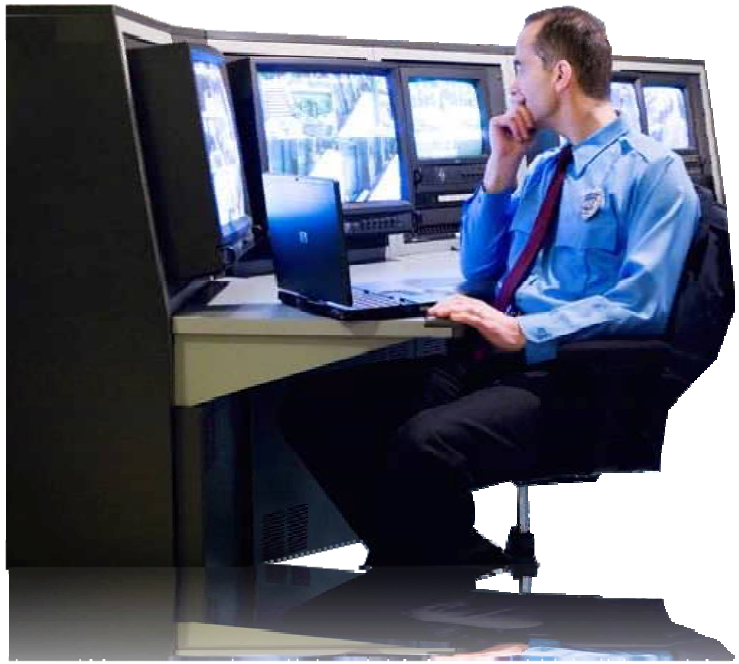

ProCurve Networking
HP Innovation

ProCurve Networking
HP Innovation

Unfortunately,
Security Issues are Here to Stay



- Vulnerabilities and incidents continue to rise
- The increasingly mobile workforce
- The costs to demonstrate business accountability continue to mount

Organizations Need to Take Control

ProCurve Networking
HP Innovation

Apply access rights and take control over network usage

Eliminate unwanted network traffic

Demonstrate regulatory compliance

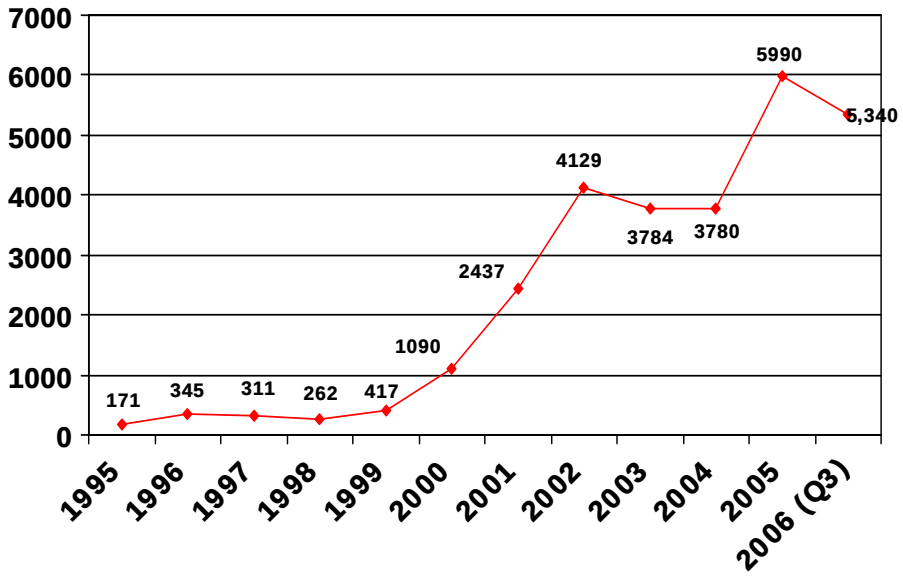
Solution needs to be

- Simple to deploy and to use
- Inherently secure and dependable
- Reliable
- Affordable

