



# TRIPWIRE ENTERPRISE

SINGLE-POINT ENTERPRISE CONFIGURATION AUDITING AND CONTROL

2007. 08. Today Systems. Co., Ltd.

TODAY  
SYSTEMS

## 제품 개요

## 공급사 소개

### ■ TRIPWIRE Inc.

- 보안 컨설턴트이자 Purdue University의 Dr. Eugene Spafford과 Dr. Gene Kim에 의해 1992년에 최초 공개된 공개용 버전의 유닉스 보안 툴 “Tripwire”에서부터 출발
- 전 세계적으로 250000건 이상의 실 사용처가 존재하는 공개용 소프트웨어에 기반하여 1997년 회사 설립
- Data Center용 대용량 형상 감사 제품 전문 기업으로 제품 기능 확장
- 2002년 ‘Computer World’ 선정, ‘주목할만한 100대 기업’ 중 20위
- 2007년 “Business Journal” 선정, ‘급성장하는 100대 기업’ 중 29위
- 한국인 CTO에 의한 2Byte 문화 권에 대한 배려

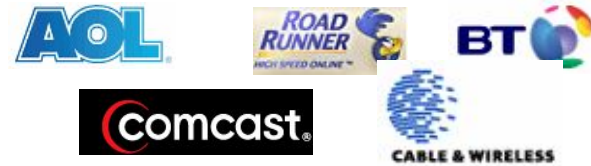
# TRIPWIRE의 고객들

- 전 세계 5500여 개 이상의 고객 확보

## Financial Services



## Communications



## Manufacturing



## Government



## Retail & Hospitality



## Education



# 파트너



## “형상 감사”란 무엇인가?

- 가트너 그룹에서는 변경, 형상관리 정책을 실제 IT 업무 환경에 성공적으로 적용하고 지속적으로 유지하기 위해서는 반드시 변경,형상관리업무에 **형상감사 (Configuration Auditing) 업무**가 동반되어야 한다고 정의합니다.
- EMA(Enterprise Management Associates)에서는 "Configuration Audit & Control" 업무가 구성(형상)관리나 변경관리와는 별개의 업무로 정의하고 있습니다.
- EMA에서는 형상 감사, 변경관리, 구성(형상)관리 각각을 다음과 같이 정의합니다.
  - **Configuration Management**: IT infrastructure에 변경을 가하기 위한 프로세스. 새로운 릴리즈에 대한 배포, 패치, 소프트웨어 구성 업데이트 등이 해당됨.
  - **Change management**: Configuration Management에서 사용될 변경 그 자체를 관리하기 위한 업무 절차/승인절차. 일반적으로 변경 요청이 접수되어 변경 스케줄이 짜여지며, 해당 리소스를 식별하고 변경하여 IT infrastructure에서 사용될 컴퍼넌트에 최종 반영될 때까지의 절차를 관리
  - **Configuration Audit & Control**: 타 시스템과는 독립적으로 존재하며 어떠한 변경이 조직에서 의도하는 변경과 구성 정책에 위배되지 않았음을 보증할 수 있는 기능을 제공

## 왜 "형상감사"가 필요한가?

- 사후 관리의 부재
  - 기존의 형상관리 시스템을 도입한 공공기관, 기업들의 대부분이 형상관리 업무에 의해 운영 시스템으로 넘겨진 변경 내역에 대한 지속적인 모니터링 부재
  - 형식적인 형상관리 업무 수행에 따른 형상관리 대상과 운영환경 간의 차이 발생을 미연에 방지
- 표준 시스템 운영에 의한 업무 효율 증대
  - 다수의 운영 시스템을 관리하여야 할 경우, 운영 표준 시스템과 나머지 운영 시스템과의 차이를 지속적으로 모니터링 함으로써 문제 발생에 대해 신속한 원인 파악 및 복구 가능
- 내/외부 감사에 대한 신속 대응
  - 각종 내/외부의 IT 감사(ex. 금감원 내부거래 감사, SOX 감사 등)용 표준 보고 대응 가능
  - IIA(내부감사협회) & ISACA(정보 시스템 감사협회)의 IT 감사
  - 금감원 내부거래 감사법 (K-SOX)
  - PCI DSS(Payment Card Industry Data Security Standard) 표준 (Visa-Master 카드 표준) 감사

# 기업 IT 환경에 대한 전문가 분석

“IT에 투자되는 10달러 중 8달러는 단지 쓰기 위한 죽은 돈일 뿐이다.”

Gartner

“현장에서 발생하는 이슈 중 80%는 사람과 허술한 프로세스에 기인한다.”

Gartner

“IT 리스크 중 가장 타격이 큰 것은 엉뚱한 실수와 실무와는 동떨어진 엉뚱하고 잘못된 변경절차이다.”

FORRESTER

“가트너 그룹은 2008년까지 CMDB 프로젝트의 75%가 실패할 것이라고 전망했다.”

