

# COMPLIANCE ENGINE



- 1615 Introduction** — Shannon Simpson
- 1620 How to achieve and maintain compliance using COMPLIANCEngine** — Kevin Dowd
- 1635 The COMPLIANCEngine in action** — Gerry Lawrence, CTO, NetBenefit
- 1650 Demonstration of the COMPLIANCEngine Service Suite**  
Service overview— Martin Dipper  
Demonstration of Portal and CE — Paul Rose
- 1725 Questions and Wrap up**
- 1730 Bar Open**
- 1900 Bar Closes**

# COMPLIANCE ENGINE – KEVIN DOWD



# COMPLIANCEngine Concept

- One stop Compliance portal for Infosec
  - Compliance with Standards
  - Compliance with Internal Control Targets
  - Compliance with Regulatory Requirements
  
- Write Once, Read Many
  - One instance of each audit activity
  - Many outputs mapped to a central database
  
- Multiple inputs
  - Agents and Real Time Events
  - Consultant Input
  - IDS/IPS
  - “Live” view of compliance

# COMPLIANCEngine Phase 1

- Real Time Security = Priority
  
- Key customer challenges = Priority
  
- Therefore focus on
  - Agent-based and agentless build validation
  - Patch checking
  - Monitoring & Logging
  
- Consultant based input, read once/write many
  - In place via templates
  - Integrated with main CE at report level

# COMPLIANCEngine Future

- ❑ All inputs to an integrated portal
- ❑ Customer input of compliance controls & targets
- ❑ Reporting entirely through integrated portal
- ❑ Compliance alerting
  - ❑ E.g. PCI Req 2 out of compliance for infrastructure X, rather than server Y is out of build compliance

# COMPLIANCEngine Benefits

- We see the same issues all the time...
  - Difficulty in managing build standards
  - Difficulty in implementing monitoring and logging
  - Difficulty in patch reporting
  - Difficulty in demonstrating compliance
  
- COMPLIANCEngine solves all of these
  - Knowledge base removes research/resource issue
  - Service element removes staffing issues
  - Portal means demonstrable compliance
  
- Also – configurable! Service based!
  
- Can help with ANY compliance issue



# PCI Service Provider Compliance Engine in action

Gerry Lawrence

CTO

[gerry.lawrence@netbenefit.com](mailto:gerry.lawrence@netbenefit.com)