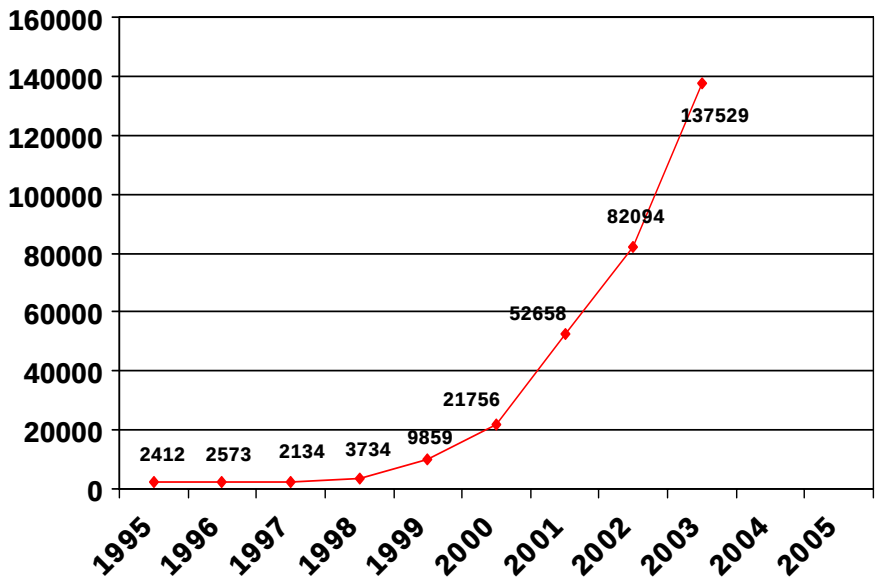
ProCurve Networking
HP Innovation

Exposure and Incidents are Increasing

Vulnerabilities Reported



Incidents Reported



Note: Incidents are no longer counted by CERT because they have become commonplace and simply counting them provides little information about the scope or impact of an attack.

Reference: http://www.cert.org/stats/cert_stats.html

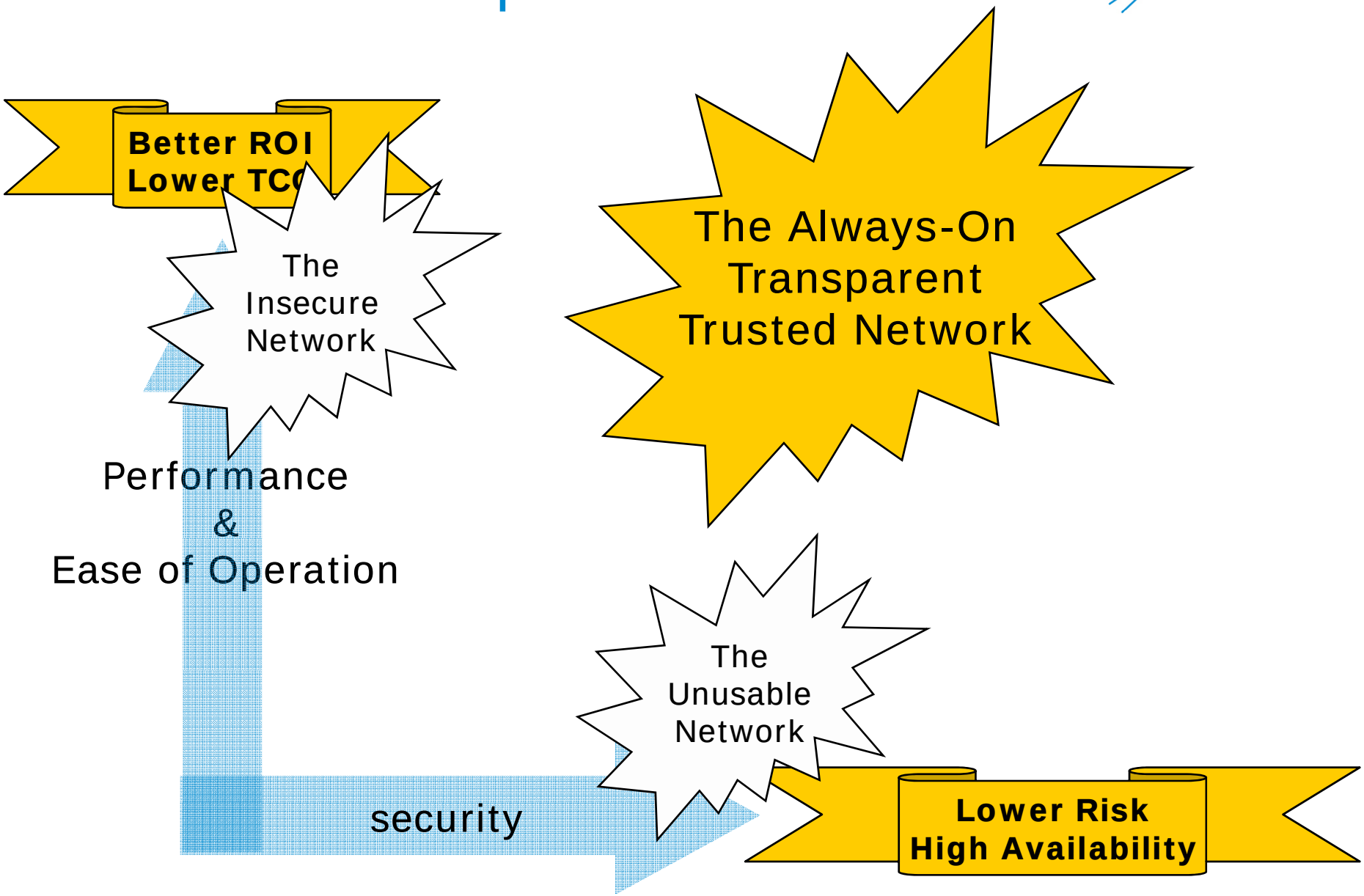
CSI/FBI Survey 2006
Businesses Under Attack