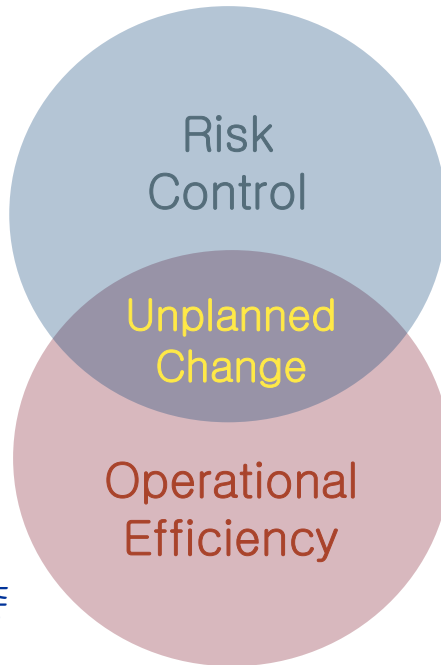
Gartner

“변경과 관련된 이슈는 IT감사 중 가장 중요한 3대 이슈 중 하나이다.”

protiviti

“조직이 당면한 중대한 과제는 테스트, 리포트, 통제 등의 감사 기능이 충분히 갖춰지지 않은 데에서 오는 내부 보안 위협을 해결하는 것이다.”

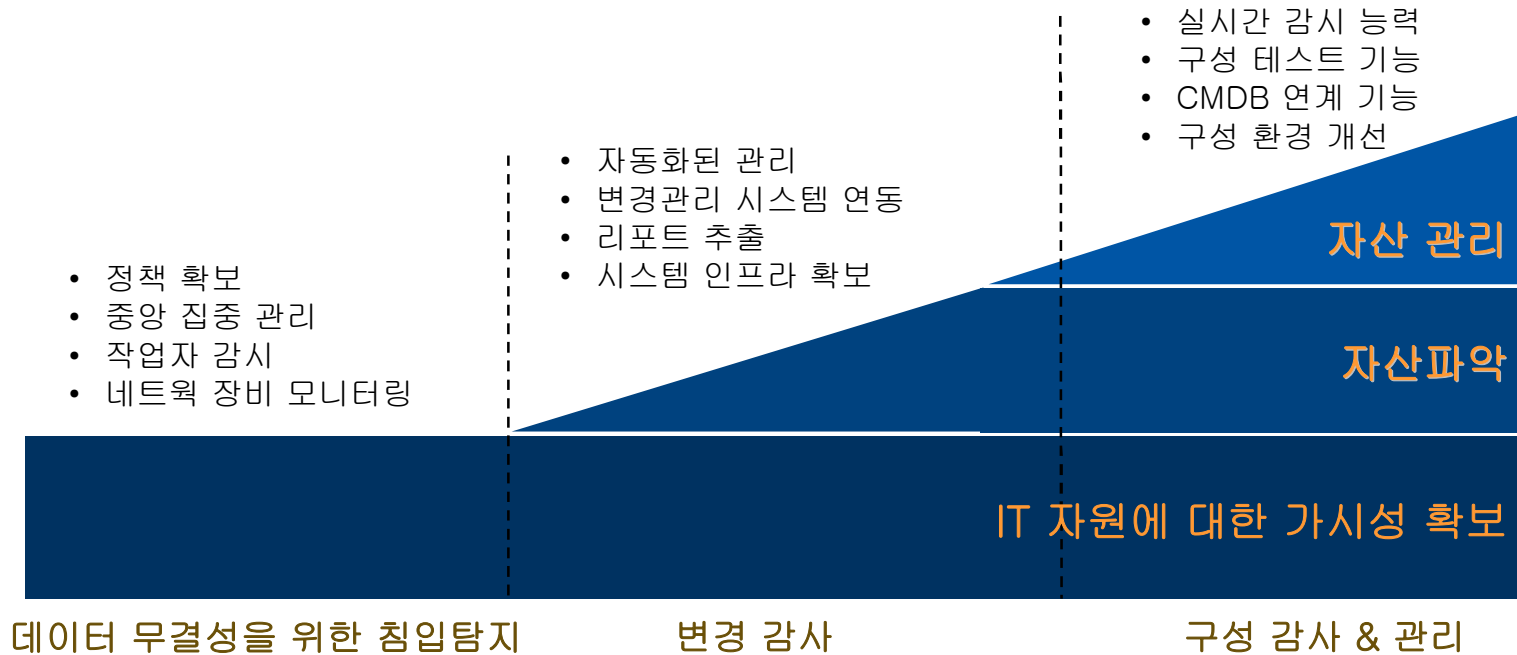
IDC



# TRIPWIRE ENTERPRISE 7

## Real-time Configuration Control Solution

- 데이터 센터 전반에 걸쳐 IT 자산의 전사적 실시간 감시, 구성관리, 리포트 기능 제공
  - Network devices, server, desktop, directory server, database, application 등



## 왜 TRIPWIRE ENTERPRISE 7인가?

- Tripwire Enterprise 7은 데이터 센터 전반에 걸쳐 지속적이고 실질적인 규제와 보안 통제를 제공합니다.
- Tripwire Enterprise의 형상감사 기능은 IT infrastructure의 구성 설정에 대한 평가 및 유효성 검사와 함께 구성 변경에 대한 탐지, 임의 구성 변경의 제재 등의 기능을 실시간으로 사전에 정의된 정책에 따라 자동적으로 수행합니다.
- Tripwire Enterprise 7은 구성 설정에 대한 평가 및 변경 탐지 기능을 동시에 수행할 수 있는 최초의 솔루션입니다.
  - 조직이 IT Infrastructure의 구성에 대해 신뢰할 수 있고 통제 가능한 상황을 확보
  - IT Infrastructure 조직 전체의 위험요소 감소
  - IT Infrastructure 내에 업계 표준 및 자체 표준 품질관리 정책을 손쉽게 반영 가능함
  - IT Infrastructure 내의 업무 효율성을 위한 프로세스의 자동화
  - 다양한 리포트를 통해 일관되고 효과적인 방식으로 각종 감사 및 보고에 대응 가능
  - 업무 현장(현업)에 대한 서비스 질 향상

