CloudShield™

A Multi-Mission Network Centric Warfare Platform

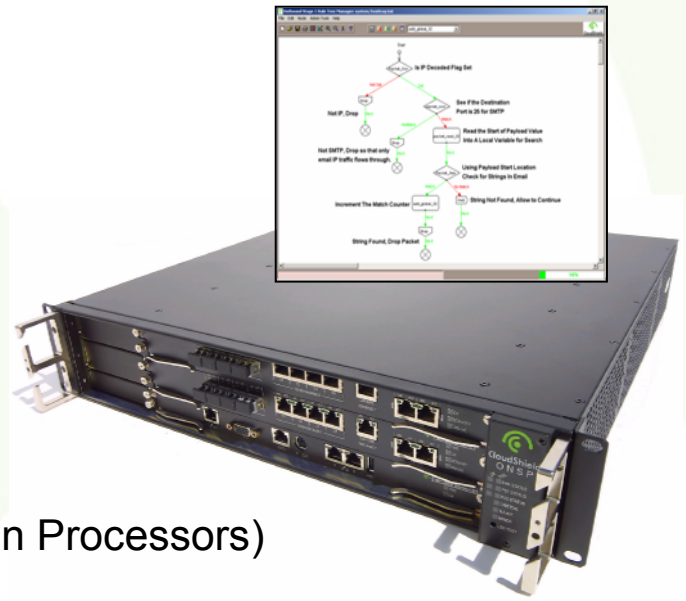
Session 3C4

Peder Jungck, CTO & Founder

peder@cloudshield.com

CloudShield®

- Founded in 2000; Patented Technology
  - ~50 Employees, Headquarters in Sunnyvale, CA
- 3rd Generation Platform Available Now
- Privately Held (>$50M Funding to Date)
  - Foundation Capital, Paladin Capital Group, ComVentures, TPG Ventures, SVIC, Xilinx
- Target Market Focus
  - Government
    - DoD / Intel
  - Commercial
    - Service Providers (Carrier, ISP, MSO, RBOC)
    - Large Financial Institutions (Banks, Transaction Processors)



- Partner Based Business Model
  - We Build Systems, Operating System, Development Environment
  - Government Solutions Delivered Through System Integrators

Network Centric Warfare Implications

- ***High-level technical challenges***
  - Traffic and performance demands increasing
  - Changing requirements is inevitable, often too expensive
  - Need to connect disparate systems but technology progressing at different rates

- ***High-level operational challenges***
  - More systems, greater overall complexity
    - training and management costs are compounded
  - Scope of network security threat is broadened
    - more network entries, once in more systems accessible

You can't solve tomorrow's problems with yesterday's solutions

Tackling the Challenges While Adopting an Open Systems Model

> "The modern battlefield demands network-centric warfare (NCW), and open architecture is its most critical enabler."
>
> *Richard T Rushton*. **United States Naval Institute.**

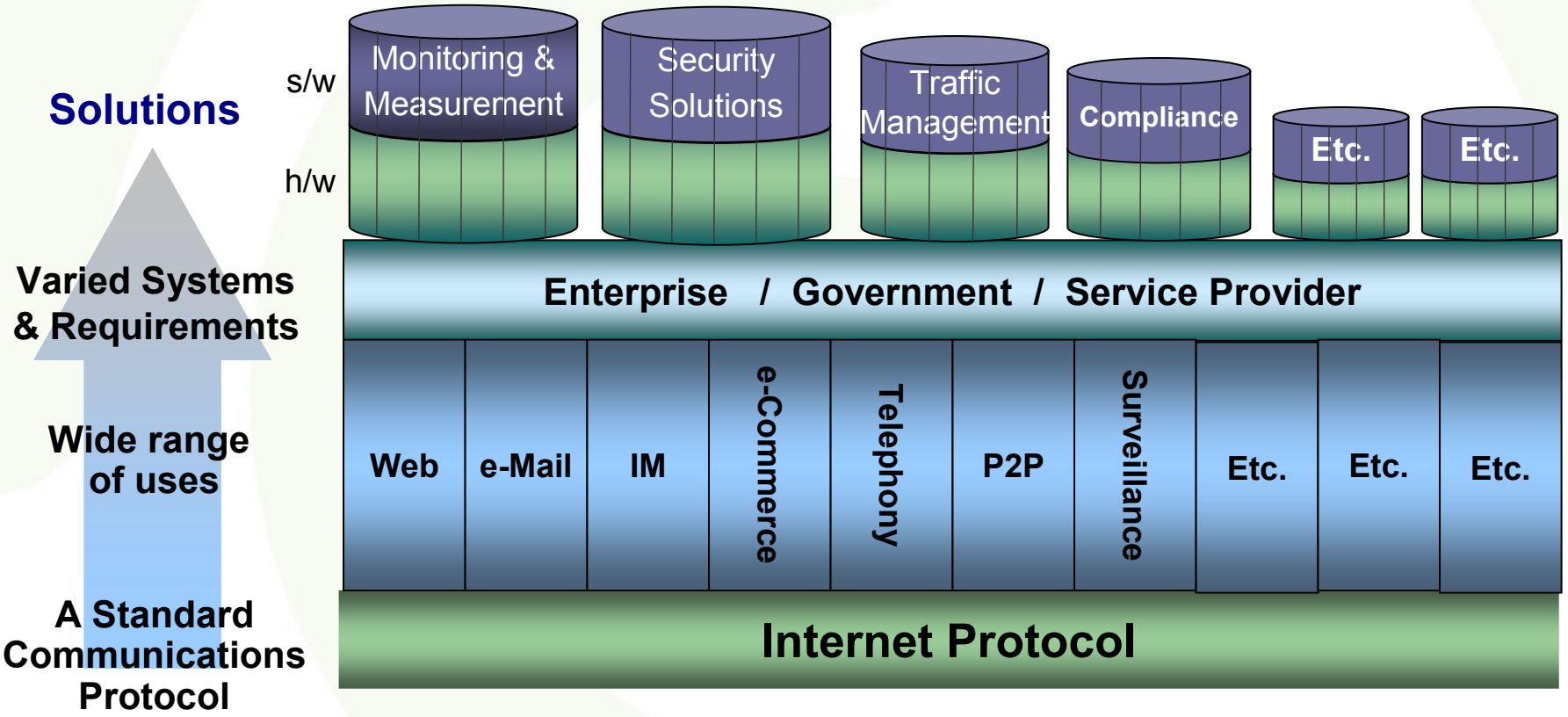
The dynamic networking environment of NCW demands:

- ***De-coupling Hardware from Software***
  - Yields flexibility, adaptability and improved economics
- ***Incorporating requirements for standards & accreditation***
  - Ensures systems will continue to inter-operate as needs change
- ***Actively seek COTS or COTS enabled GOTS solutions***
  - Reduces cost, reduces time to deployment, leverages innovation