## Background

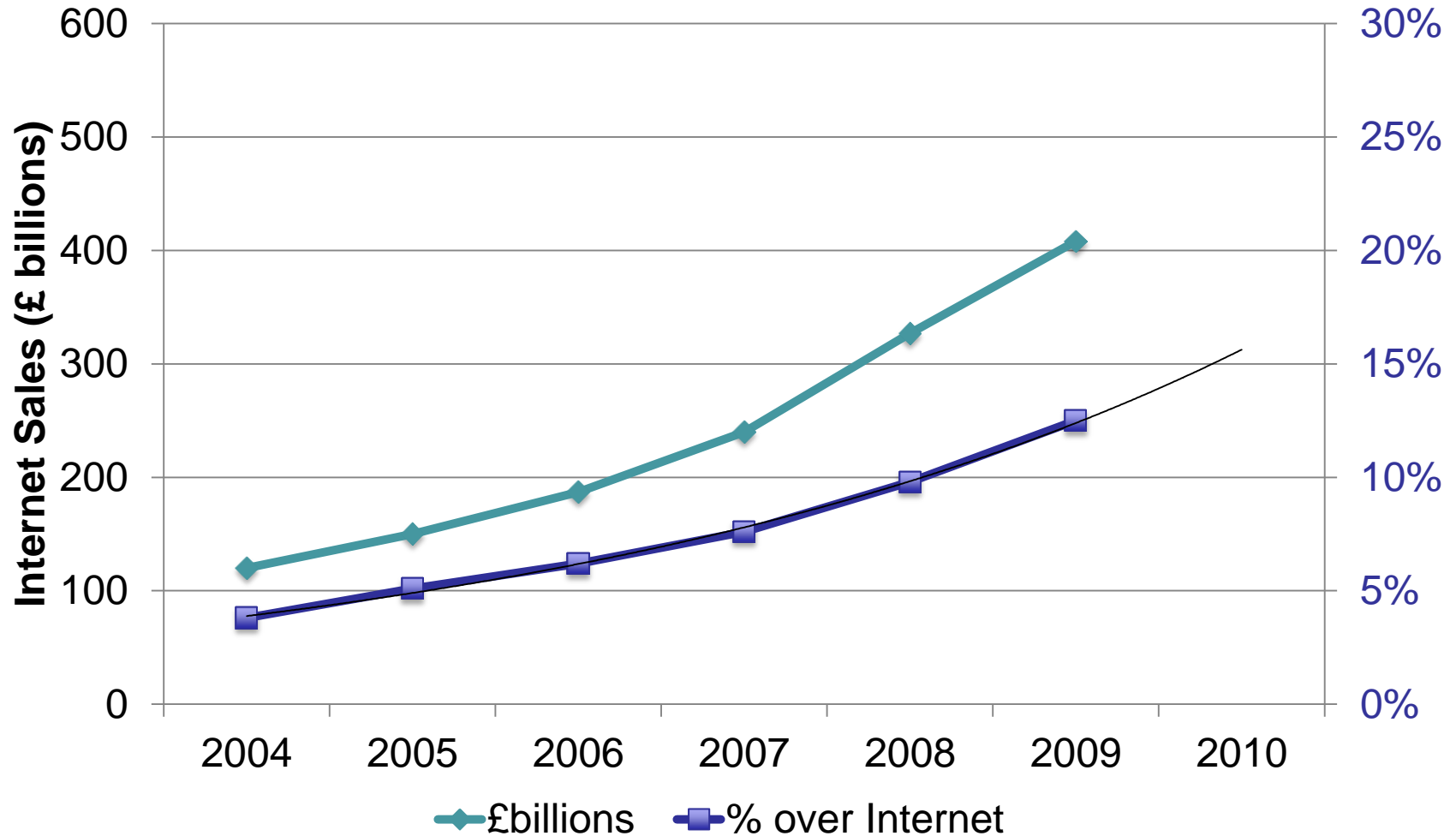
- ▶ Experts in business critical hosting
- ▶ Wide range of customers
- ▶ ...including many e-commerce sites



