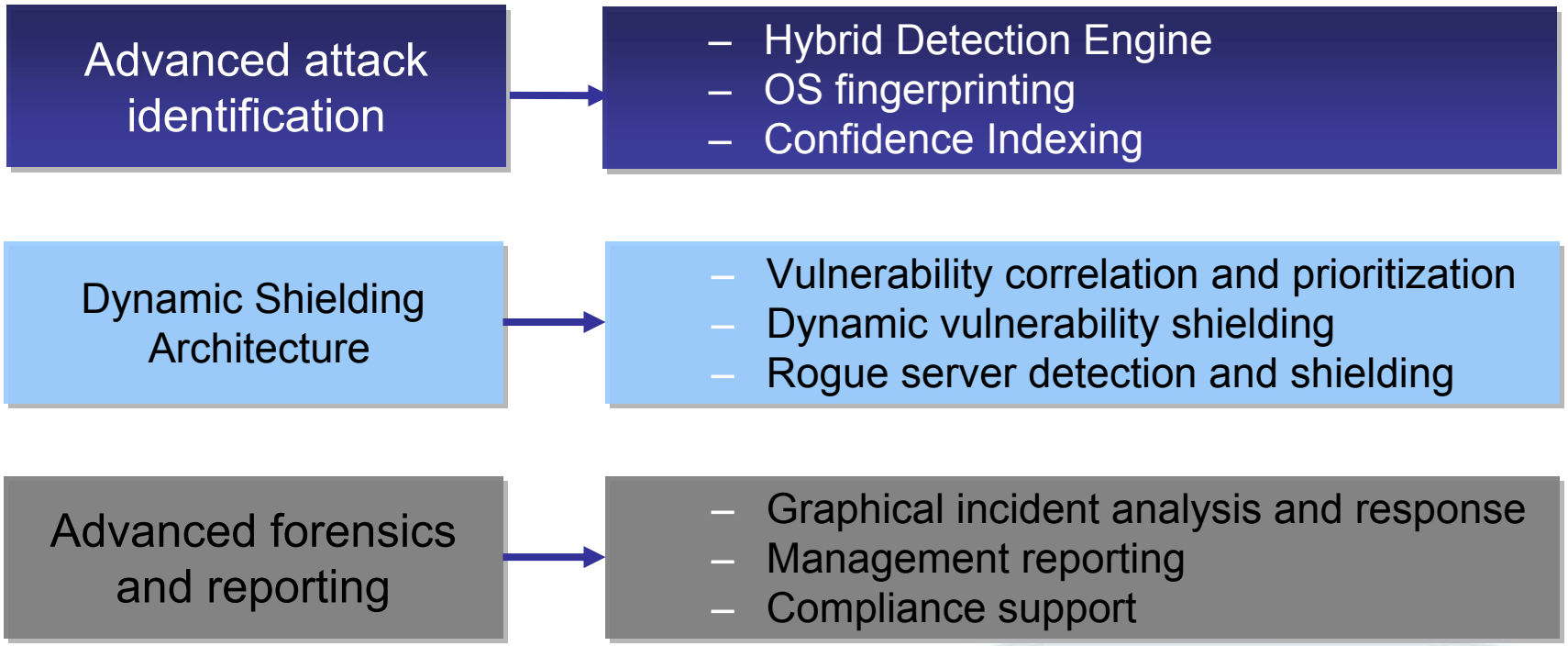
# Check Point IPS-1: Спокойствие и возврат инвестиций

- **Безопасность и доступность - непрерывно**
  - Отказоустойчивый режим: Fail Pass-through mode
  - Настраиваемое время задержки: Configurable Latency Tolerance (typically <1ms)
  - Режим обучения: “Learning Mode”
  - Наиболее конфигурируемая, адаптирующаяся IPS среди существующих
  - Check Point IPS-1 Sensors: **НИ ЕДИНОЙ УЯЗВИМОСТИ**
  - Защищенный обмен (AES-128)

- **Возврат инвестиций (ROI)**
  - Reduce Annual Loss Expectancy (ALE)
  - Comply With Regulations (SOX, HIPAA, etc.)
  - Appliance model saves administration costs

# Функции и особенности IPS-1

- Уникальная возможность комбинировать несколько источников для идентификации атаки
- Надежная адаптивная безопасность для автоматической реакции

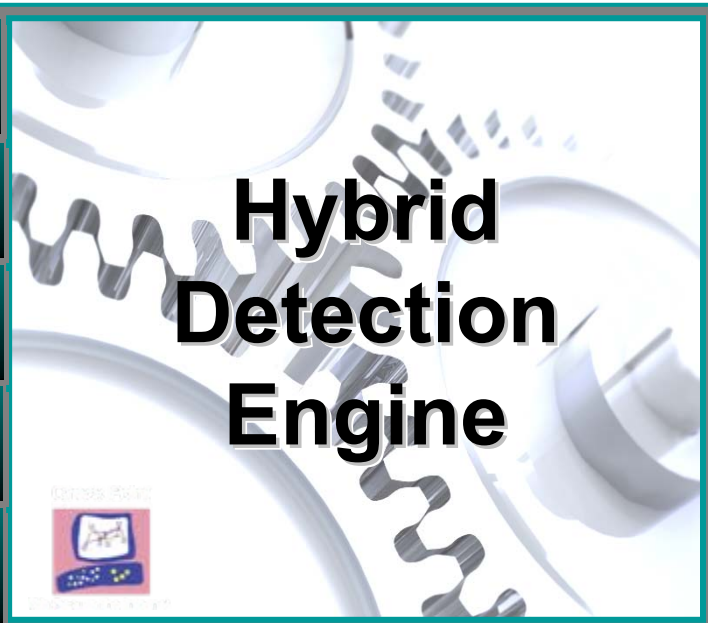


# Hybrid Detection Engine

**Надежный «гибридный» detection engine гарантирует обнаружение и предотвращение атак**

**Мощный и гибкий язык N-Code расширяет возможности по обнаружению и предотвращению атак**

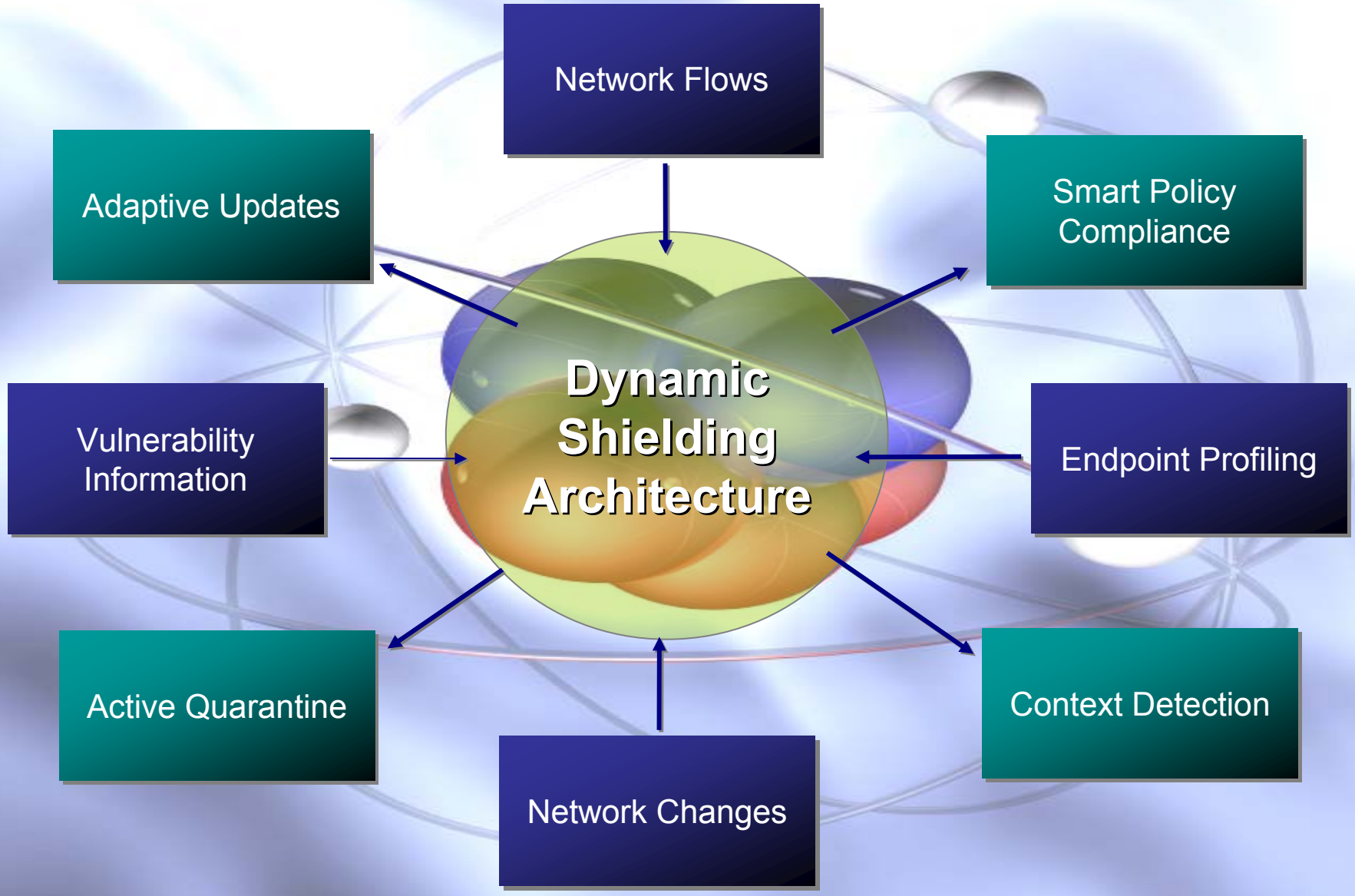
- Vulnerability signatures
- Exploit signatures
- Anomaly detection
- Protocol analysis
- Multi-element correlation