Current State of Security Solutions Industry

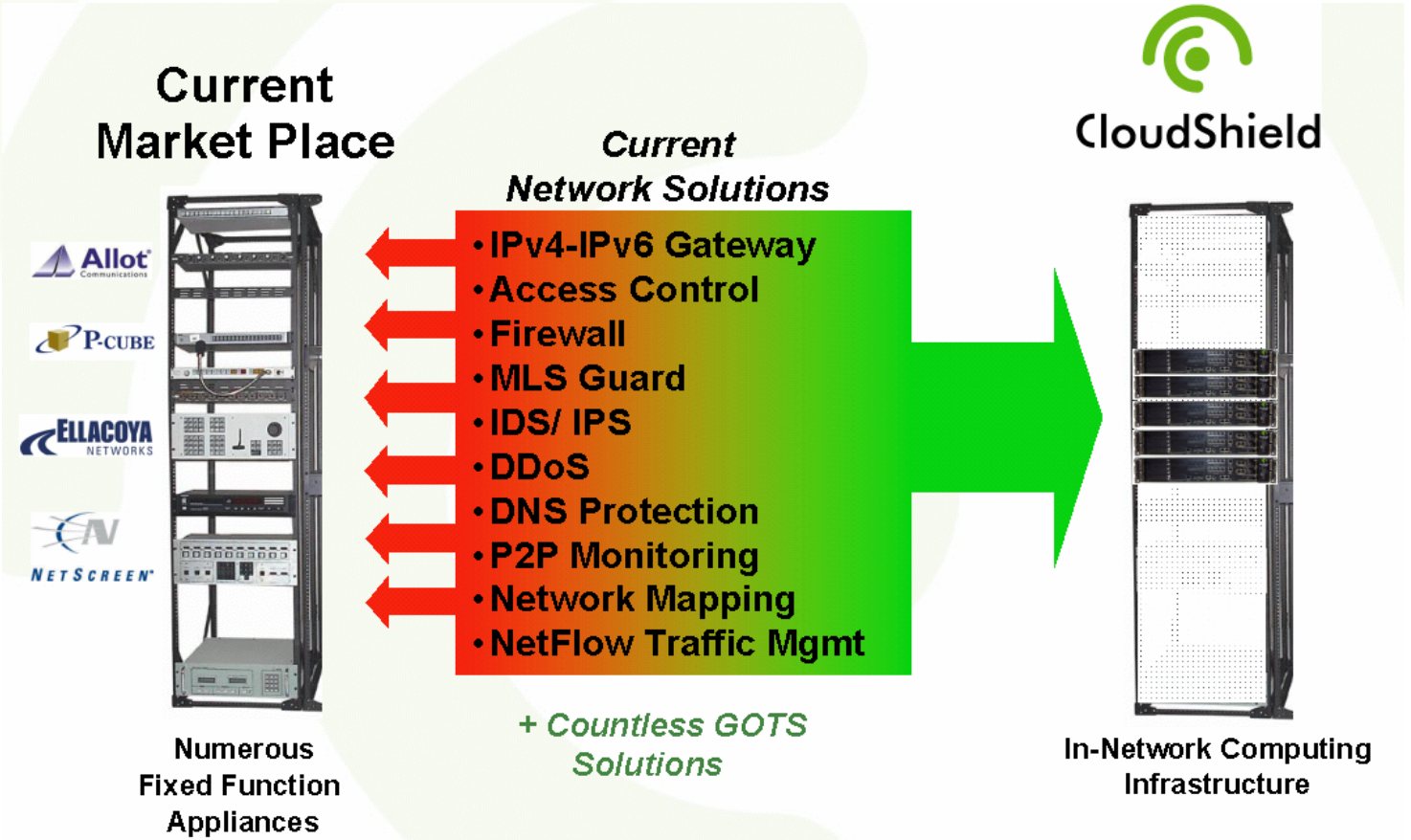
CloudShield™

Solutions Silos; Inefficiencies, Expensive Model



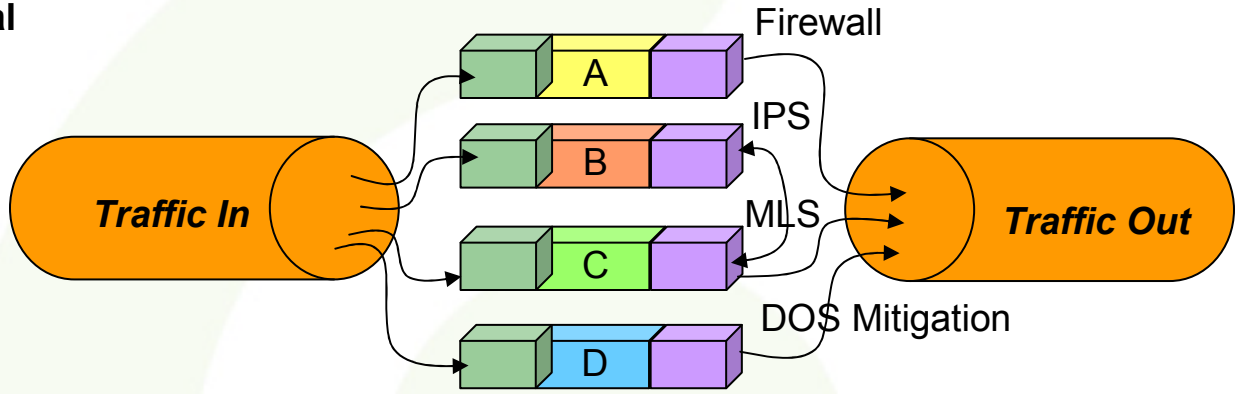
Multi-Mission Platform Benefits
Reduced Operational Costs & Complexity

CloudShield is leading the transformation to multiple service systems that place flexible platforms into the network to handle a variety of network security, traffic management and mission specific solutions.



Technical Challenges
Rack & Stack Imposed by Current Methodologies

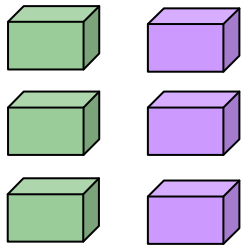
Result of traditional COTS Silo world



Expensive to Deploy

Load balanced sandwiches of multiple systems for each feature set are costly to procure and deploy. Redundant functionality is paid for over and over again.

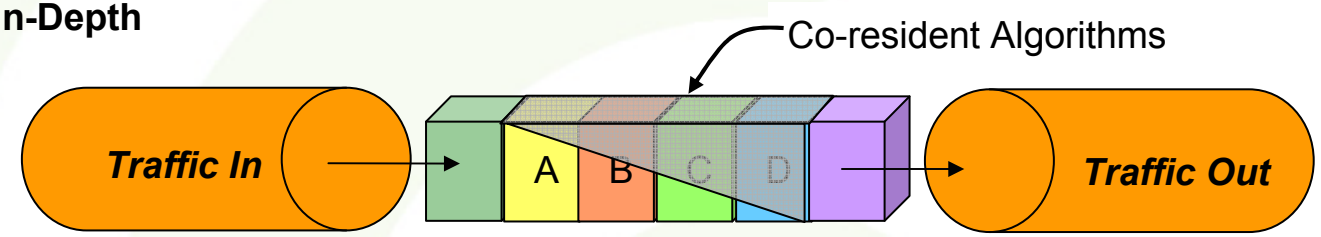
Redundant Processes



Next Generation Implementation Model
Merge Shared Features, Improve Technology

Network Centric Platform

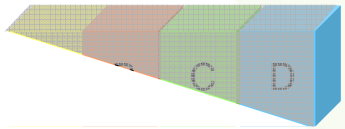
Defense-in-Depth



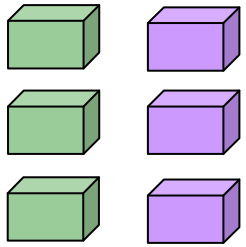
Often 5 - 20x Improvement

Yields dramatic improvement in performance and cost per gigabit or user. This is done in overall reduction of processing required and streamlining of functionality into more efficient processing paradigm.