ProCurve Networking
HP Innovation

- **Frequency of attacks.** Over 62% of respondents experienced computer security incidents in a year's time; 24% of them indicated they had experienced 6 or more attacks
- **Financial impact.** More than 50% of reported losses were caused by viruses contamination and unauthorized access, accounting for $26 million in losses for 313 respondents.
- **Defenses.** Survey respondents use a variety of security products
  - 98% use Firewalls
  - 97% use Anti-virus software
- **Sources of the attacks.** Over 68% of respondents believe that “Inside jobs" account for some portion of losses.

The Great Compromise

ProCurve Networking
HP Innovation



Adaptive Process in Practice

ProCurve Networking
HP Innovation

Policies

Trusted Network
Infrastructure

Validation

Adaptive Networks must be:

- Adaptive to users
- Adaptive to applications
- Adaptive to organization needs

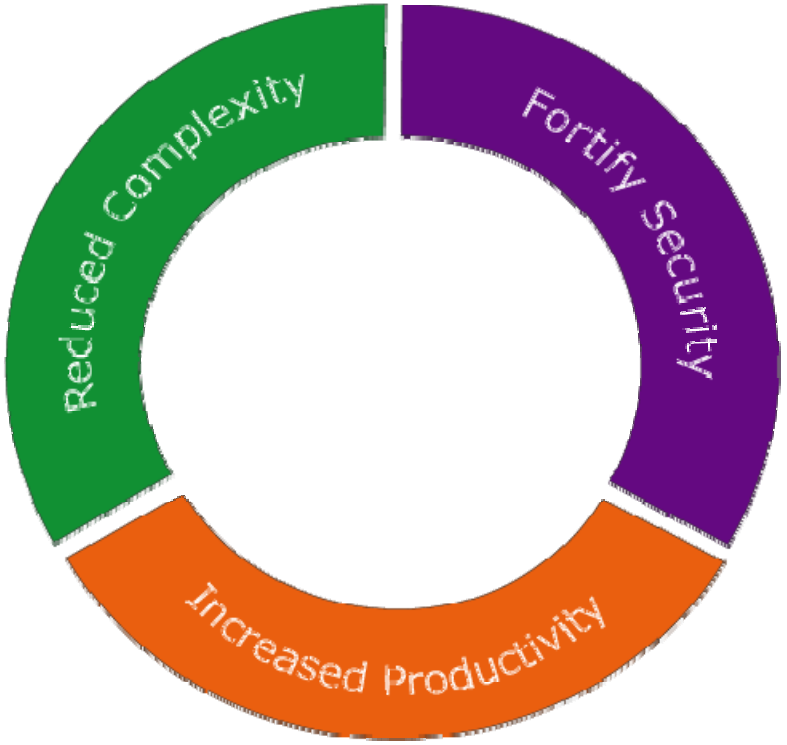
All on a cohesive, flexible network infrastructure that is highly secure and available

ProCurve Networking
HP Innovation

What is an Adaptive Network?