# 도입 효과

리스크  
관리

- 비 인가된 변경에 대한 탐지
- 정책 타당성 테스트
- 자동화된 감사 리포트 제공

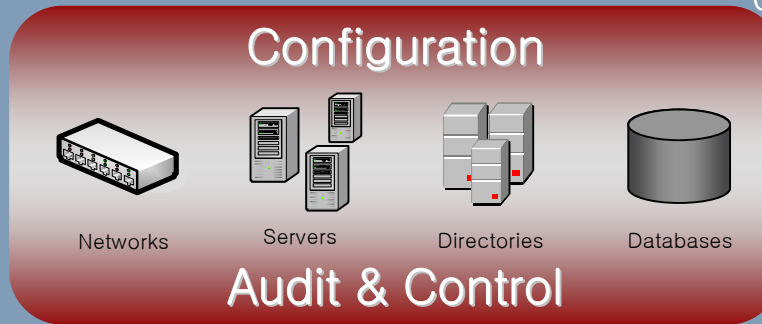
Compliance & Security

위험 감소  
& 비용 경감

- 정확성 & 타당성에 대한 보증
- 변경 내역 & 이력 제공
- 변경에 대한 신속한 수용성

CMDB

ITSM/ITIL Projects  
에 대한 신속한 투자  
비용 회수



서비스 중단율  
감소 & 신속한  
복구

계획되지 않은 작  
업량 감소

운영  
효율성

Availability

- 비정상 변경에 대한 알림 기능
- Root 권한 획득 모니터링
- 정확한 오류 정보 제공

Change/Configuration Automation

- 변경 복구
- 해킹 위험 감소
- 통제 & 가시성 향상

## 도입 효과 (계속)

### ▪ Compliance & Security

- 자동화된 감사, 테스트, 리포트 기능 제공
- 저 비용 & 고 가용성
- IIA(내부감사협회) & ISACA(정보 시스템 감사협회)의 IT 감사에 대응하는 리포트 제공

### ▪ Availability

- **15-50%**의 시스템 가용성 향상 효과
- **10-50%**의 MTTR(평균 시스템 수리 시간) 감소 효과
- 정확한 오류 정보 제공에 의한 확실한 오류 수정 기회 제공

### ▪ Change & Configuration Automation

- **10-80%**의 비인가 작업 비율 감소 효과
- 확실한 변경관리에 대한 보증

### ▪ CMDB

- ITSM/BSM/ITIL projects에 대한 업무 효율성 향상
- 시스템 구성 오류 방지
- 규정에 근거한 시스템 변경에 대한 보장

## 제품 상세 소개

# 적용 대상

실시간 감시  
정량적이고 효율적인 정보 제공  
10,000개 이상의 구성/정책 룰 제공  
자동화된 베이스라인 관리  
다양한 EMS와의 실시간 연동 가능

## Databases

- Oracle 9i & 10g
- SQL Server

## Servers

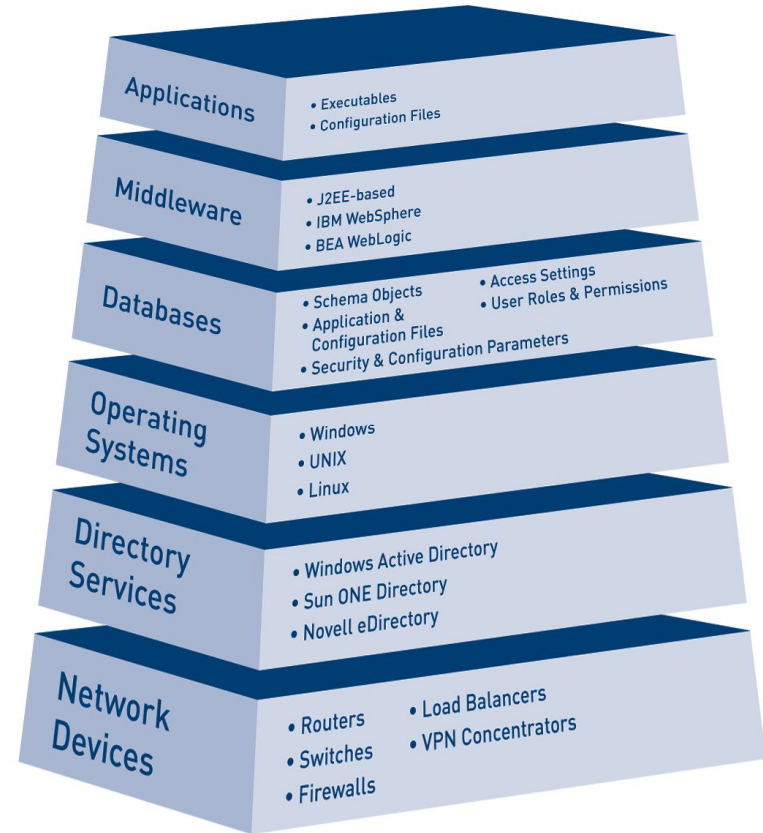
- AIX
- HP-UX
- Red Hat Enterprise Linux
- SUSE Linux

## Network Devices

- Alcatel OmniSwitch
- Cisco IOS, CatOS & PIX OS
- Cisco VPN 3000 Series
- Cisco Catalyst 1900/2820
- Check Point (Nokia IPSO)
- Extreme
- F5 BigIP
- Foundry

## Directory Services

- Solaris Sun One Directory
- Windows Active Directory
- Novell eDirectory
  
- Windows 2000 Server
- Windows 2003 Server
- Solaris (SPARC)
- Solaris (x86)
  