- Application awareness
- IP reassembly
- OS fingerprinting
- Application fingerprinting
- Dynamic worm mitigation

N-Code™ Signature Language

# Dynamic Shielding Architecture

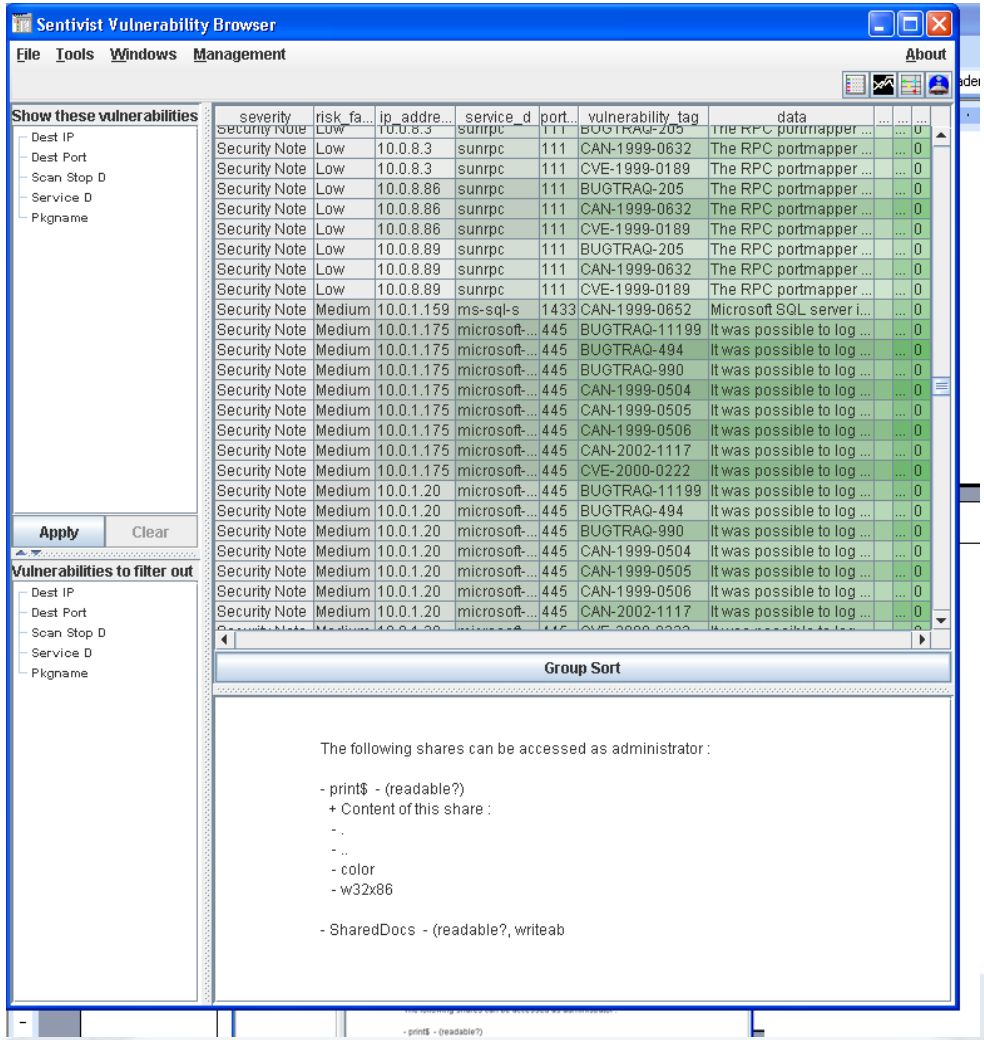


# Инструменты расследования инцидентов и механизмы формирования отчетности

- Quickly dissect attack data
- Monitor in real time attack and prevention activity
- Pinpoint attacks by grouping and drilling down on events and alerts
- Create informative reports from either ad hoc or pre-defined reports

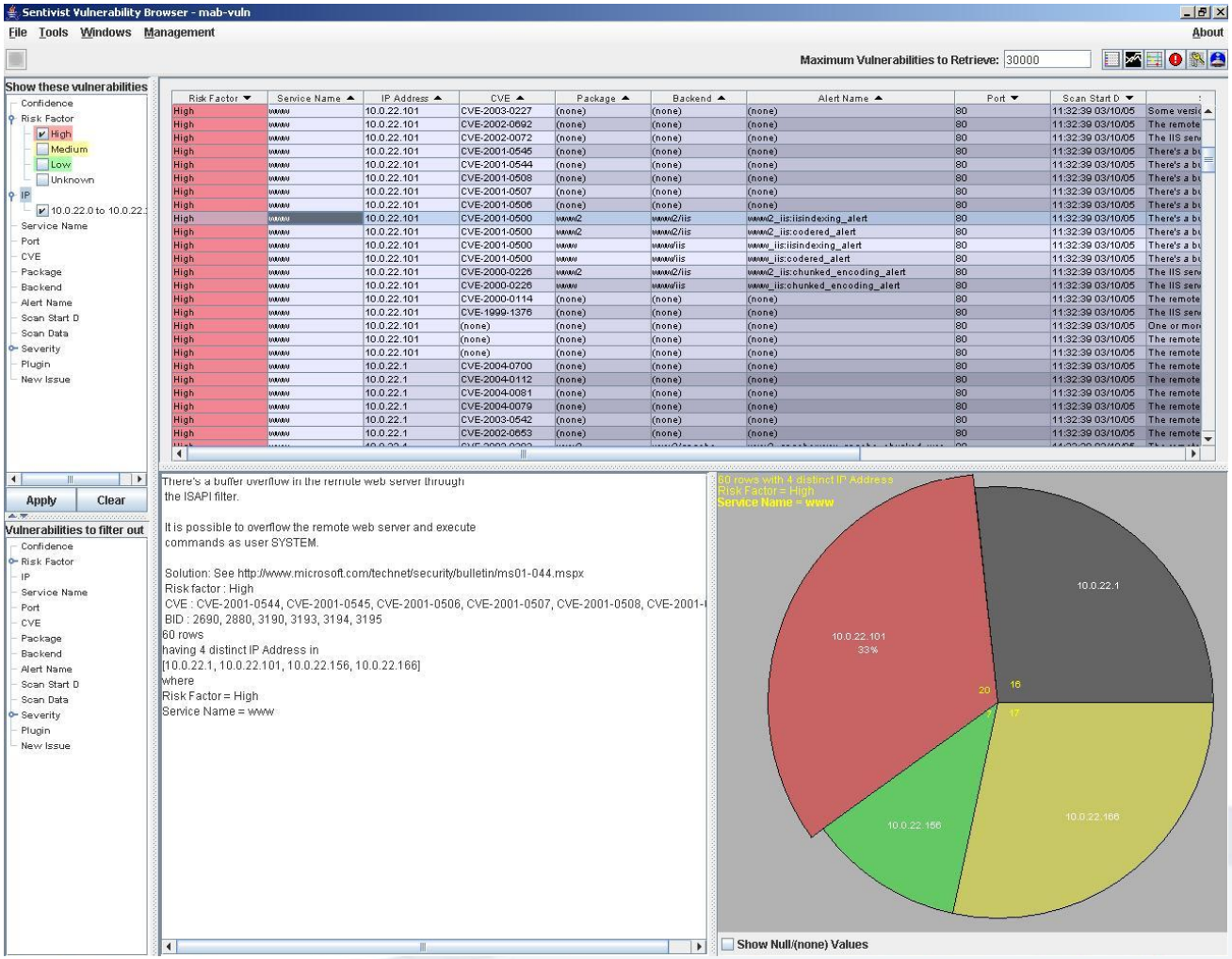
# Dynamic Network Protection : Active

- Легко идентифицирует уязвимости с ВЫСОКИМ (HIGH) риском
- Основывается на импорте Активных сканирований (поэтому “Active DNP”)
- Позволяет пользователям непрерывно видеть рискованные события, требующие немедленного вмешательства