A cohesive, flexible network infrastructure that enables your organization to:

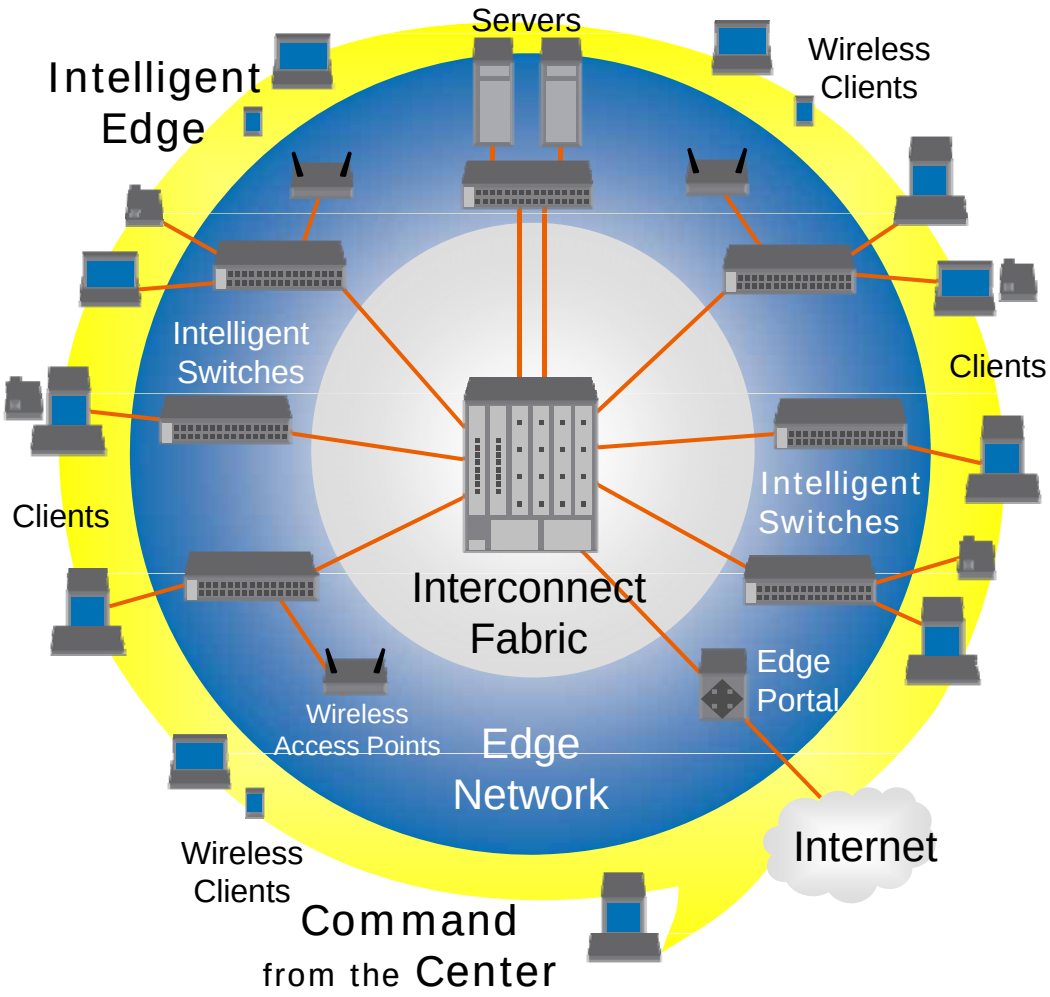
- Fortify security
- Increase productivity
- Reduce complexity



Adaptive EDGE Architecture

Network Design for the Future

- Control at the Edge
  - Authentication
  - Bandwidth shaping
  - Data prioritization
  - Advanced Routing
  - WLAN management
  - Deep packet inspection
  - Encryption
- Simple, high-bandwidth Interconnect Fabric
- Identity-driven, dynamic configuration