- HP ProCurve Series
- ISS (Nokia IPSO)
- Juniper M/T Series
- Marconi ForeThought
- NetScreen
- Nokia IPSO OS
- Nortel Alteon & Passport
- POSIX-compliant appliances



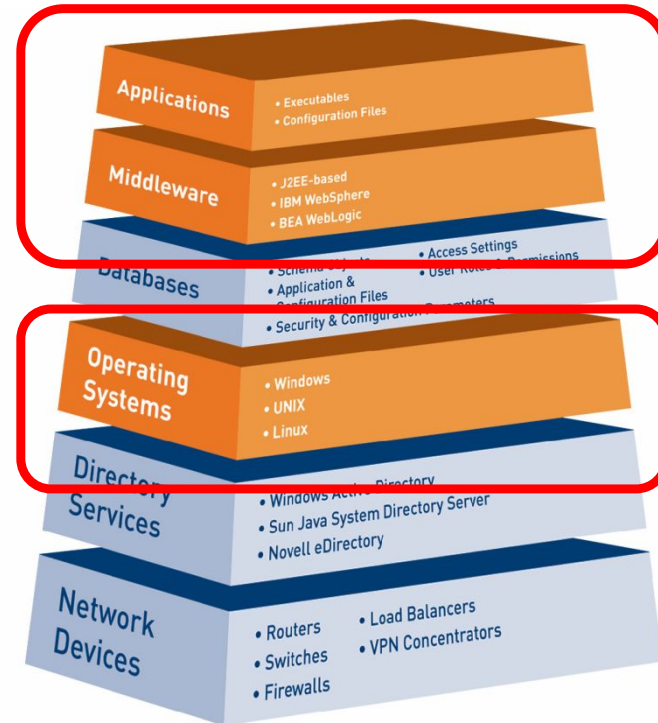
## EMS Integrations

- HP Service Desk
- HP Network Node Manager
- Remedy AR System
- Open Web Services API

## 적용 대상 (계속)

### ■ File Server & Desktop

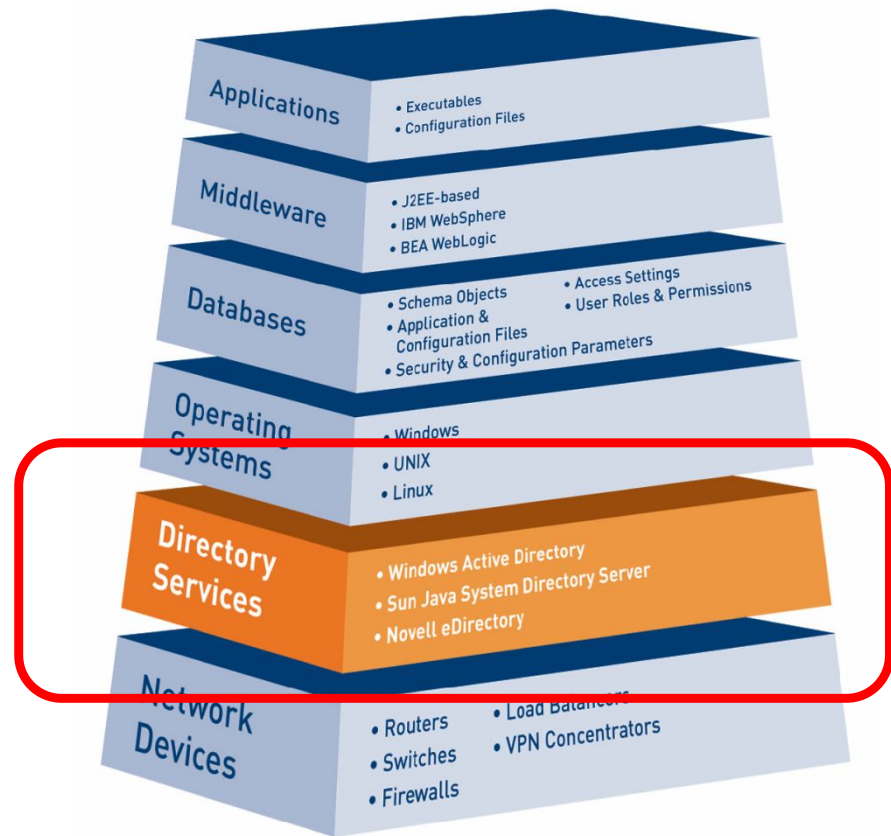
- File system 내에서 일어나는 모든 변경 사항에 대해 실시간 모니터링합니다.
- 감사 대상
  - OS 별 파일 시스템 내에서 일어나는 모든 변경
- 적용 대상 플랫폼
  - Solaris (SPARC) 8, 9 & 10
  - Solaris (x86) 10
  - Windows NT 4.0
  - Windows 2000 Server
  - Windows Server 2003 (incl. x64 Editions)
  - Windows XP Professional
  - Windows 2000 Professional
  - HP-UX 11.0, 11i v1 & 11i v2
  - AIX 5.1, 5.2 & 5.3
  - Red Hat Enterprise Linux 2.1, 3 & 4 AS, ES &
  - Red Hat Desktop Linux 3 & 4
  - SUSE LINUX Enterprise Server 9
  - CentOS 4.2
  - Fedora Core 2