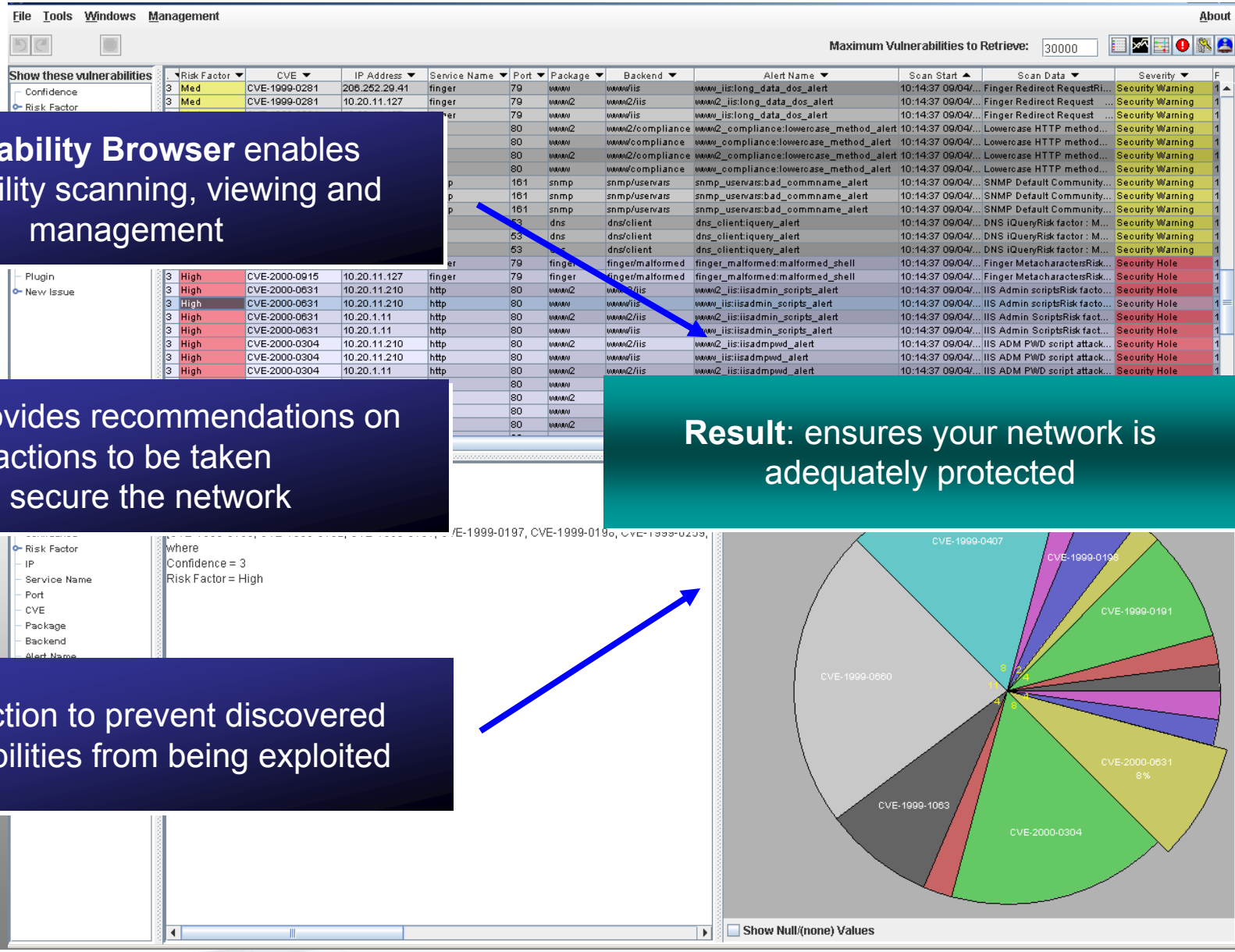


# Просмотр уязвимостей с DNP

**Взаимодействие между данными об уязвимостях (VA) и патентованной технологией Dynamic Network Protection (DNP) для взаимодействия с Check Point IPS-1.**



# Просмотр уязвимостей с DNP (продолжение)




**Vulnerability Browser** enables vulnerability scanning, viewing and management

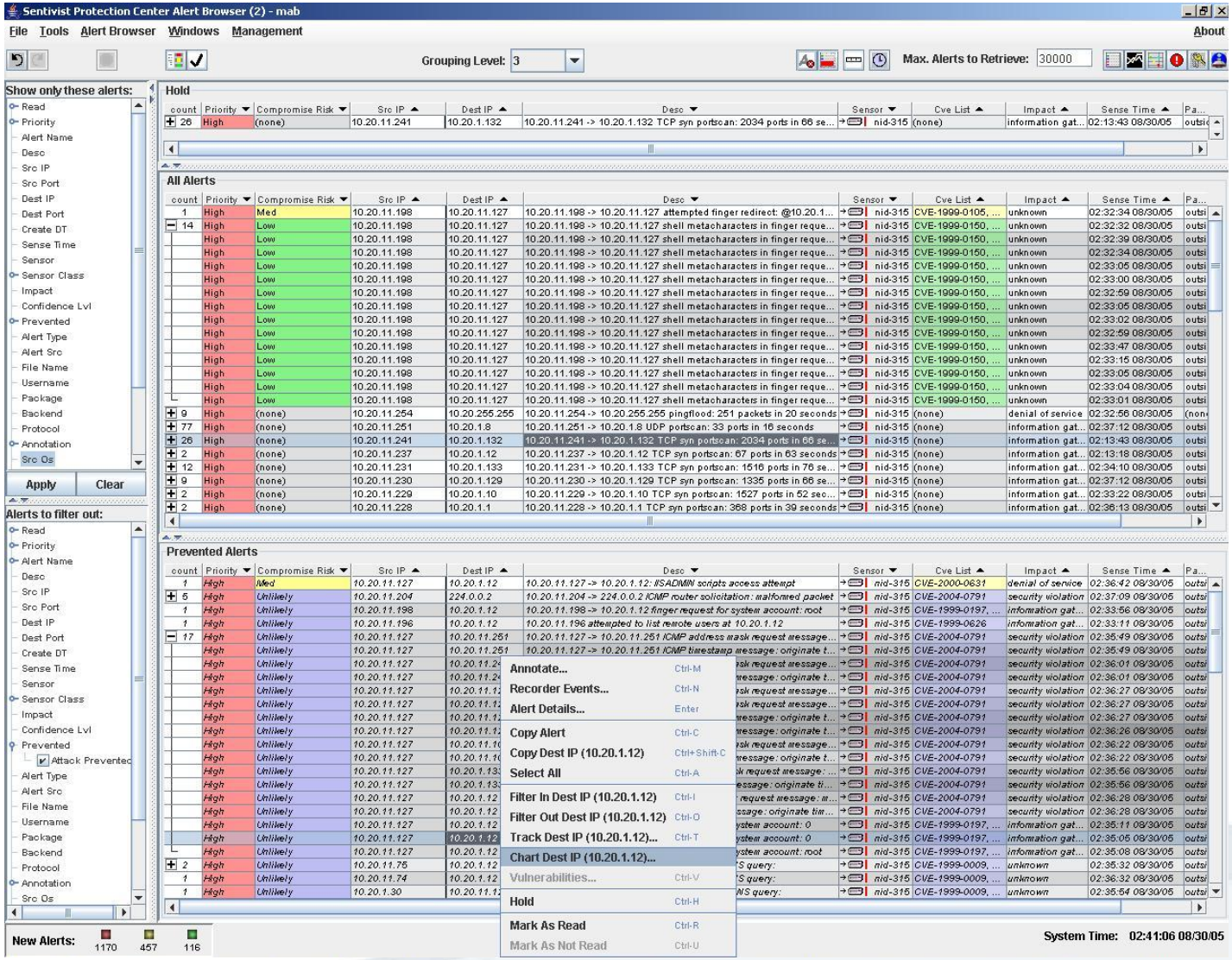
IPS-1 provides recommendations on actions to be taken to secure the network

**Result**: ensures your network is adequately protected

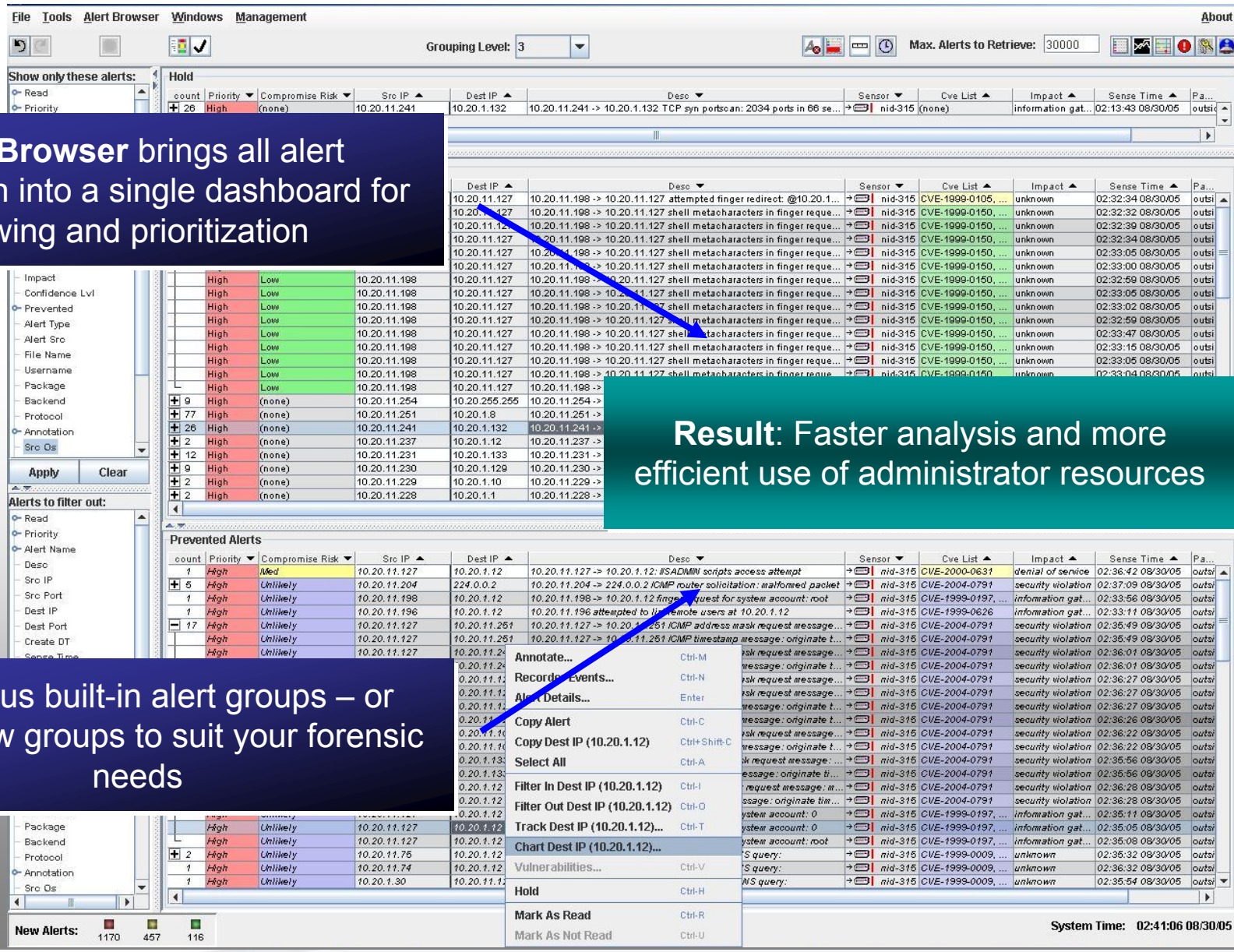
Take action to prevent discovered vulnerabilities from being exploited