Algorithm Reductions



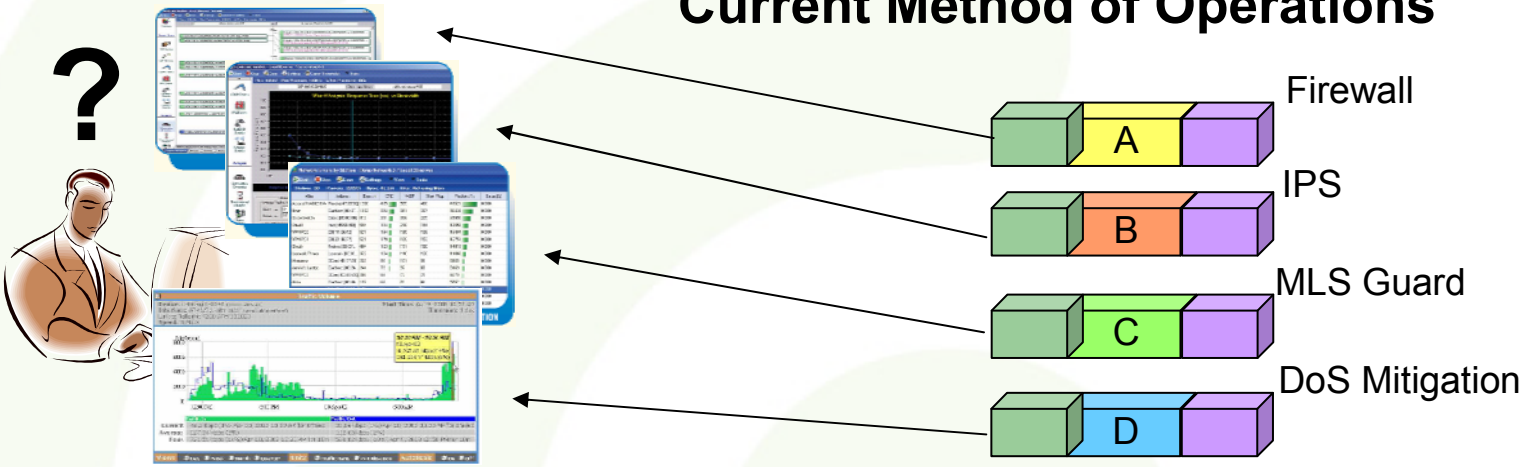
Redundant Processes



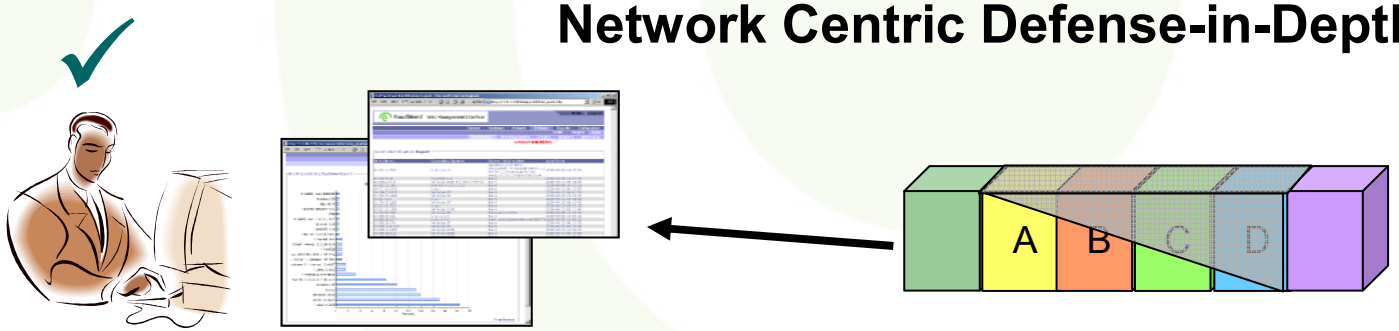
Command and Control

Independent systems increase C2 burden.