## 적용 대상 (계속)

### ▪ Directory Servers

- LDAP 혹은 그에 호환되는 디렉토리 서버에 대한 독립적인 형상 감사를 제공합니다.
- 감사 대상
  - LDAP Schema
  - Password 설정
  - User Permission 설정
  - Network 리소스
  - 그룹 업데이트
  - 보안 정책
- 적용 대상 플랫폼
  - Windows Active Directory
  - Sun Java System Directory Server
  - Novell eDirectory



## 적용 대상 (계속)

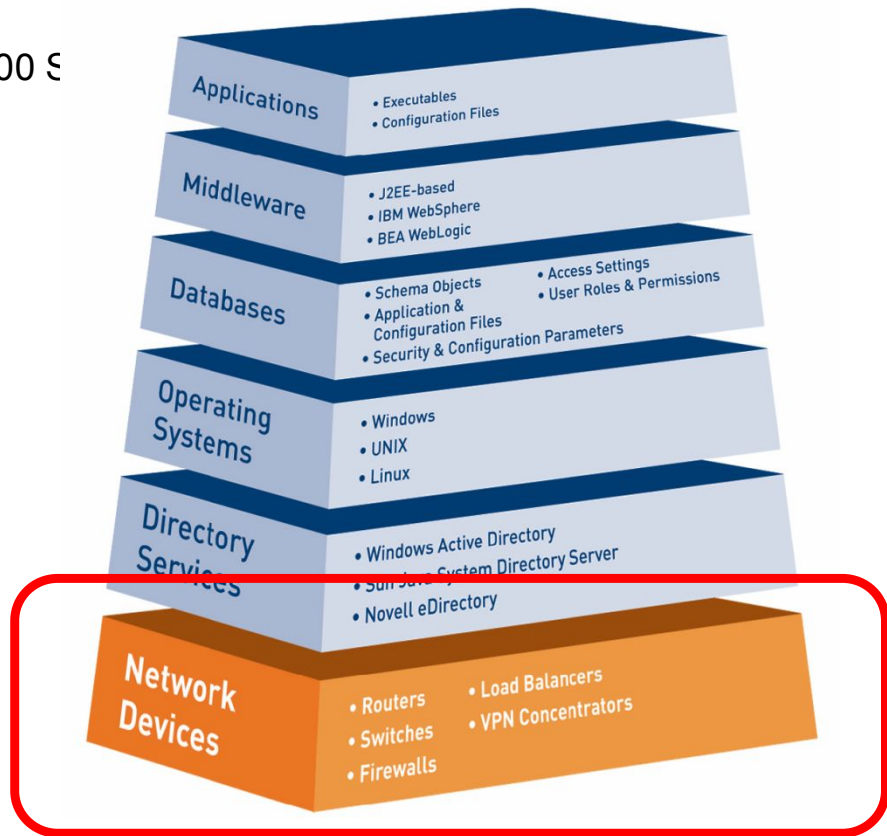
### ▪ Network Devices

- 네트워크 디바이스 중 스위치, 라우터, 방화벽, VPN 서비스 등에서 SNMP 등을 통해 제공하는 설정/환경 정보에 대한 변경을 모니터링합니다.

- POSIX 호환의 OS 기반의 어떤 장비도 호환 가능

### • 적용 대상 장비

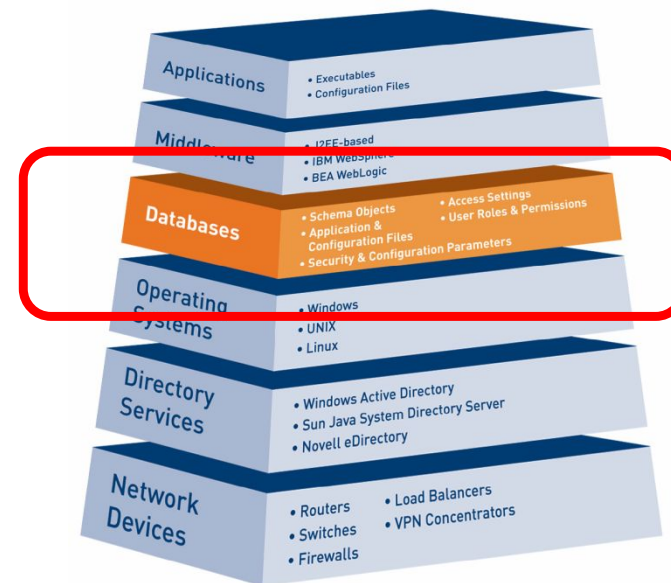
- Cisco IOS, CatOS & PIX OS , VPN 3000 E
- Cisco Catalyst 1900/2820 Switch
- Alcatel OmniSwitch 6xxx/7xxx/8xxx
- Check Point Nokia IPSO Systems
- Extreme
- F5 BigIP
- Foundry
- HP ProCurve Series
- ISS Nokia IPSO Systems
- Juniper M/T Series
- Marconi ForeThought
- NetScreen
- Nokia IPSO OS
- Nortel Alteon & Passport
- POSIX-compliant operating systems