The Future of the EDGE

Every port holds an application hosting environment

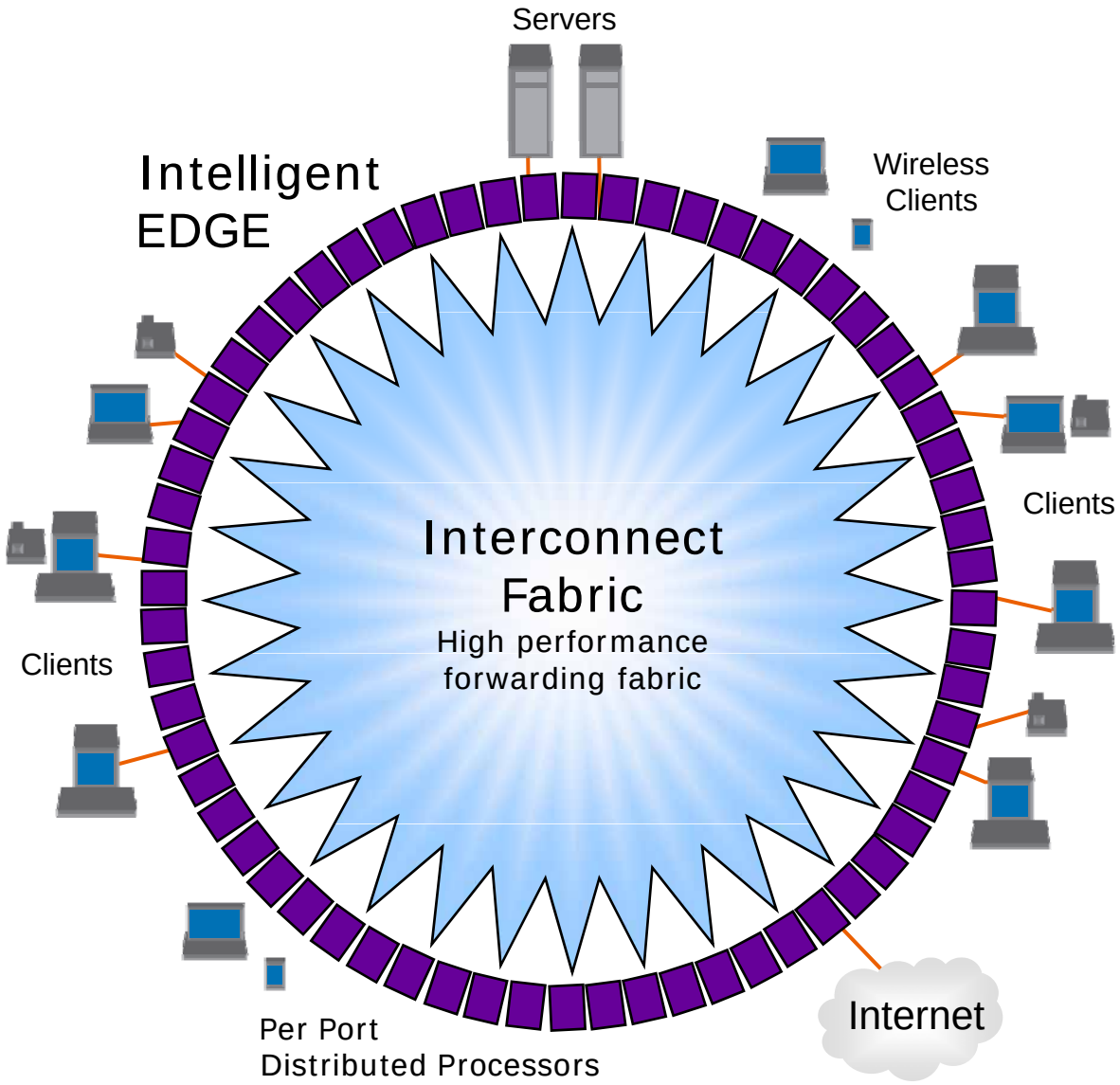
- ignitable client applications
- network and traffic services
- IDM launches designated services

Each port incorporates a rich set of network capabilities

- deep packet inspection
- load balancing
- caching
- encryption

Emerging distributed applications

- client integrity and inspection
- infection abatement
- advanced mobility
- advanced voice and media routing
- application load balancing