Current Method of Operations



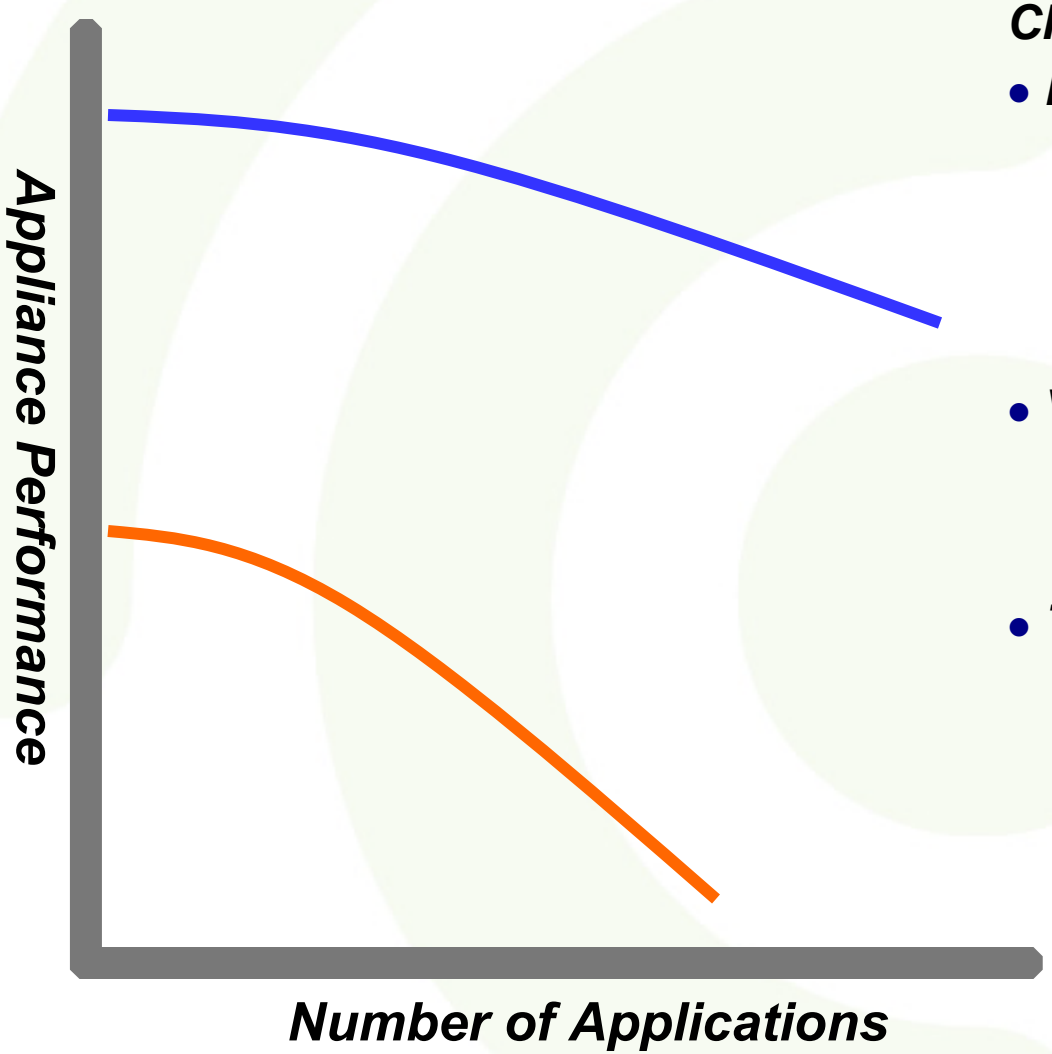
Network Centric Defense-in-Depth



Provisioning of Functional Components Remains Focused and Secure, Common Mechanisms can Converge for Reduced Expense.

Convergence of Solutions without Penalty

CloudShield Scales Better Than Any Other Solution



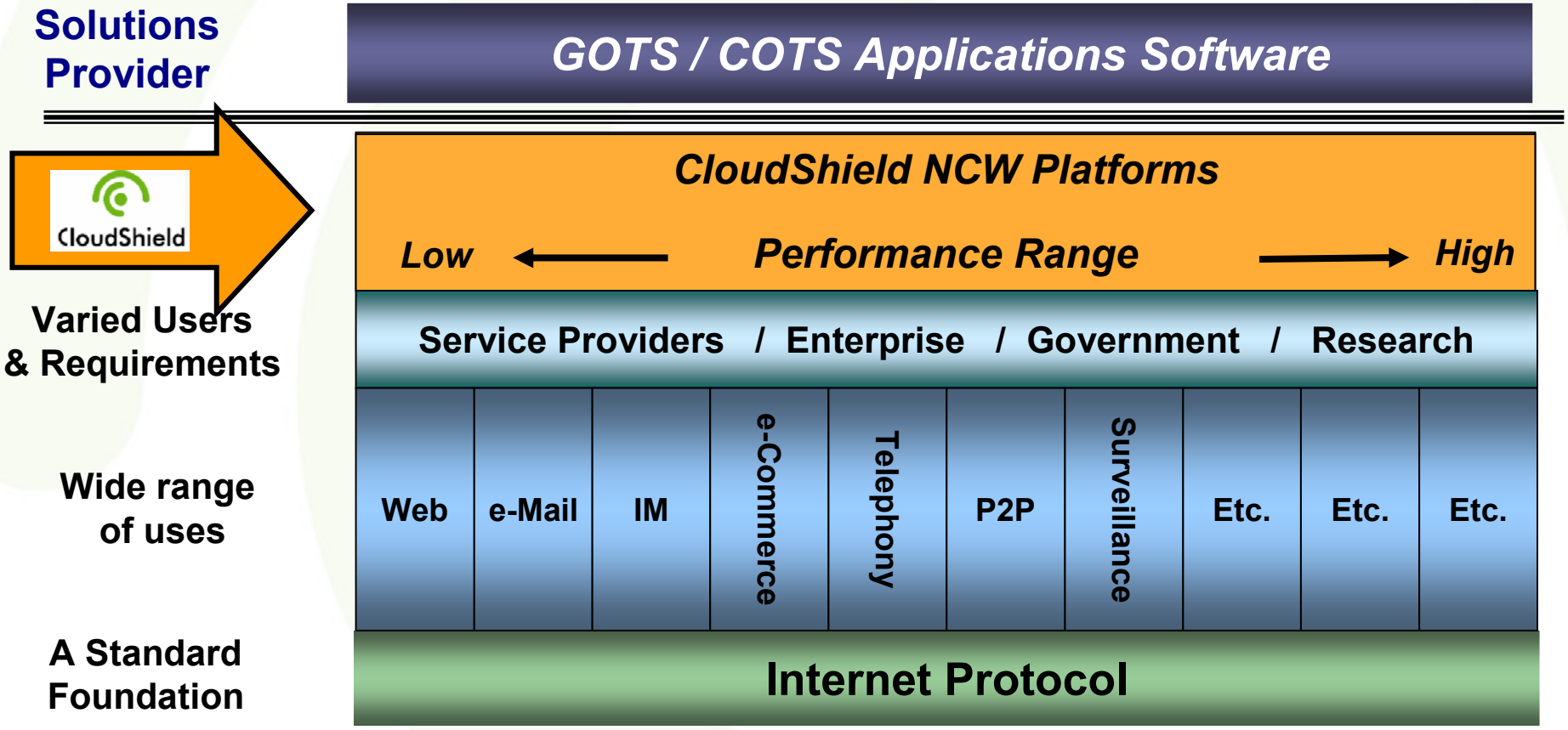
CloudShield Market Solutions:

- ***Network Security***
  - DDoS
  - Firewall
  - IDS / IPS
  - Web/Content Control
- ***VoIP***
  - Security
  - Quality of Service
- ***Traffic Management***
  - Network Monitoring
  - QoS/BW Management
  - Peer to Peer

Marketplace

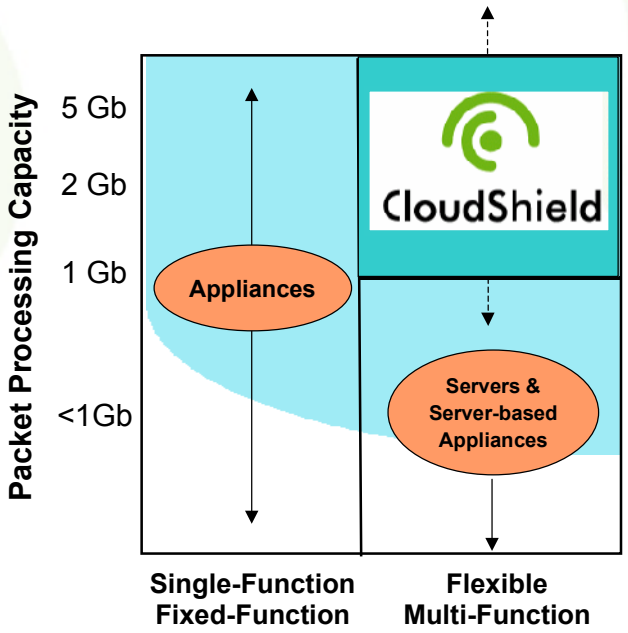
CloudShield

De-Couple Software from Hardware



NCW Platform Design Goals

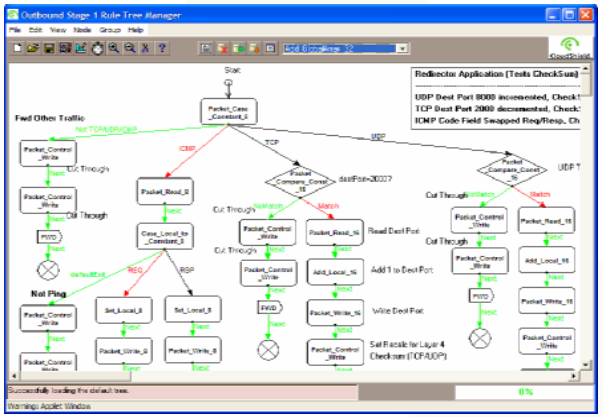
- Build a flexible, common network applications platform
  - COTS hardware/software platform, ready for deployment
- Allow mission changes with software-only updates / modifications
  - Same software many systems, software changes remotely
- Resiliency and High Availability
  - Ensure that solutions are able to handle rigors of NCW
- Make it high-capacity to meet needs of networks
  - Provide resource capacity to handle complex and integrated network applications
- Standards based and accredited for operation
- Provide mechanisms for rapid deployment against new missions by customers and integrators.