# Просмотр событий с DNP

## Предотвращенные атаки с интеграцией с DNP в унифицированном отображении



# Просмотр событий с DNP (продолжение)



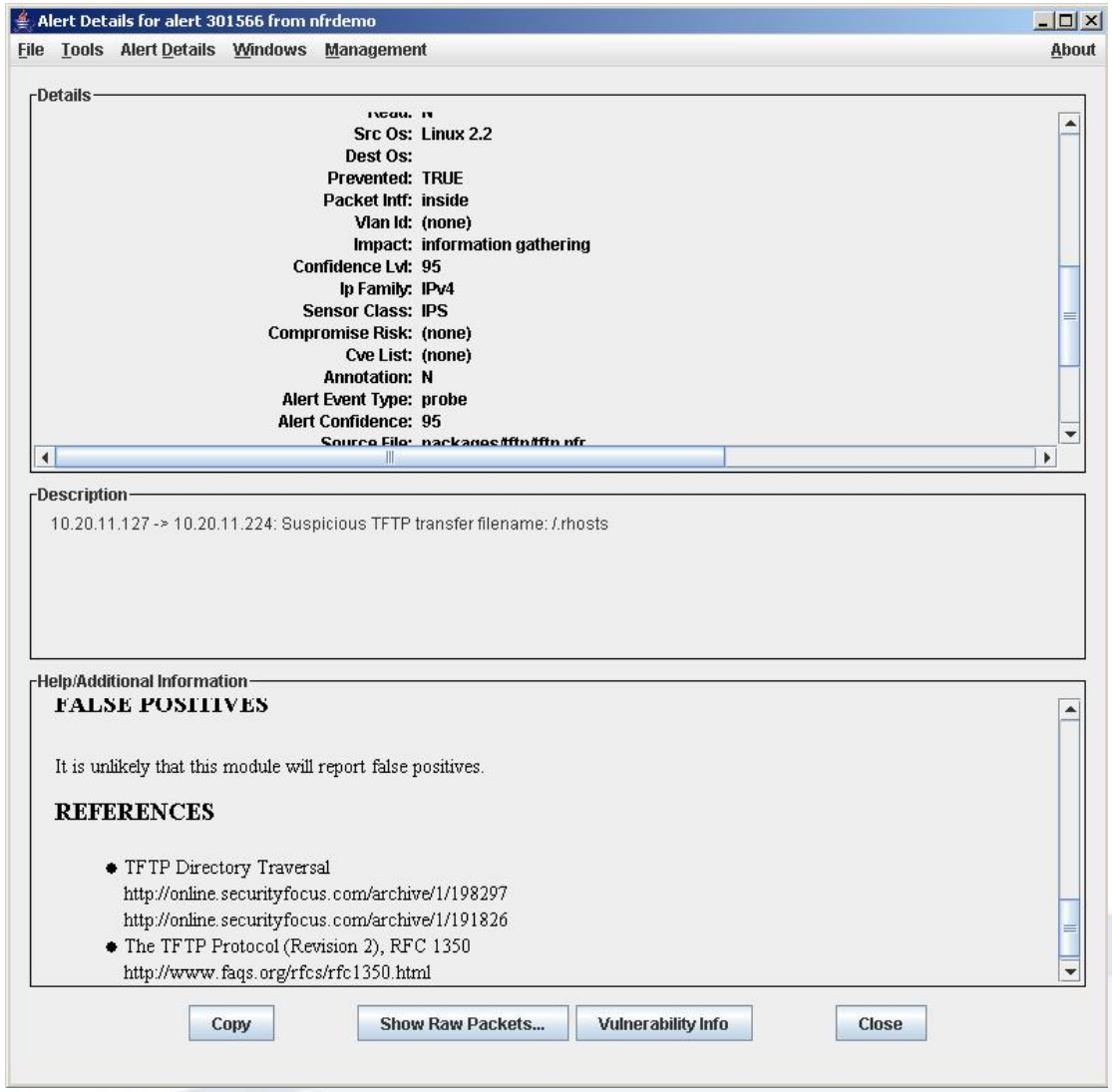

**Alert Browser** brings all alert information into a single dashboard for viewing and prioritization

**Result**: Faster analysis and more efficient use of administrator resources

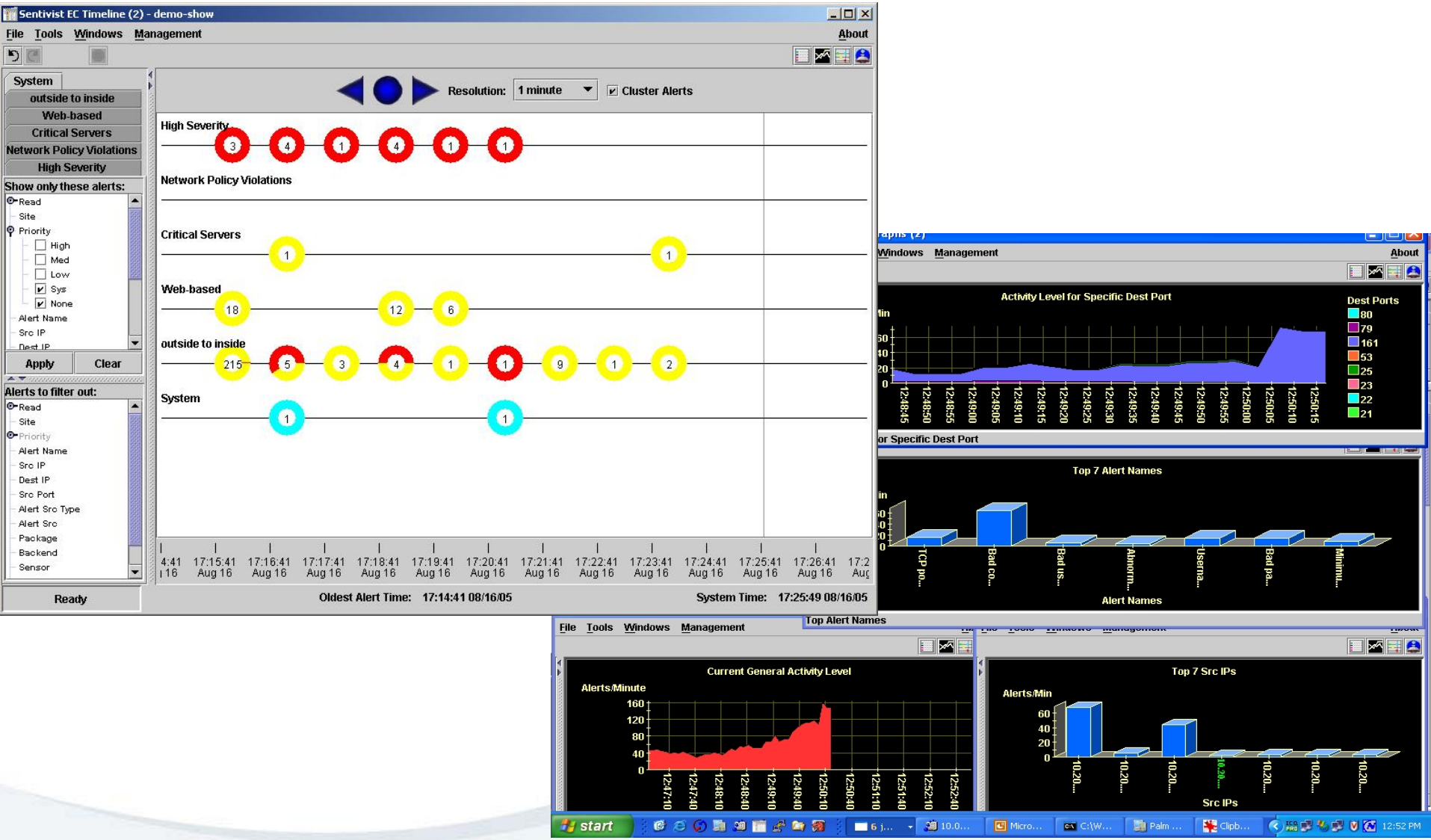
Numerous built-in alert groups – or create new groups to suit your forensic needs