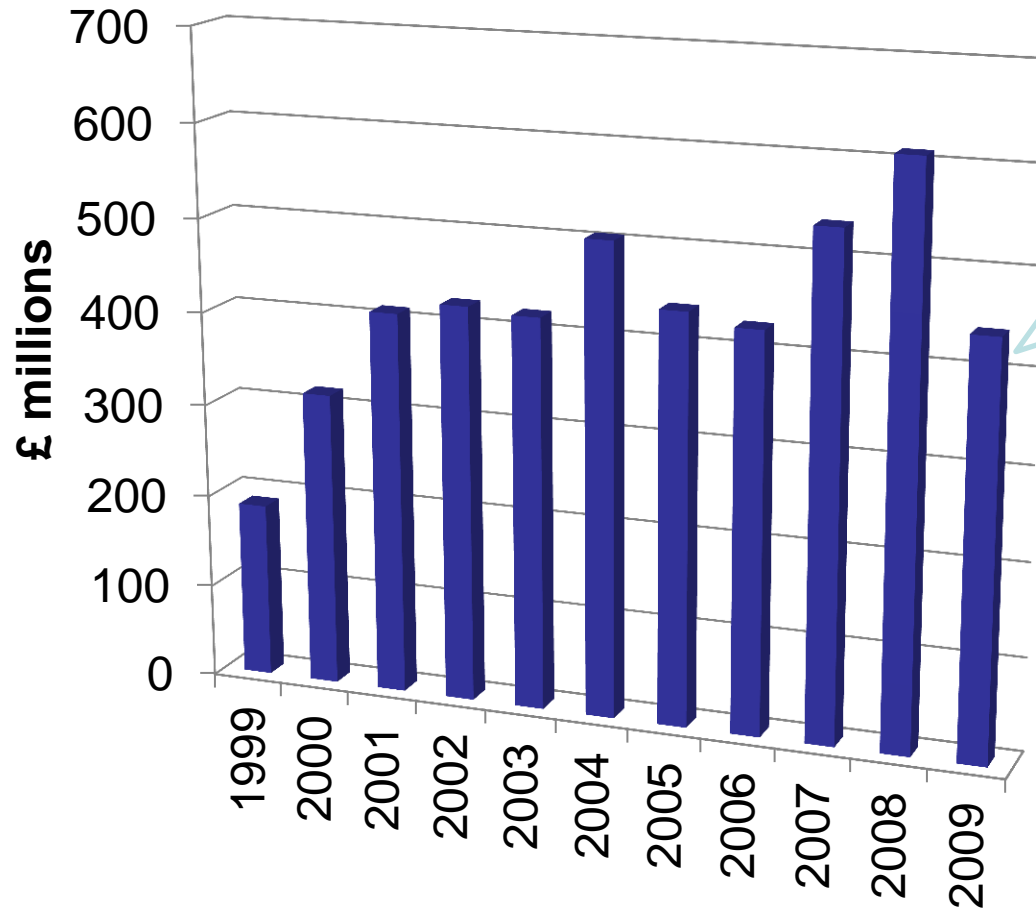
NEWSTATESMAN



## Growth of e-commerce



## Card fraud



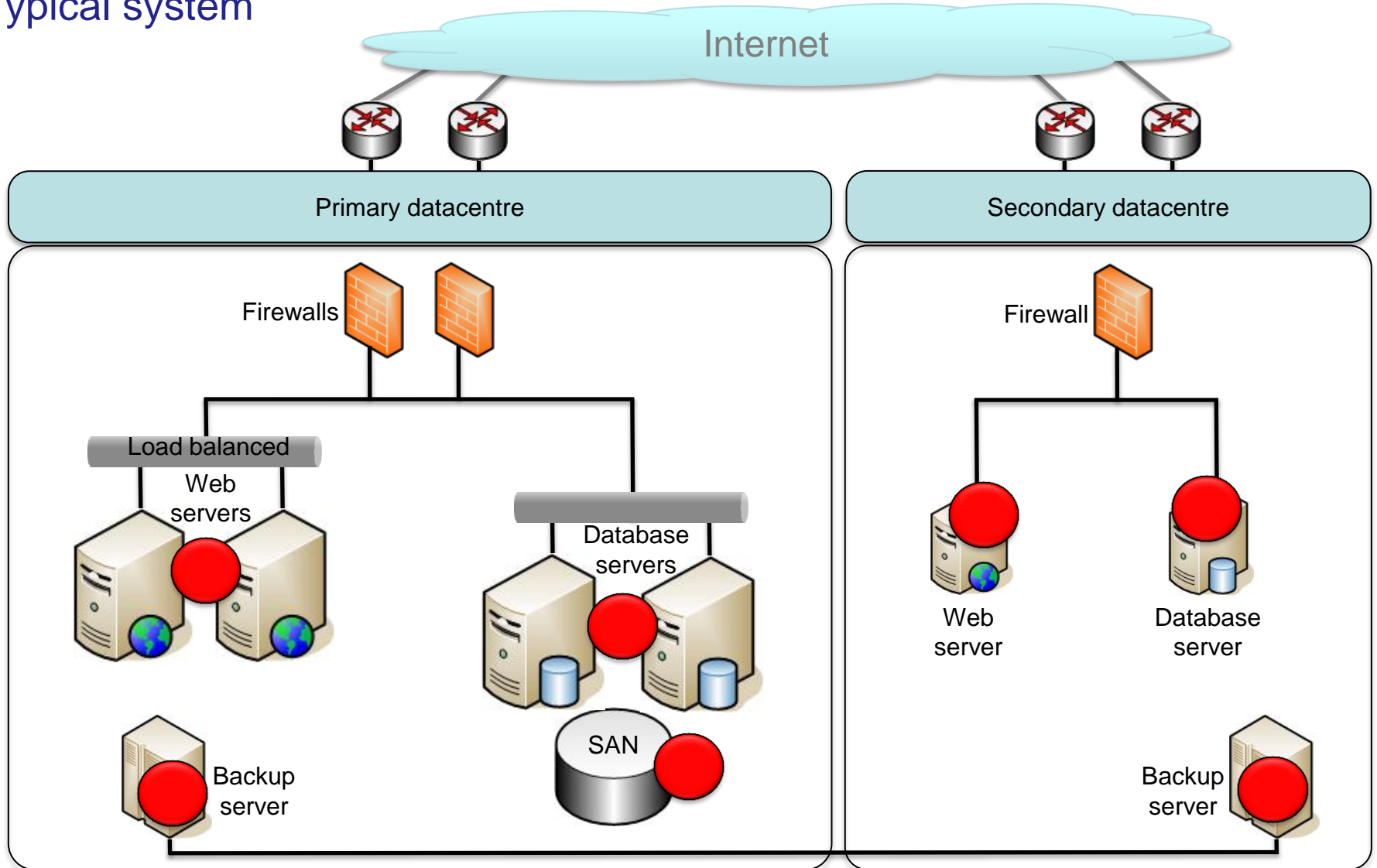
Reduction due to:

- Sophisticated fraud screening
- Cardholder authentication
- Awareness campaign
- PCI compliance improvements

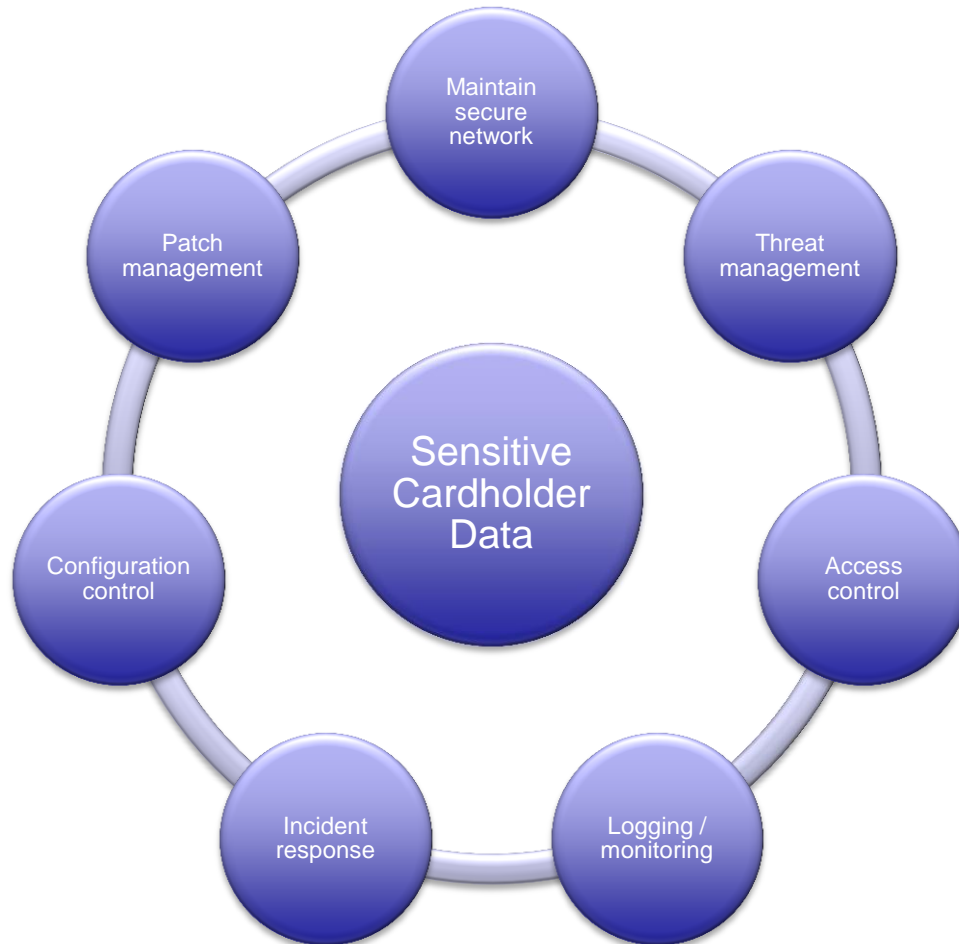
## PCI improvements

- ▶ PCI awareness increased
- ▶ PCI standards more organised, more specific and tougher
- ▶ Banks now following through on non-compliance