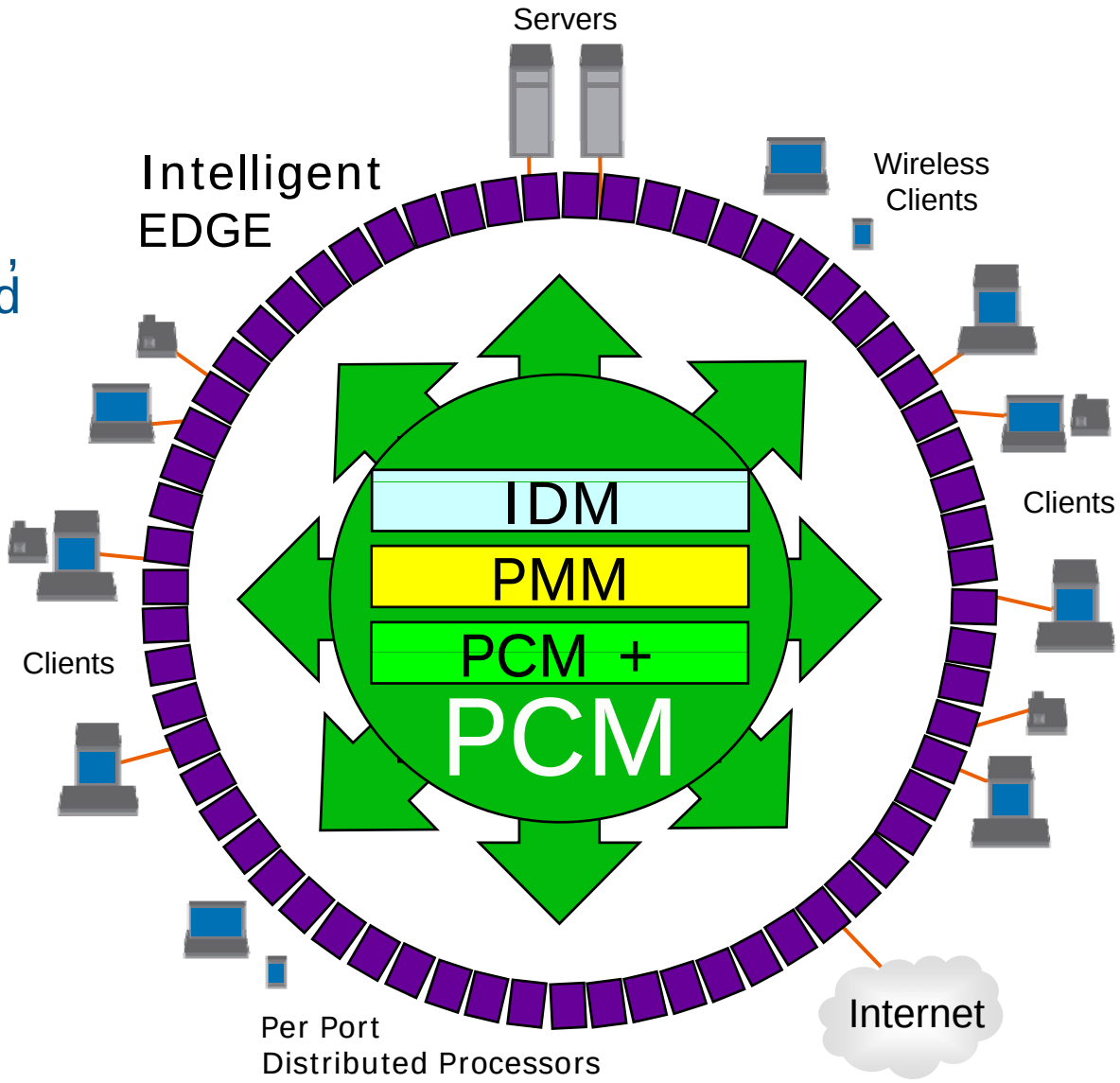
The future of Management

ProCurve Networking
HP Innovation

Add capabilities for advanced configuration, traffic management and automation

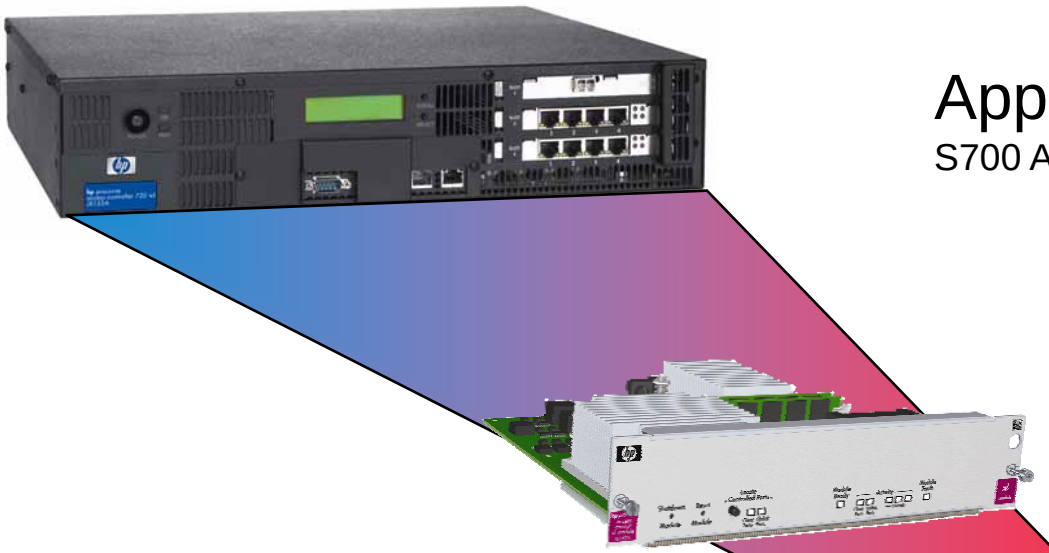
Integrate mobility management with the rest of your network infrastructure management