# Детальные описания от SRT

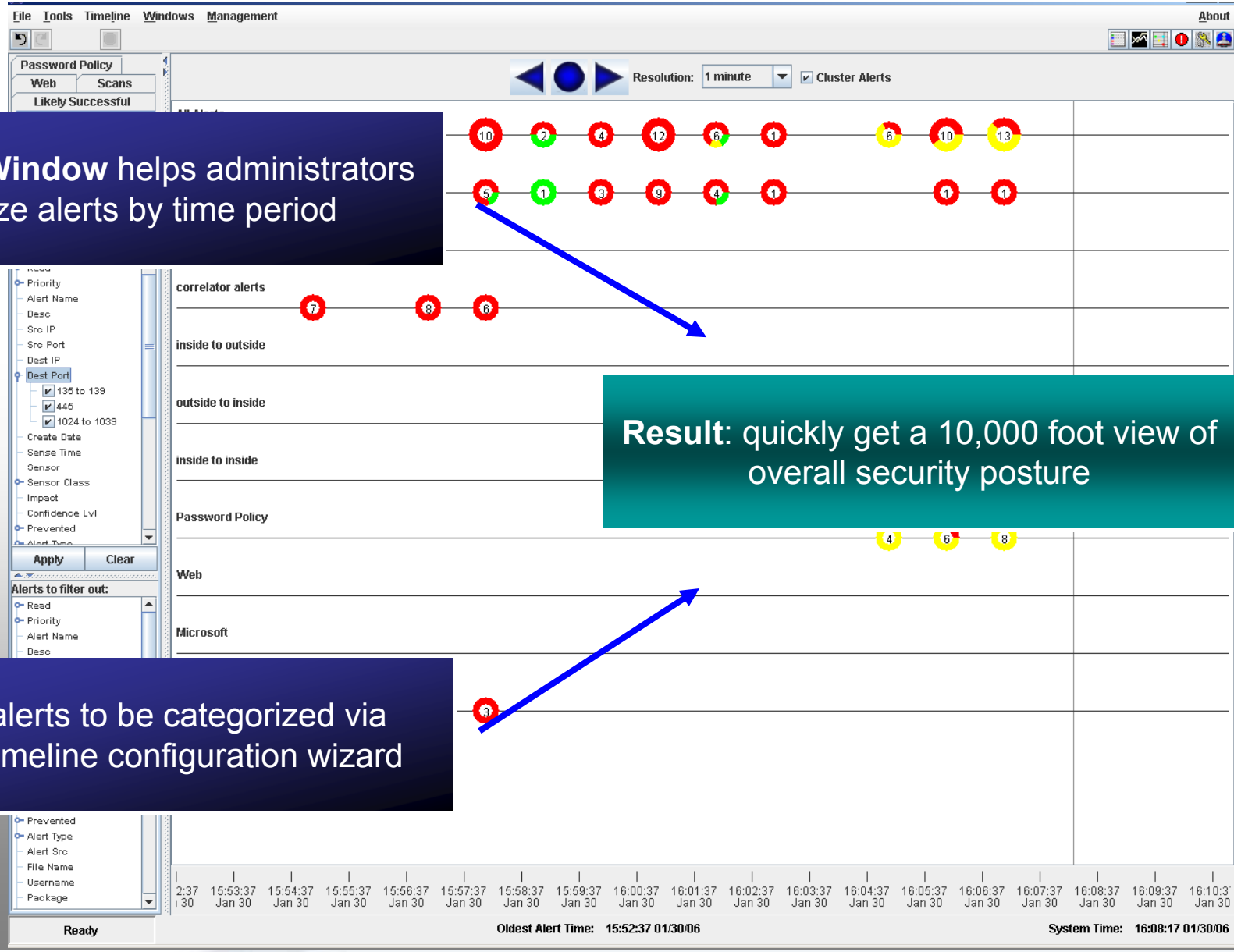
**Подробная информация от Security Response Team (SRT)**



# Отображение информации в реальном времени



# Отображение информации в реальном времени




**Timeline Window** helps administrators analyze alerts by time period

**Result**: quickly get a 10,000 foot view of overall security posture

Allows alerts to be categorized via simple Timeline configuration wizard

# Отчетность

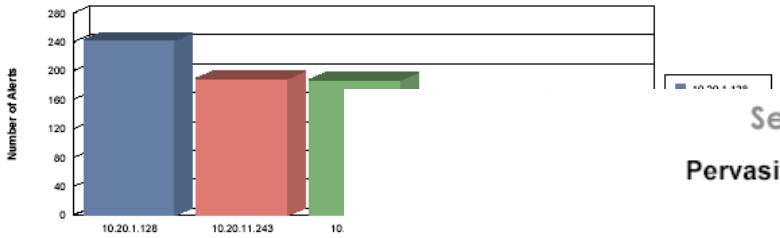
## Security Status

From: 1/26/2005 6:44:50AM

To: 1/26/2005 9:44:50AM

This report gives an overview of the network's security status. Graphs outline the major threats including highlights of which systems are under the most attack, where the attacks are coming from, and how severe those attacks are.

### Most Targeted Hosts



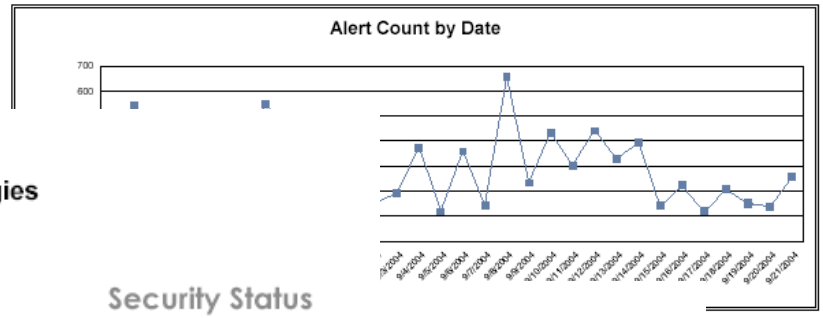

This graph shows the IPs of the 5 host machines
6:44:50AM to 1/26/2005 9:44:50AM. A host ma
an alert. These particular machines may be at hi
resources are allotted to keep security patches u
critical nature of the targeted host machines, furt

## Alerts by Date

From: 8/21/2004 11:18:02PM

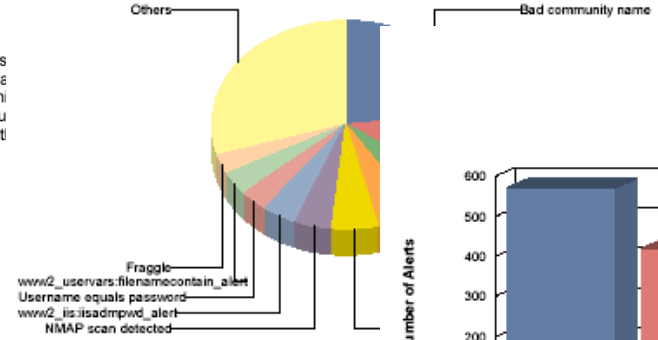
To: 9/21/2004 11:18:02PM

This report shows the number of alerts that occurred between 8/21/2004 11:18:02PM and 9/21/2004 11:18:02PM grouped by the date.




## Security Status

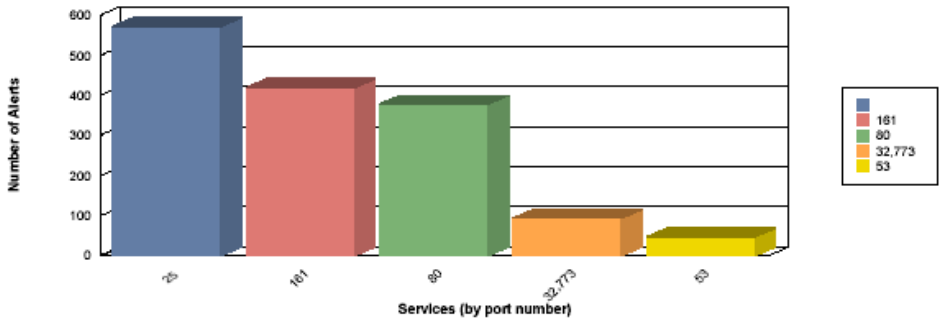
### Pervasive Attack Strategies




Above is shown the top ten strategies at
methods of attack used between 1/26/2
network is protected against them.