# Typical system



# Compliance responsibilities



## In-house or external resources

### Skills

- ▶ Deep understanding of the compliance and regulatory framework
- ▶ Secure network design
- ▶ Systems design
- ▶ Detailed log analysis
- ▶ Incident response

### Time/resource

- ▶ Many skills only needed some of the time
- ▶ Monitoring is **very** time consuming
- ▶ Monitoring needs to happen 24x7

## Choosing a partner

### Selection criteria:

- ▶ Security industry expertise to compliment our own
- ▶ Specific PCI compliance experience
- ▶ Pro-active 24 hour monitoring and response service
- ▶ Cultural fit and great attitude

Working together



# COMPLIANCE ENGINE – MARTIN DIPPER



# KEY Components

## THREATengine

Vulnerability & Exploit Lifecycle Management  
Discover, Monitor, Trend & Defend

## VALIDATIONengine

Build Validation Lifecycle Management  
Audit, Validate and Report

## PATCHengine

Patch Lifecycle Management  
Test, Assess & Manage

## CONFIGURATIONengine

Network Configuration Management  
Identify, Control & Review

## LOGengine

Security Incident & Event Management (SIEM)  
Open Log Management & Alerts  
Collect, Store and Search  
Real-time Compliance Monitoring

## LOGwatch

Log Inspection  
Incident Response & Escalation Service  