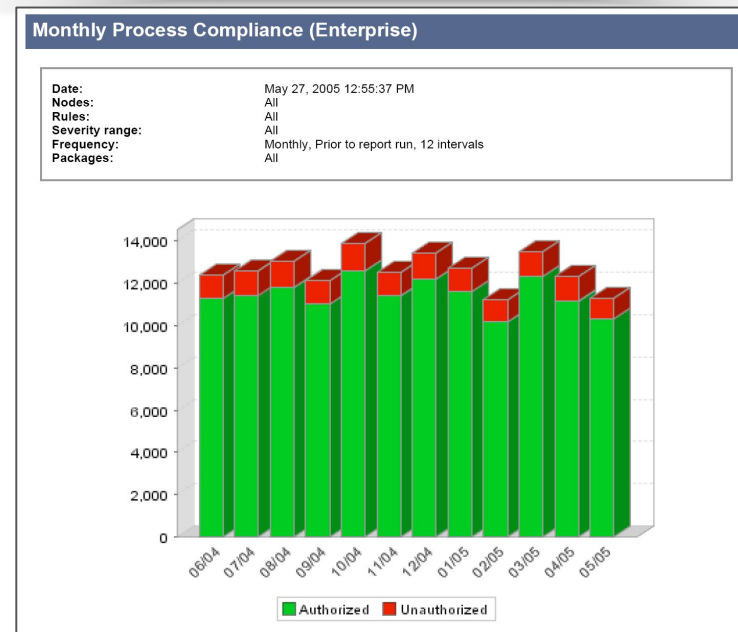
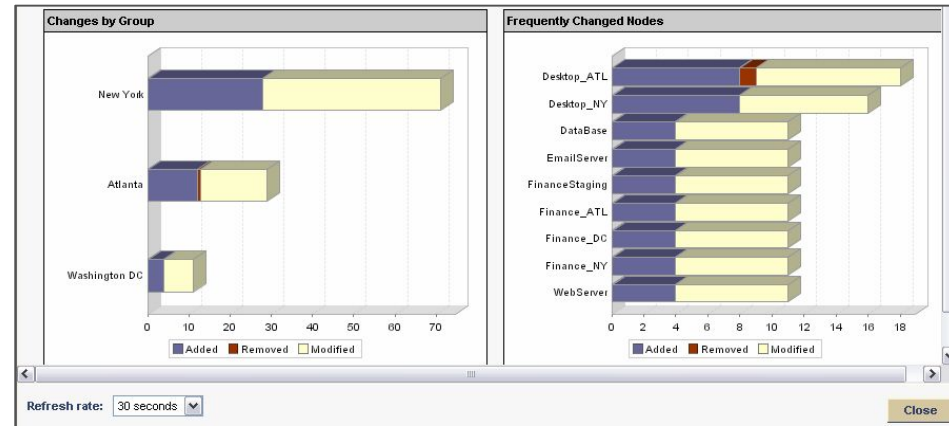
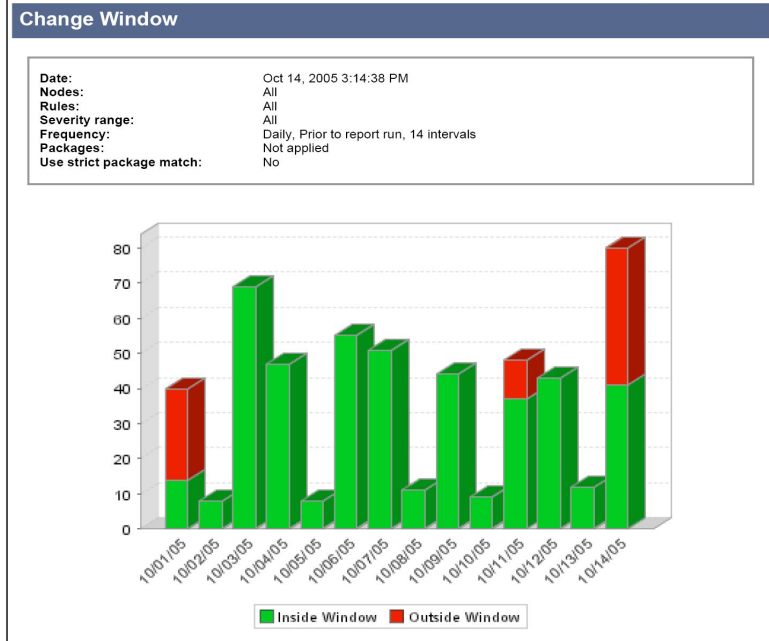
# 적용 대상 (계속)

## Database

- Tripwire가 지원하는 Database (Oracle, MS-SQL) 내의 거의 모든 정보의 변화를 모니터링 합니다.
- 감사 대상
  - Oracle Object(Function, Index, Procedure, Table, Trigger, View, Package, Sequence, Stored outline, Synonym, Type, Library, Database Link, Cluster, Directory, Table space, System Privilege, Object Privilege, Audit Parameter, User, Profile, Role 등)
  - SQL Server Object(Table, Index, Trigger, View, Stored Procedure, Function, User-defined type, Configuration Parameter, Database, Login, Server Role, Database User, Database Role 등)
- 적용 대상
  - Oracle 9i & 10g
  - Microsoft SQL Server 2000 & 2005