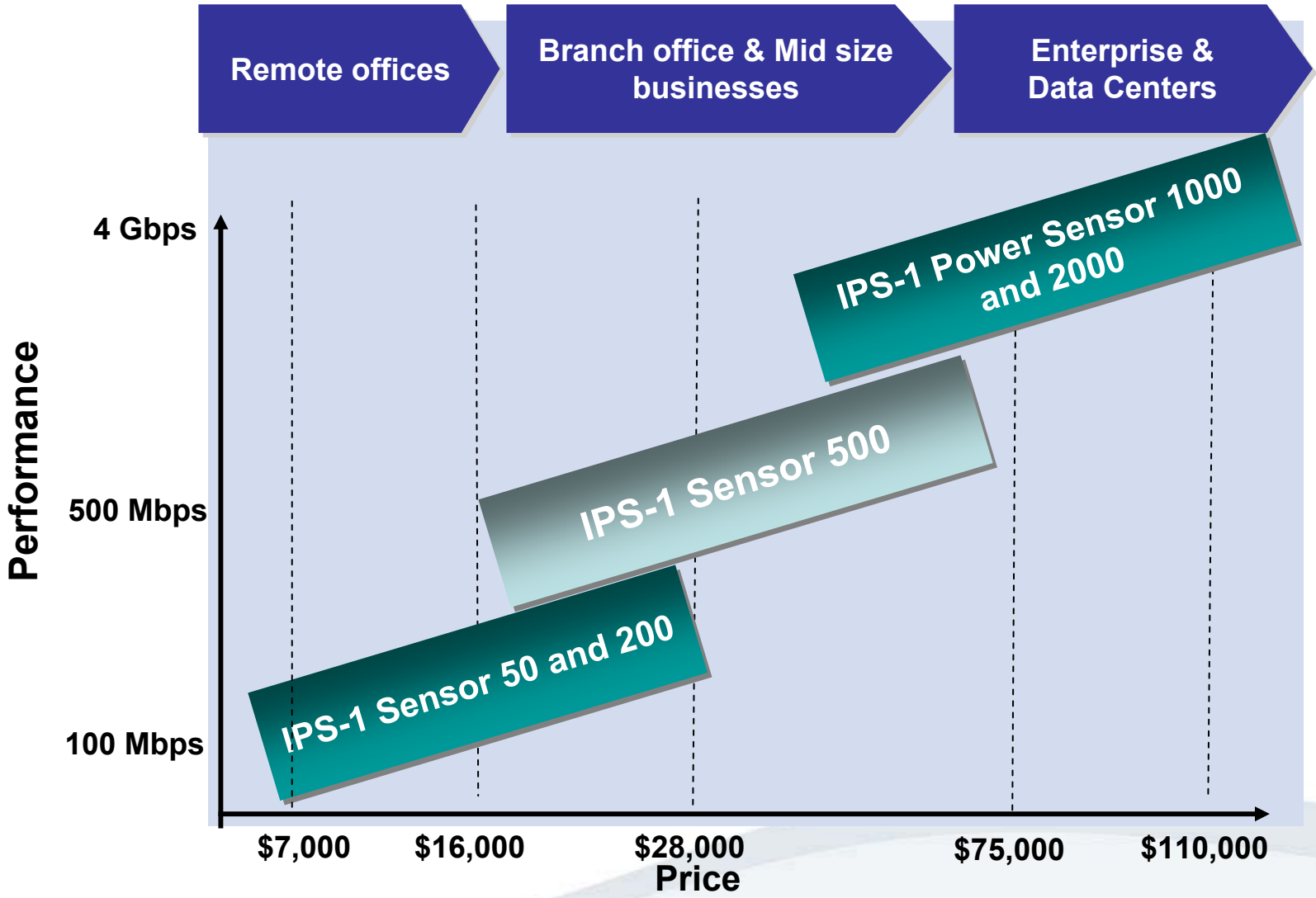
## Security Status

### High Risk Services




This graph shows the 5 services which are experiencing the most attacks. The services are represented by their port number. A service is any application's functionality which is made available via a network. Each service on a network has a port number by which it can be contacted. Most services use a consistent number by default. For example, Oracle servers usually use port number 1521. If port 1521 has a high alert count and you have an Oracle server on your network, then your Oracle server may be at high risk for compromise. Thus, this graph indicate which services on your network are at most risk.

# Линейка продуктов IPS-1



# Характеристики продуктов IPS-1

| | IPS-1 Sensor 50 | IPS-1 Sensor 200 | IPS-1 Sensor 500 | IPS-1 Power Sensor 1000 | IPS-1 Power Sensor 2000 |
|---|---|---|---|---|---|
| **Network location** | Remote office/network perimeter | Remote office/network perimeter | Network perimeter (multi-segment) | Network core (multi-segment) | Network core (multi-segment) |
| **Throughput (IPS/IDS)** | 50/75 Mbps | 200/250 Mbps | 500Mbps/ 1Gbps | 1/2Gbps | 2/4Gbps |
| **Concurrent sessions** | 100,000 | 200,000 | 500,000 | 1.2 million | 2.8 million |
| **Monitoring interfaces** | 2 x 10/100/1000 Mbps copper | 2 x 10/100/1000 Mbps copper or 2 x 1000 Mbps fiber | 4 x 10/100/1000 Mbps copper or 4 x 1000 Mbps fiber | 8 x 10/100/1000 Mbps copper or 8 x 1000 Mbps fiber | 8 x 10/100/1000 Mbps copper or 8 x 1000 Mbps fiber |

# Характеристики продуктов IPS-1 (продолжение)

| | IPS-1 Sensor 50 | IPS-1 Sensor 200 | IPS-1 Sensor 500 | IPS-1 Power Sensor 1000 | IPS-1 Power Sensor 2000 |
|---|---|---|---|---|---|
| **Management interfaces** | 1 x 10/100/1000 Mbps copper | 1 x 10/100/1000 Mbps copper | 1 x 10/100/1000 Mbps copper | 1 x 10/100/1000 Mbps copper | 1 x 10/100/1000 Mbps copper |
| **Redundant power supplies** | NO | YES | YES | YES | YES |
| **Redundant storage** | NO | NO | NO | YES | YES |
| **Form factor** | 1-RU | 1-RU | 1-RU | 2-RU | 2@2-RU |

# Преимущества IPS-1…

- Hybrid Detection Engine
  - *Умные сенсоры усиливают множество техник детектирования и анализа включая сигнатуры уязвимостей, эксплойтов, обнаружение аномалии протоколов, контроль состояния, глубокие проверки пакетов, “Smart IP Reassembly”, идентификация ОС и приложений, корреляцию множества событий и динамическое противостояние червям.*

- Облегченное внедрение IPS
  - *Заказчики могут постепенно внедрять предотвращение атак; Сенсоры могут включаться только для обнаружения атак (IDS), для обучения характеру трафика. По достижению комфортного уровня, достаточно включить режим защиты.* ***Confidence Indexing*** *позволяет сотрудникам службы безопасности детально настроить уровни защиты в соответствии с ценностями защищаемых объектов.*

- Информация о сетевых объектах
  - *IPS-1 интегрирует, коррелирует и графически представляет информацию об угрозах. Ее можно ранжировать по уязвимости, серьезности, воздействию, приложению – структурировать для удобного использования*

# Преимущества IPS-1…

- Dynamic Shielding Architecture
  - *Осведомленная, адаптивная и действенная безопасность – автоматически распознает скрытые возможности для атак – такие как несанкционированные изменения сети, критические уязвимости – и динамически защищает эти точки от неизбежных атак.*
- Контроль ситуации
  - *Графическое отображение в реальном времени уязвимых точек и информации об атаках дают широкое представление об уязвимостях и событиях безопасности. Simple point and click actions allow focus on specific events to monitor the source's activity and potentially take action.*
- **Уровни безопасности**
  - *IPS-1 Smart Сенсоры обеспечивают множество механизмов защиты IDS, IPS, Dynamic Shielding, IM (AOL), VoIP (SIP), наряду с остальными - в одном устройстве, с единым пользовательским интерфейсом.*

# Преимущества IPS-1…

- Высокая производительность
  - *Смарт Сенсоры работают на скоростях от 20Mbps до 10Gbps. Сенсоры линейки Enterprise предлагают высокую плотность портов, функции high availability и возможность расширения.*
- Поддержка IPv6
  - *NFR была в передовиках в этом направлении, внедрив поддержку IPv6 еще в 2002. Поддержка IPv6 является обязательным требованием государственных органов США и Европы.*
- Открытый язык описания
  - *Сигнатуры IPS-1 пишутся на специальном языке N-Code. Это открытый язык, заказчик может посмотреть описания сигнатур, модифицировать их, разрабатывать их самостоятельно.*
- Security Response Team
  - *The Security Response Team (SRT) постоянно отслеживает новые уязвимости и угрозы и выпускает соответствующие обновления, обеспечивая постоянно высокий уровень безопасности.*

# Преимущества IPS-1 по сравнению с конкурентами

| Vendor | Comment | IPS-1 |
|---|---|---|
| **Cisco** | No credible inline offering – weak detection and analysis. Slow response on signature updates. Cisco is a networking company, not a security company. | IPS-1 beats Cisco in head-to-head bake-offs. Superior detection/prevention via Hybrid Detection Engine and Confidence Indexing. Signature updates consistently beat Cisco, often on their own IOS vulnerabilities. Full IPv6. |
| **Juniper** | Performance ratings are overstated leading to performance issues. Have UTM virtualization support. Unconfirmed IPv6 support. | Superior ease of use, forensics, and overall flexibility. Full IPv6 support. |
| **3Com** | "…just a pure play IPS focused on speeds and feeds…". Poor management for large deployments. Lack flexibility to support custom security needs. | Superior management and forensic analysis. Integrated network node intelligence, Dynamic Shielding. Open signature language for custom security needs. Full IPv6. |
| **ISS** | Performance issues in multi-gig offering. *Twenty-one* sensor vulnerabilities since 2000. Customers dissatisfied due to poor service and strong-armed Sales tactics. Uncertainty due to IBM acquisition; IBM is not security focused. Claim IPv6 support. | Superior multi-gig performance. Check Point is the pure security play. *Zero* IPS-1 sensor vulnerabilities since 2000. Full IPv6 support. |
| **McAfee** | Poor management for large deployments. Performance issues at the high-end. | Superior management and forensic analysis. Integrated network node intelligence, Dynamic Shielding. Open signature language for custom security needs. |
| **SourceFire** | Questionable inline offering. High false positive rate.<br>*Eleven* Snort vulnerabilities since 2000. | True inline prevention. Superior alert management and forensic analysis. Lower false positive rates through Confidence Indexing and Alert Flood Suppression capabilities. *Zero* IPS-1 sensor vulnerabilities since 2000. Full IPv6 support. |

# Повестка дня

- Состояние рынка систем IPS
- Решение IPS-1 от Check Point
  - Архитектура
  - Функциональные возможности
  - Линейка продуктов и характеристики
  - Цены и лицензирование
  - Преимущества по сравнению с конкурентами
- **Стратегия Check Point в отношении IPS-1**
- Заключение
- Вопросы

# Стратегия Check Point в отношении IPS-1

IPS-1 – самостоятельная линейка устройств предотвращения вторжений (атак)

Интеграция средств управления IPS-1 с SmartCenter

Интеграция технологий IPS-1 в линейку продуктов Check Point, включающих в себя IPS

Достижение более высокой производительности IPS

Развитие новых гибридных технологий защиты

# Решения IPS-1 и Interspect – что и когда?

- Решение Check Point IPS-1
  - Потребность в отдельной системе (средствах) IDS/IPS.
  - Потребность в централизованном управлении компонентами IDS/IPS.
  - Потребность в расследовании инцидентов в вычислительной сети а также потребность в соответствующем инструментарии.
  - Потребность в гибридных механизмах анализа трафика в вычислительной сети.
  - Наличие в организации отдельных сотрудников, ответственных за систему (средства) IDS/IPS.