Service Desk Access

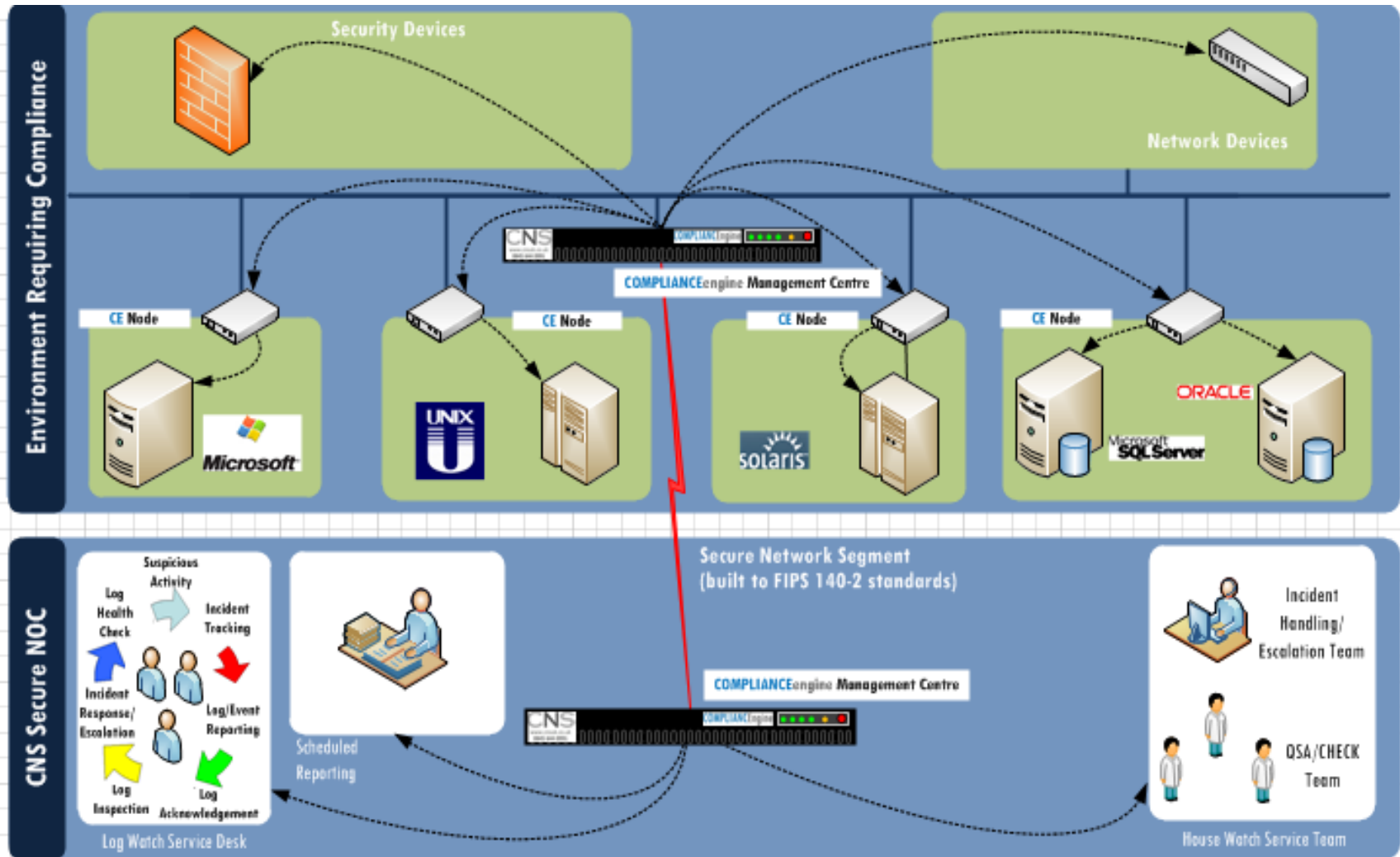
## HOUSEwatch

Professional Services  
Threat & Compliance Advisory

# COMPLIANCEngine Managed Service (LOGwatch)

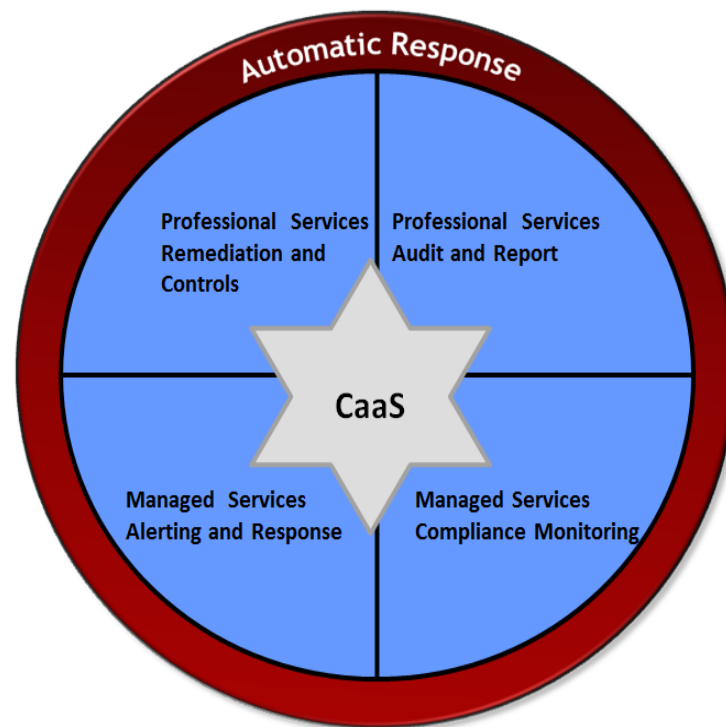
- Service setup and tuned during one month implementation period
- Customised alerting, ticket creation and response to events
- Alerts for all compliance violations and security incidents
- Supported by CNS Service Desk 24x7
- Alerting when scans/checks are due and when complete
- Central management portal for authorised users
- The service is deployed using two platforms, supplied and setup by CNS.
  - COMPLIANCEmgmtcentre— this contains the logging engine, administration, customer portal, service catalogue and rules engine, which defines the logging and alerting operation
  - COMPLIANCEnode — that can contain the Threat, Patch, Validation and Configuration functionality

# ARCHITECTURE OVERVIEW



# COMPLIANCE-as-a-SERVICE

- Compliance against baseline
- Infinitely customisable
- Centralised management portal
- Reduce cost of compliance
- No upfront capital expense
- Improve business continuity
- Lifecycle compliance monitoring
- Professional Services wrap-around
- Automated toolset
- 24 x7 Service



# COMPLIANCE ENGINE – PAUL ROSE



# DEMONSTRATION LAB