# REPORT



- 대쉬보드 기능 제공
- 각 항목에 대한 상세 리포트 제공
- 고객 환경 및 조직에 맞는 논리적 그룹에 의한 리포트 기능 제공

# REPORT (계속)

## Report library

변경 정책  
상세 변경 내역  
변경 프로세스 metrics  
변경 이력

## Online dashboards

웹 기반 리포트 제공  
순차적 상세 리포트 제공

## Capabilities include:

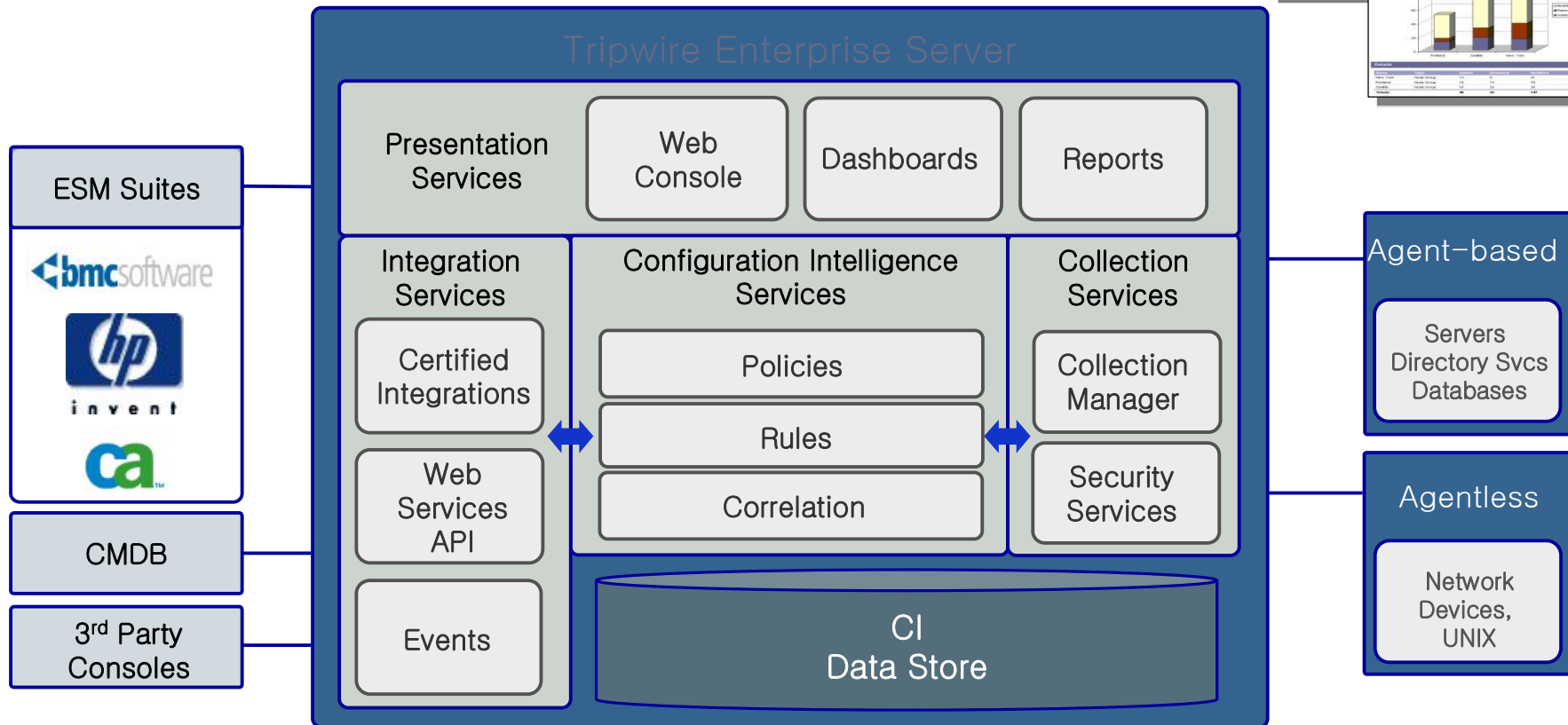
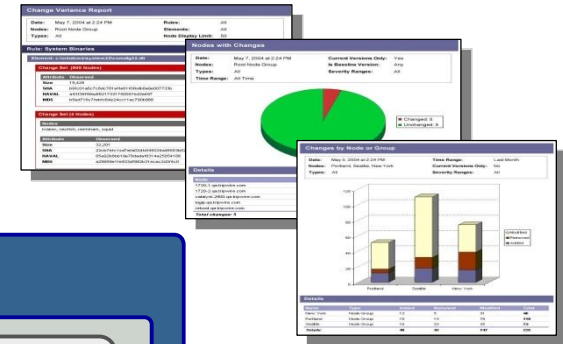
최적화된 조건 및 카테고리  
작업 스케줄 관리  
기간 별 리포트  
Archive Storage  
HTML, XML, PDF 포맷의 리포트 결과 제공