- Решение Check Point Interspect
  - Потребность в сегментации вычислительной сети.
  - Потребность в контроле доступа и возможность блокирования злоумышленника – на уровне сегмента вычислительной сети.

- Решение Check Point комбинированное IPS-1 и Interspect
  - Потребность в эшелонированной (многоуровневой) защите вычислительной сети.
  - Территориально-распределенная структура предприятия.
  - ДОПОЛНЯЮЩЕЕ, а не исключающее друг друга решение!

# Заключение

- Check Point IPS-1 – **самостоятельная** линейка выделенных (dedicated) устройств предотвращения вторжений (атак).

- Check Point IPS-1 – **новая линейка устройств**, которая дополняет уже существующий набор средств и систем защиты информации от компании Check Point.

- Check Point IPS-1 – **новый набор технологий**, дополняющих существующие технологии SmartDefense и Interspect от компании Check Point.

Спасибо!

# Introducing IPS-1

- Dedicated, inline Intrusion Prevention solution
  - Intrusion detection and prevention
  - Signature and heuristic technologies
- Provides important solution to Check Point portfolio.
- Complements existing SmartDefense integrated IPS strategy.
- Award winning technology.

INFORMATION SECURITY Hotpick

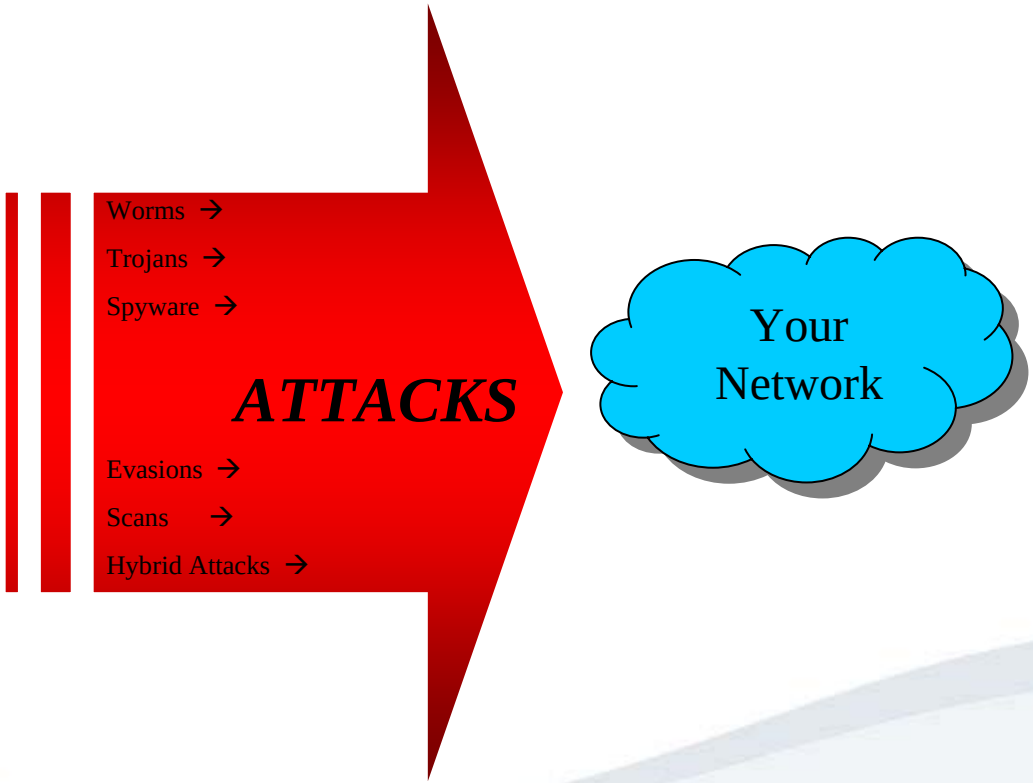
NSS approved

2005 DATAMATION PRODUCT OF THE YEAR

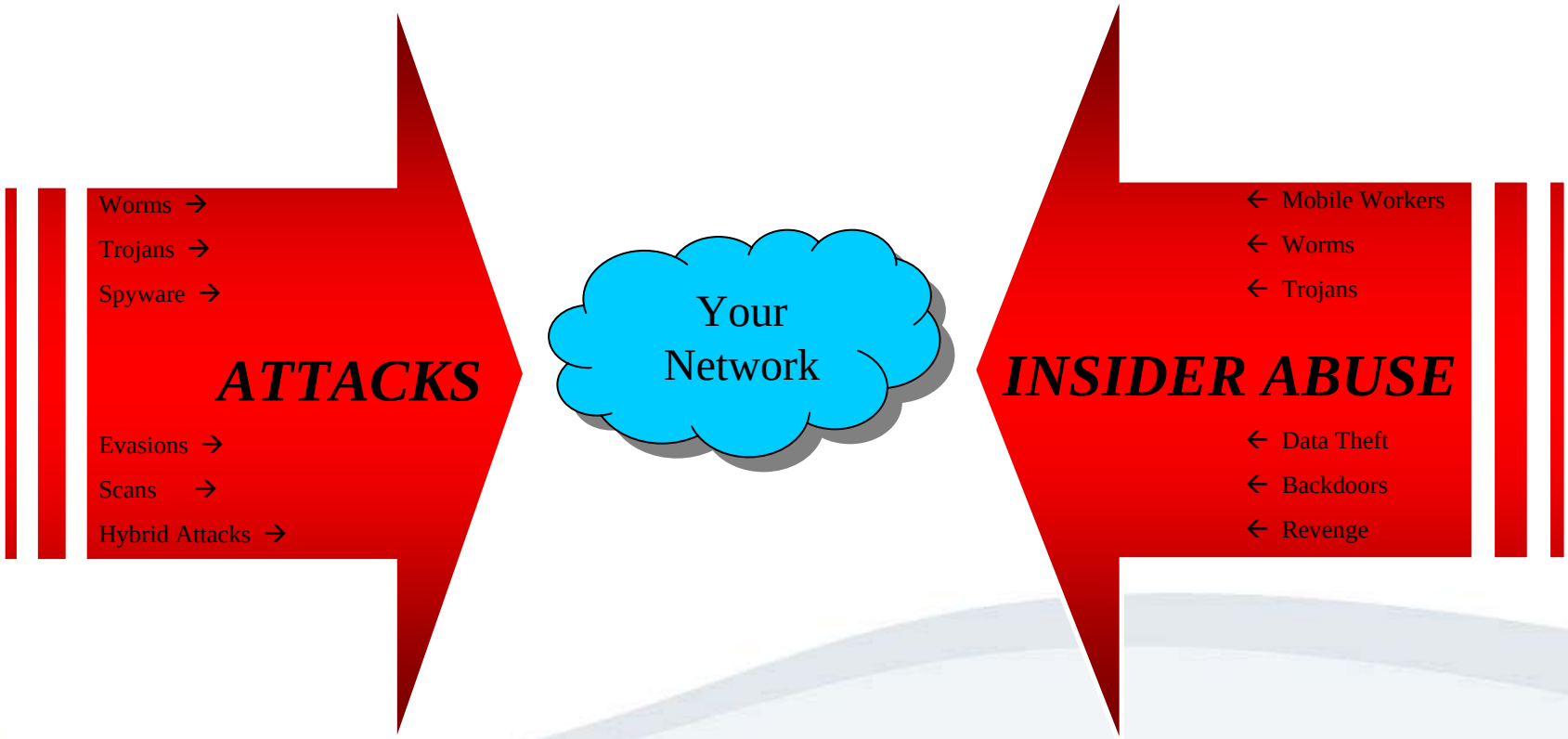
2005 FROST & SULLIVAN Customer Service Leadership Award