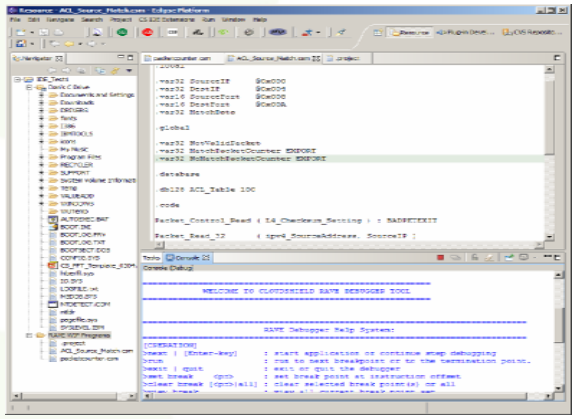


CloudShield CS-2000 NCW Platform

- The **CS-2000 Platform** for network services
  - A **Deep Packet Processing Module** is coupled with a general purpose Intel Pentium server module to enable open source and 3rd party network applications to achieve higher throughput

- Using **CloudShield's Software Development Tools, APIs & Utilities,** high performance network applications are rapidly and easily developed





CS-2000 Series Physical Architecture

Deep Packet Processing Module (DPPM)

- Executes Network Application Inspecting and Controlling Packet Data
- Real-Time Silicon Database and Unstructured Packet Searches
- Single or Dual DPPM Configurations for HA, Performance or Multiple Use
- Physical Connectivity: Gigabit Ethernet and OC-3/OC-12/OC-48 SONET/SDH

Chassis

- 2RU (3.5 inch)
- Modular Design
- Redundant AC or -48V DC Power
- System Status Module

Auxiliary Slots

Future use for

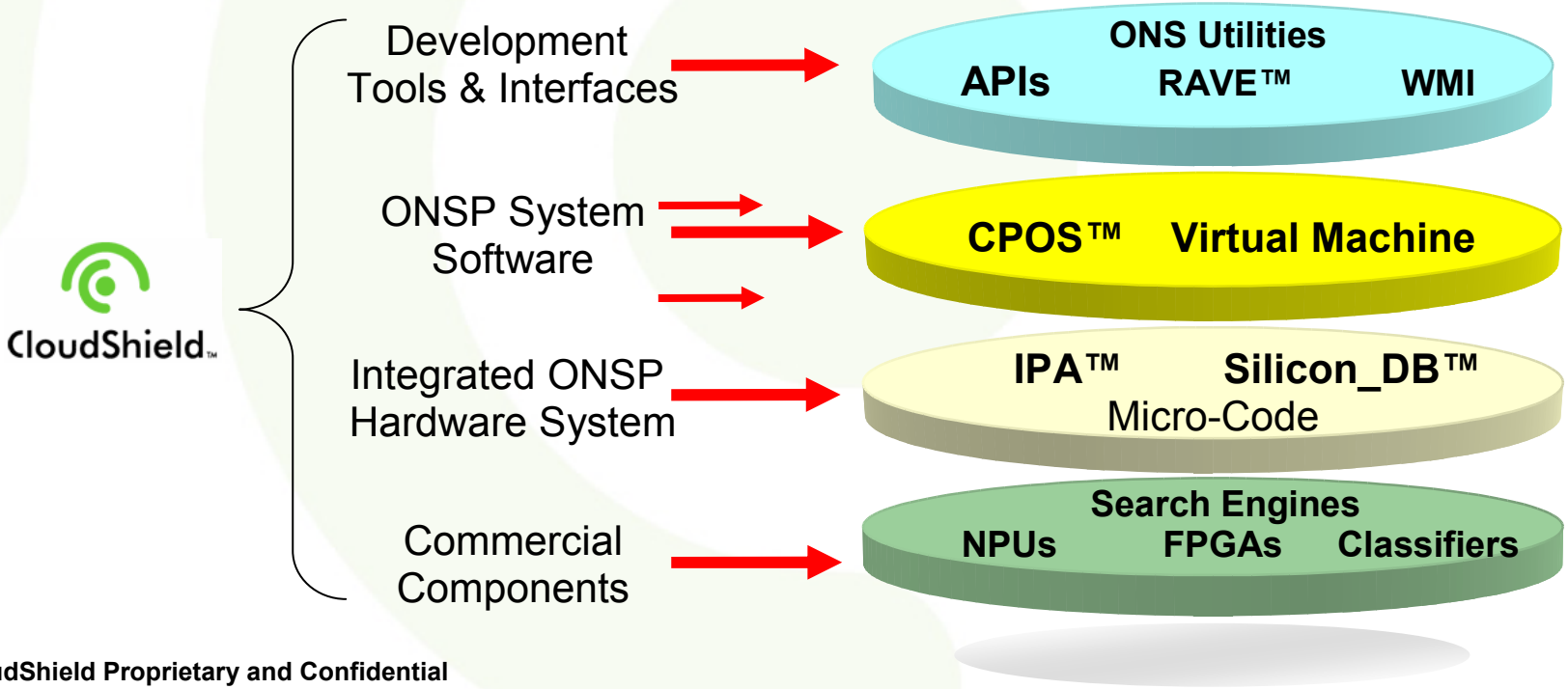
- HDD Module
- Telemetry Inputs/Outputs
- Optical Bypass/HA Module

Application Server Module (ASM)

- Hardened Linux Infrastructure
- Hosts Analysis Applications
- Network Element Management (Web, CLI, SNMP, ODBC)
- Mandatory Access Control

Layered Construction for Portability

- Best-of-breed, commercial silicon used for performance *and* flexibility
- Patented hardware architectures scalable across a range of performance targets
- Deep packet processing application building block functions embedded in micro-code, controlled by CPOS
- Developers shielded from hardware complexities; access functions from higher level