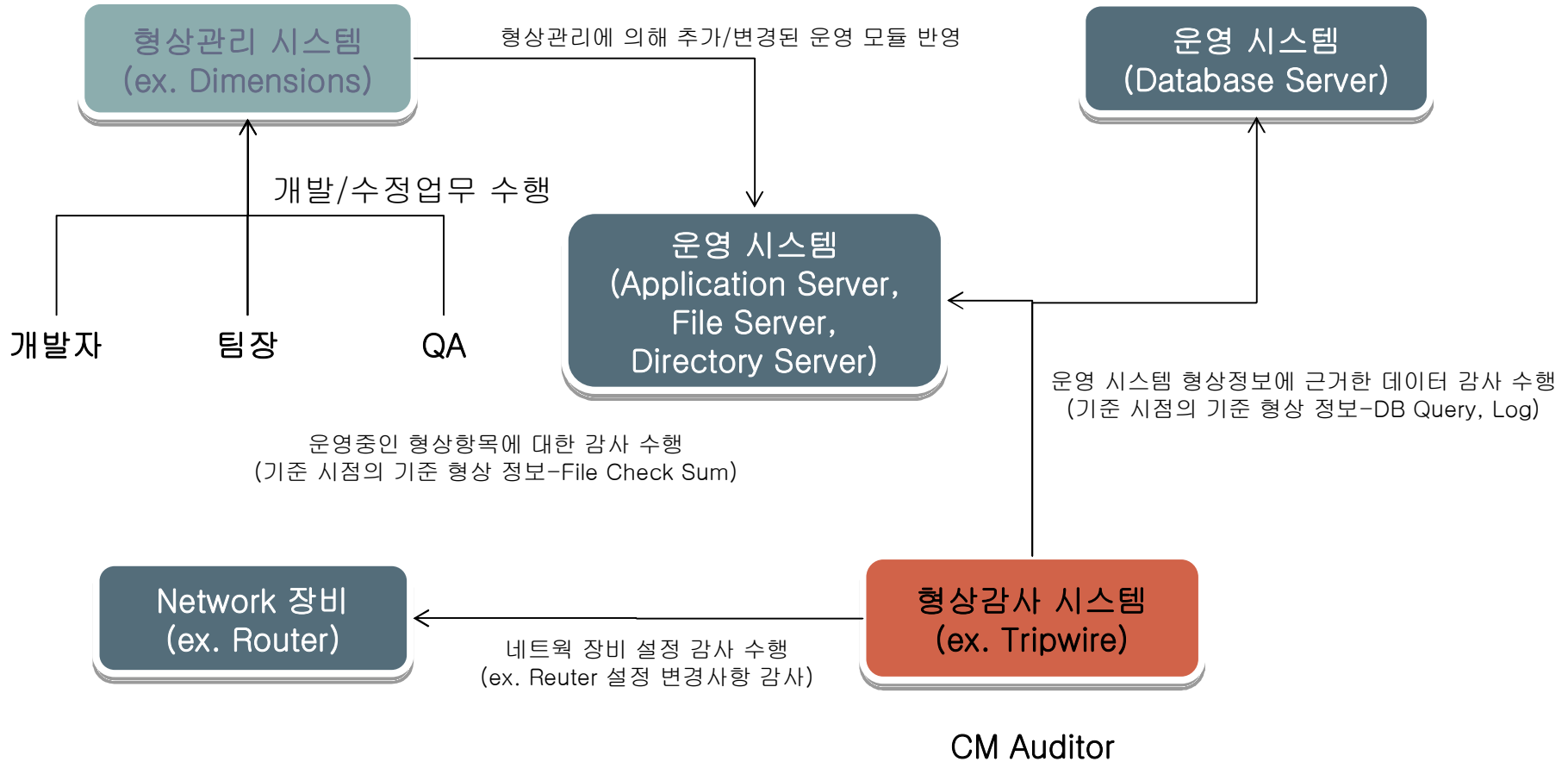
# REPORT 종류

- 기본 제공 Report
  - Baseline Elements , Change Process Compliance
  - Change Rate, Change Variance, Change Window, Changed Elements
  - Changes by Node or Node Group, Changes by Severity, Detailed Changes
  - Device Inventory, Elements
  - Frequently Changed Elements, Frequently Changed Nodes
  - Inventory Changes, Last Node Check Status, Missing Elements, Monitoring Policy
  - Nodes with Changes, Reference Node Variance, System Access Control
  - System Log, Unchanged Elements, User Roles
- 추가 Report
  - Tripwire에서 지속적으로 업계 표준의 Report를 추가 개발하여 제공합니다.

# ARCHITECTURE



# 형상 관리/형상 감사 시스템 구성 예



## 고객 사례

# CLIENT CASE STUDY – 뉴욕 증권 거래소



KMDF 13.125 ^ 2.625 OCOB 60.8125 ^ 1.125 UHJZ 8.40 v 1.625 CAMP 47.1825 ^ .375 PTCU 22.4375 ^ .75 BINK 78.375 v 4.875 REIT 28.13 v  
DJI 10450.14 ^ 16.7 HKHS-X 14360 v 394.13 XCI 844.63 v 33.49 NYSE 625.15 ^ 1.72 SP-500 1241.23 v 7.05 XGLD 256.64 ^ 2.11 NIKI-X

## 문제점:

- 비 인가 작업에 의한 시스템 장애 및 업무 효율 저해
- 수작업으로 이루어지는 변경 기록은 단순히 기록일 뿐임

## Tripwire 적용 후:

- 모든 Production Server들에 대한 변경작업은 모니터링 되며 자동적으로 기록 됨
- 모든 변경작업은 담당자 작업 전에 검증이 이루어짐

## 장점:

- 시스템 변경작업 성공 율이 99.99% 증가
- 평균 수리 소요시간이 30분에서 12분으로 감소
- 생산력 향상에 따른 연간 비용 절감효과가 \$500K 이상
- 변경 통제 능력 보장에 의한 보안 및 변경 관리 능력향상

# CLIENT CASE STUDY- VISA PCI AUDIT



## 문제점:

- 매년 실시되는 Visa PCI, SOX, 개별 감사 준비에 따른 손실
- 전체 IT 자산에 대한 비인가 변경 내역을 감사하기 위한 인력, 비용 손실

## Tripwire 적용 후:

- Linux, Windows server들에 대해 Tripwire 탑재
- 모든 변경에 대한 감사 및 변경 작업 오류에 대한 신속한 복구 작업 가능

## 장점:

- 모든 Visa PCI and SOX audit 요구사항에 대한 충족 및 추가 정보 제공
- 내부 개발, 지속적인 시스템 감사, 시스템 변경 오류 가능성 제고에 대한 효율성 증가
- 시스템 중단 시간 감소에 따른 전체 시스템 가용성 증가
- “Tripwire가 우리의 어깨를 가볍게 해주었다.”

감사합니다.

*Today Systems*