InfoWorld INNOVATORS 2005

# The Network Security Challenge

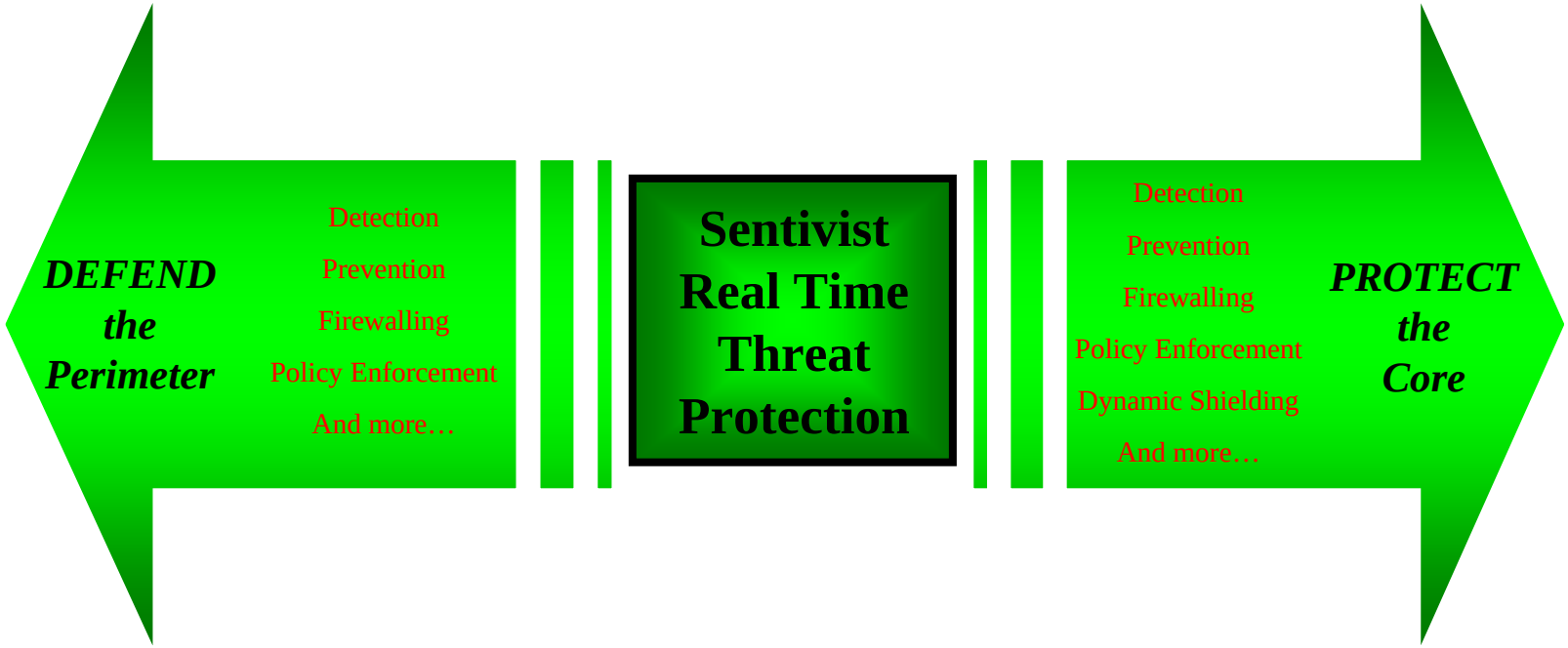


# The Network Security Challenge

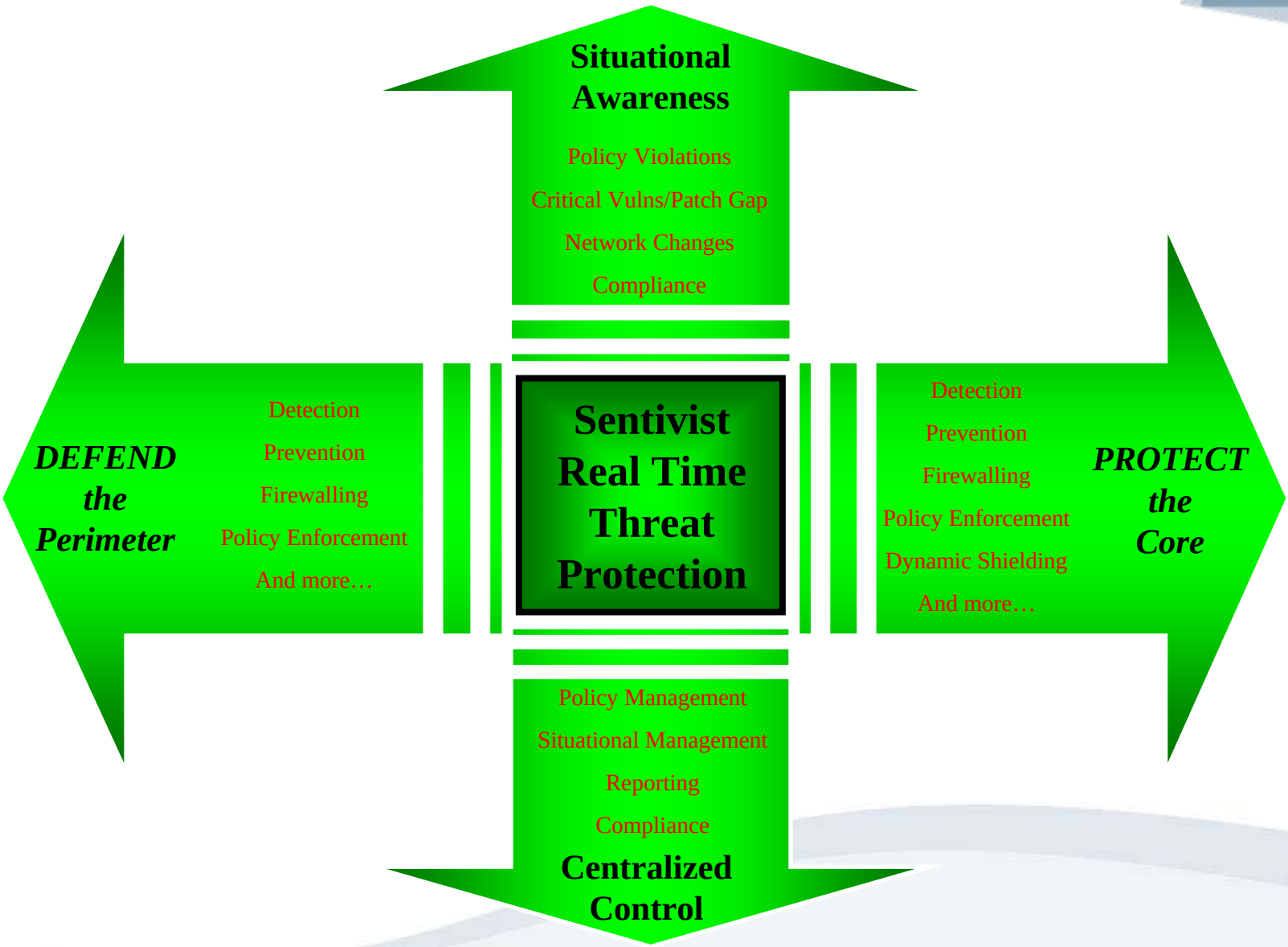


# The Network Security Challenge

# Sentivist Real Time Threat Protection



# Sentivist Real Time Threat Protection

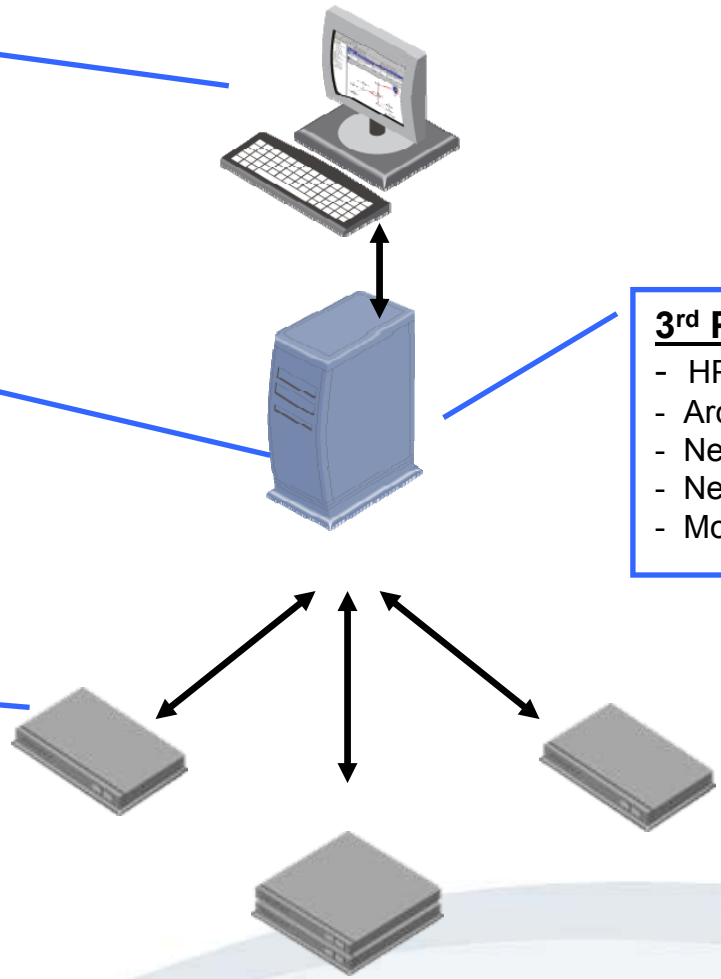


# IPS-1 Architecture

**IPS-1 Management Dashboard**
- Centralized Management
- Real Time Views
- Advanced Forensics
- Reporting and Compliance

**IPS-1 Management Server**
- Optimized Data Store
- Multi-Element Correlation
- Dynamic Shielding

**IPS-1 Sensor**
- Hybrid Detection Engine
- Confidence Indexing
- Open signature language
- Multi-mode prevention appliance with Failover



**3rd Party Integration**
- HP OpenView
- Arcsite, Intellitactics
- Netforensics
- Nessus
- More…