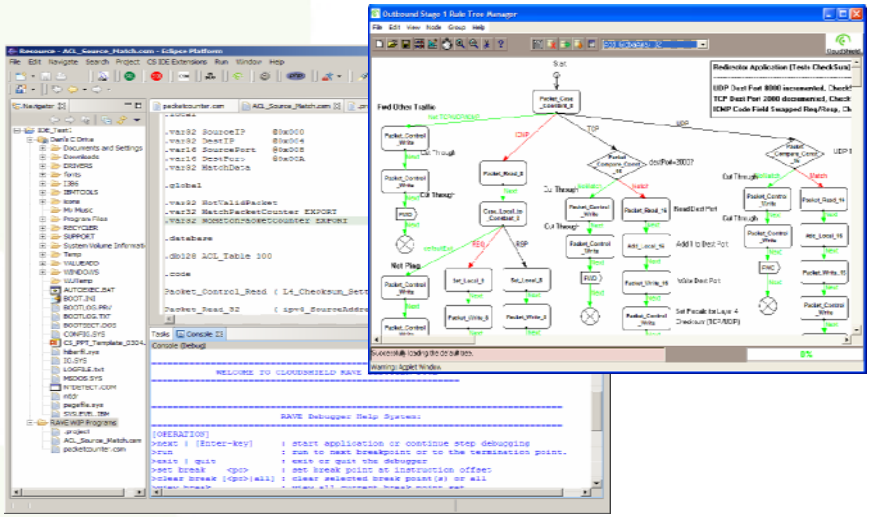
High-Level Interface for Rapid Development

- Extensible Policy Development Environment (Eclipse)
  - Libraries, Integrated Suites of Network Solutions
  - Multi-Developer, Certified System Integrators
- RAVE is a high-level language defining network policies
  - Designed to promote rapid development of packet processing operations
  - Applicable across a broad range of applications
- PC-based Design and Prototyping Environment prior to Deployment

RAVE Development Cycles

2-6 Weeks

Logic Model	Prototype and Test	Deploy



Currently Certified Solution Developers

Representative Sample of Developers/ISVs

CloudShield

Over 35 Solutions in Development

DoD & Intel Taking a Notice

Growing Adoption of CloudShield

CloudShield™

Information Assurance (Network Security)

- US Air Force - High Speed Firewall and Intrusion Detection Solution

Signals Intelligence

- Applied Signal has chosen CloudShield for a Network Application – customer trials underway

Multi Level Security Guard

- Northrop Grumman developed a Guard product on CS-2000.
  - Accreditation and customer rollouts are expect

Gateway Content Control (Traffic Management)

- Terramark offering services related to the managing traffic at International Peering Points and continues new solution development.

Network Centric Warfare Platform Concept of Operations

CloudShield™

NOC / SOC Management

App Mgmt

Device Mgmt

Application

App (2)

App (3)

App (*n*)

Supporting data

CloudShield™

Applications e.g.
- IDS/ IPS
- Access Control
- Firewall
- MLS Guard
- Data Theft
- Statistics
- Quality of Service
- Traffic Prioritization
- Network Mgmt

Battlefield Systems

Network/ Systems/ Data Integrity

- Consistent device management data, inter-connect, & interface regardless of application
- Application management connections unaffected
- Flexibility, capacity to supplement applications data gathering functions

CloudShield™

Questions?