A fundamentally new methodology for managing dynamically loadable networks



Integration

ProCurve Networking
HP Innovation



Appliance

S700 Access Controller

Blade

xl Access Control Module

Built-In Hardware Software Ignitable

Next Generation ProVision ASICs

We currently detect the following:

ProCurve Networking
HP Innovation

- **Protocol Anomalies**
  - Port scanning techniques:
    - Xmas Tree Scan
    - NULL Scan
    - FIN Scan
  - Denial of Service:
    - UDP Bomb
    - Land Attack
    - Ping of Death
    - Fragmentation attacks
- **Reconnaissance before an attack**
  - Tools:
    - Nessus
    - NMAP
    - Ping
- **Network-based attacks**
  - Tested to detect:
    - DNS Tunneling
    - Unauthorized network mapping
    - IP Spoofing
    - Various worm propagation techniques
- **Anomalous packet size**
  - Designed to inform NI to:
    - Sample suspicious traffic
    - Detect some covert channels
- **Mis-configured devices**
  - Tested to detect:
    - Duplicate IPs
    - Rogue routers
    - Rogue proxies

ProCurve Networking
HP Innovation

Project: Network Behaviour

The project goal is to understand the behaviour of large computer networks (10'000+ nodes) in High Performance Computing or large Campus installations to be able to:

- Detect traffic anomalies in the system
- Be able to perform trend analysis
- Automatically take counter measures
- Provide post-mortem analysis facilities

ProCurve Networking
HP Innovation

Project: Network Behaviour

The project will be divided into three phases:

- Data Collection and Network Management
- Data Analysis and Algorithm Development
- Prototype Development and Analysis

ProCurve Networking
HP Innovation

Data Collection and Network Management

Identify the sources of information available in the network infrastructure, including both the LAN and the WAN.

Survey the network management techniques in use, in particular at CERN and in HP ProCurve.

Perform an analysis of large-scale sFlow data collection

Investigate and propose a scalable data collector architecture

Define structures for efficient storage and retrieval of large-scale network data

Begin collecting network data for analysis

ProCurve Networking
HP Innovation

Data Analysis and Algorithm Development

Analyze collected data (and continue collecting more data)

Identify and investigate network “anomalies”

- Definition of “anomaly”

Investigate algorithms for anomaly detection

- Self-learning systems
- Rule based systems
- Traffic pattern analysis

Investigate algorithms for automatic data collector tuning

- Identification of network activity “hot spots”
- Automatic adjustment of the resolution of data collected