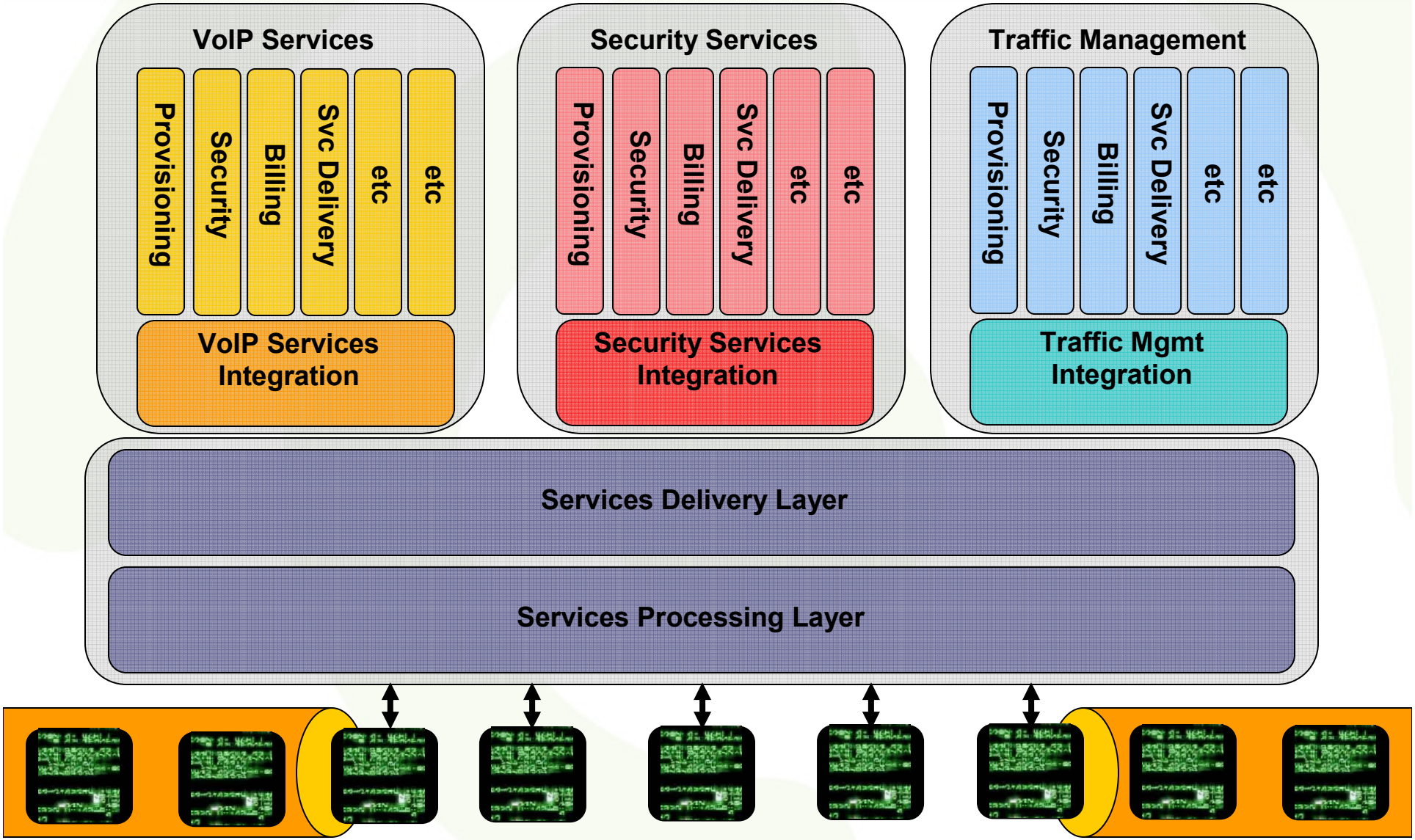
peder@cloudshield.com

CloudShield™

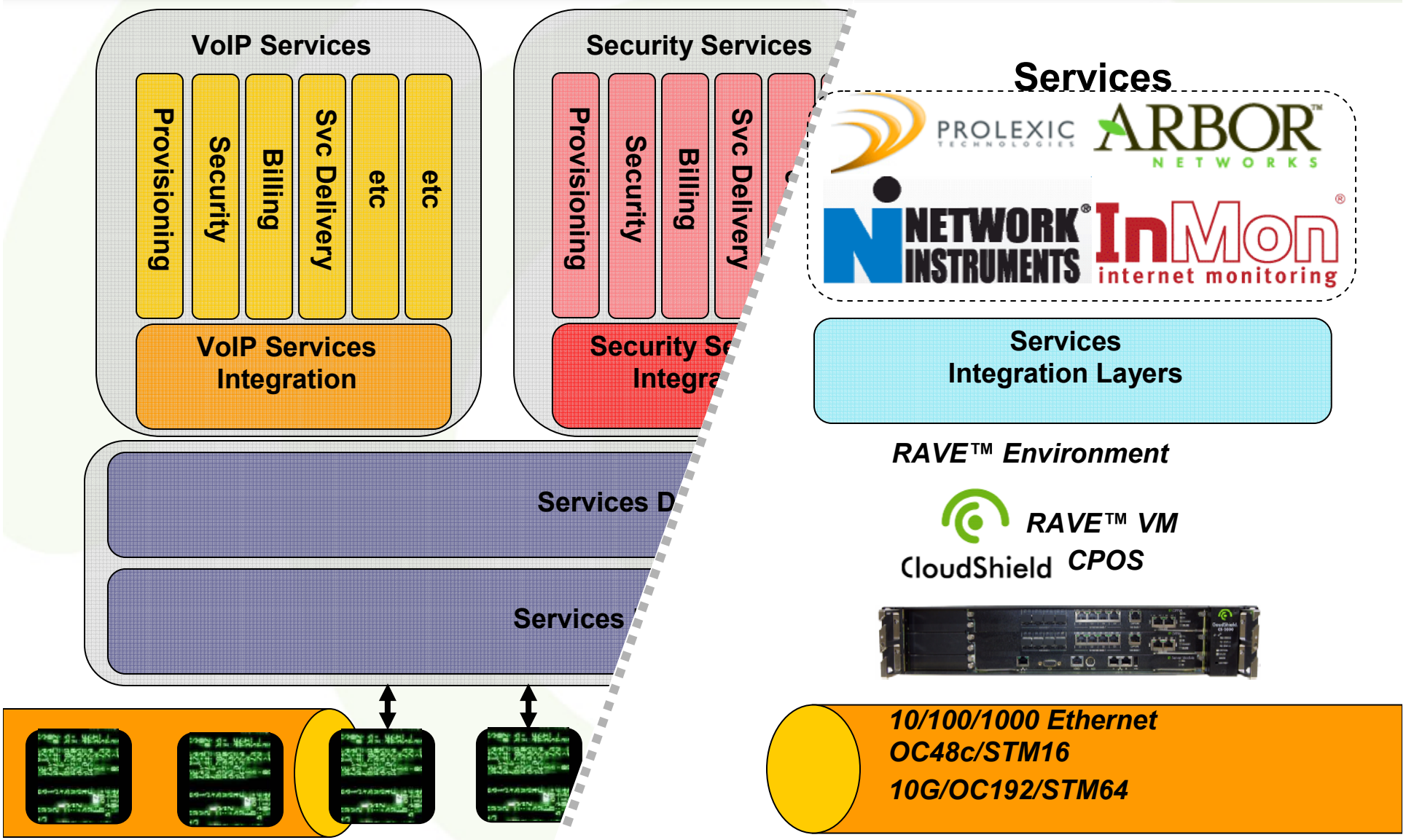
Backup

In-Network Computing *Services* Framework

CloudShield™



In-Network Computing *Services* Framework



CloudShield Proprietary and Confidential

In-Network Computing Platforms
CloudShield® CS-2000 Series

2 Gbps Ethernet Configuration

NOW

- Single DPPM
  - 4 x Gigabit Ethernet (eSFP) or 4 x 10/100/1000BaseT (RJ-45)
  - 1 x 1000BaseT Capture Port

- **All DPPMs Have Line Rate**
  - **IP Decoding**
  - **Checksum Validation/Recalc**
  - **Forwarding (Switching)**
  - **Regular Expression Processing**
  - **Silicon Database Session Mgmt**
  - **New Innovations:**
    - **Stream Processing Accelerator**
    - **Intercept Log Accelerator**

2.5 Gbps POS/SDH Configuration

NOW

- Single DPPM
  - 2xOC-48c POS or 8xOC-3/12c POS
  - OC-48c/STM-16 (SFP)
    - SR-1: 1310 nm single mode
    - LR-2: 1550 nm single mode

1 Gbps Ethernet Configuration

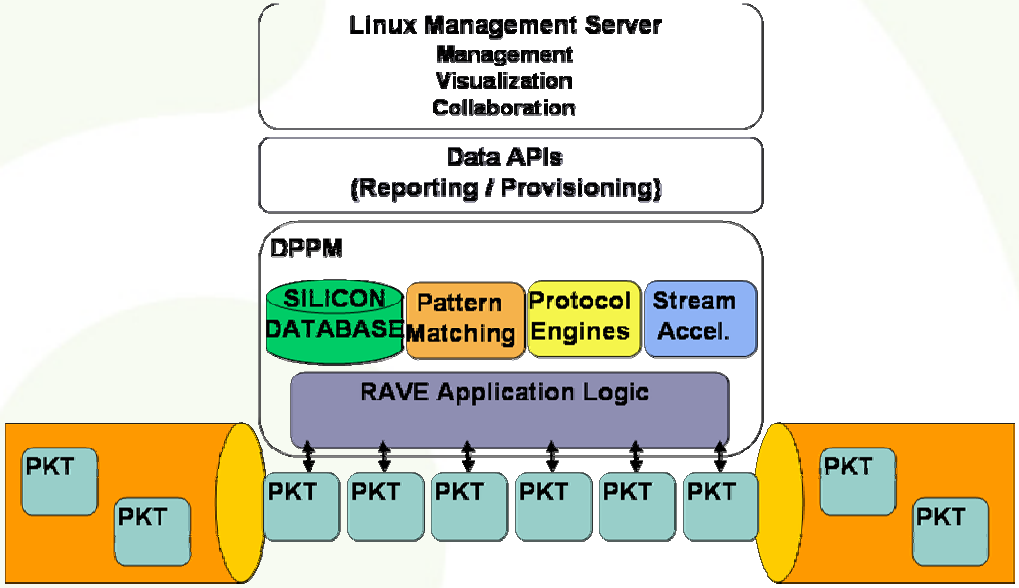
Q2 05

- Single DPPM
  - 2xOC-48c POS or 8xOC-3/12c POS
  - OC-48c/STM-16 (SFP)
    - SR-1: 1310 nm single mode
    - LR-2: 1550 nm single mode

CloudShield PacketWorks Operating System
Services Processing Layer

CloudShield PacketWorks OS

- Hardened RedHat Linux Management Operating System
- CloudShield Embedded Linux
- Proprietary Data Plane OS for RAVE Execution
- Separation of Provisioning from Execution Interfaces
- Integrated Access Control & Security Infrastructure
- Provisioning & Interface Tools
- Packaging, Deployment & System Mgmt Middleware