Investigate structures and algorithms for data reduction or compression

ProCurve Networking
HP Innovation

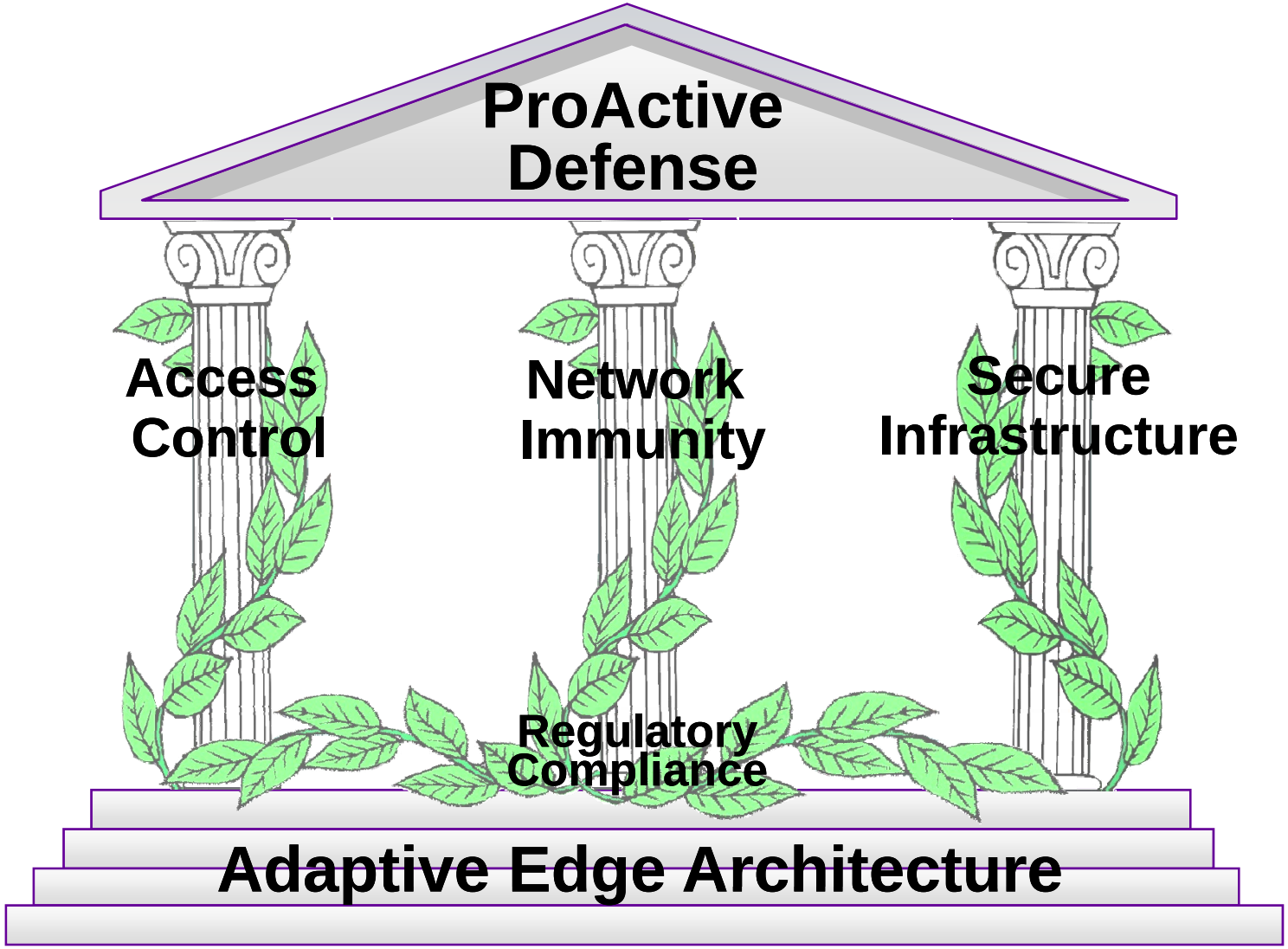
Prototype Development and Analysis

Detailed design and implementation of the integrated prototype

Investigation report on the performance and scalability characteristics of the prototype, as well as recommendations for future enhancement

Security Solutions Framework

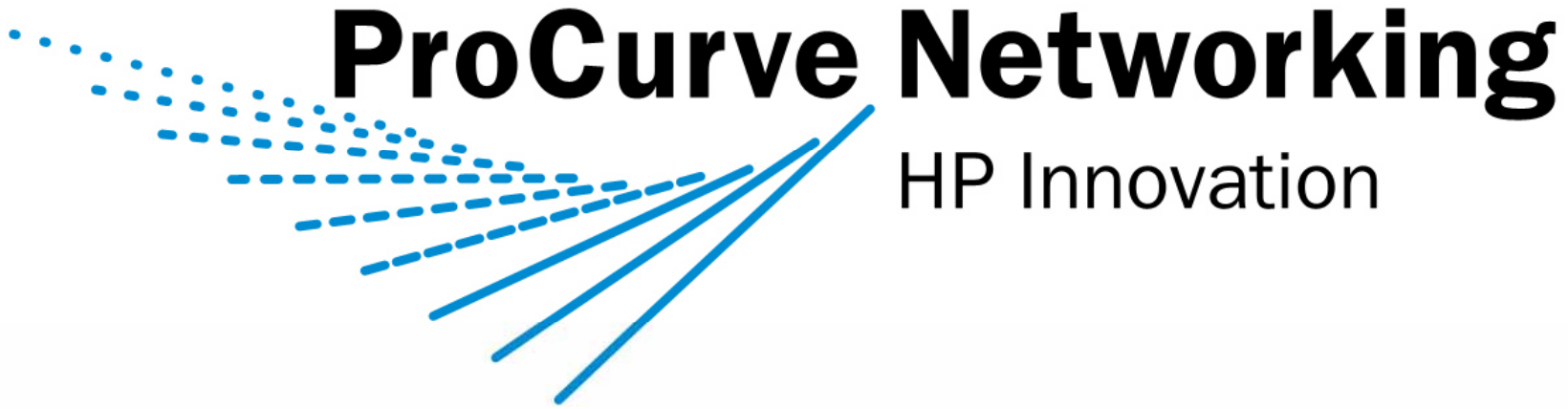
ProCurve Networking
HP Innovation



ProCurve Networking
HP Innovation

Thank You!

For more information www.procurve.com/security


ProCurve Networking
HP Innovation