Undergoing EAL 4+ Common Criteria Certification

EAL Release will include SE Linux Enhancements

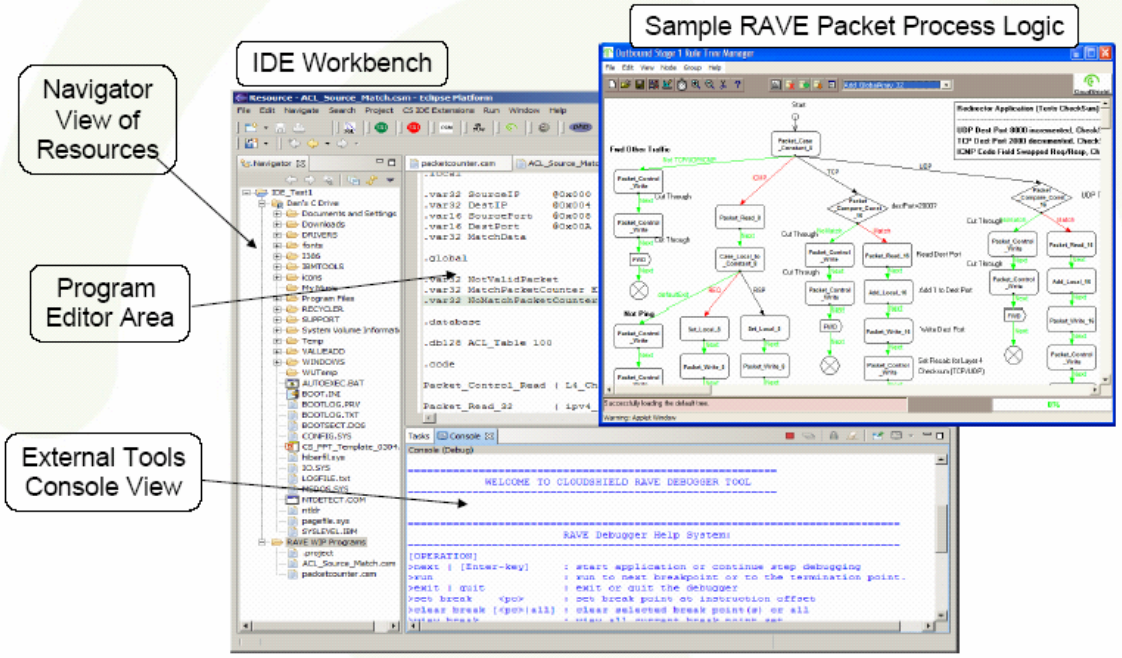
redhat.

CloudShield

RAVE™ Solutions
Services Delivery Layer

PacketWorks IDE

- Rapid Services Development
- Off-Network Debugging
- Simple Visual Learning Tools
- Life-cycle Development Tools
- Team Based Development
- Services Delivery & Packaging
- Software Development Kits
- Solution Libraries
  - VoIP
  - Security (Firewall, IDS, IPS)
  - Content (P2P, Malware, AV)
  - IPv6 to IPv4 Gateways
  - Custom Content Analysis



2-6 Weeks

Logic Model	Prototype and Test	Deploy

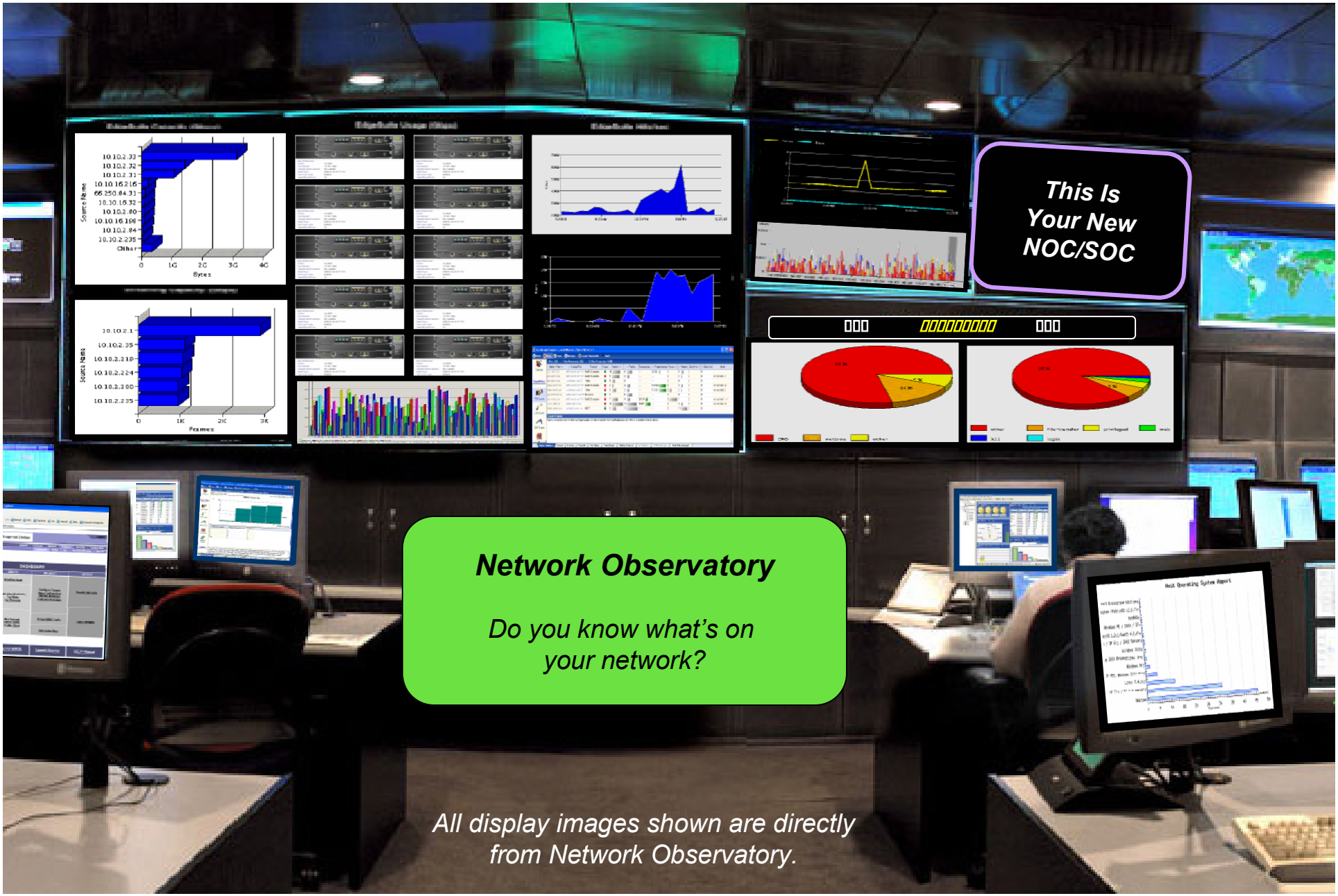
eclipse

CloudShield

NETWORK INSTRUMENTS

CloudShield

InMon
internet monitoring



Network Observatory

Do you know what's on your network?

All display images shown are directly from Network Observatory.