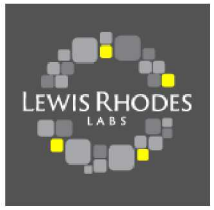


SAND2016-8744C

Neuromorphic Data Microscope

Information Assurance Symposium 2016

David Follett
Founder, CEO
Lewis Rhodes Labs (LRL)
david@lewis-rhodes.com

John Naegle
Senior Scientist/Engineer
Sandia National Labs
jhnaegl@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Vision

Neuromorphic Processing Units (NPUs)
are stunningly power efficient
at pattern matching

Mission impact,
pervasive & profound

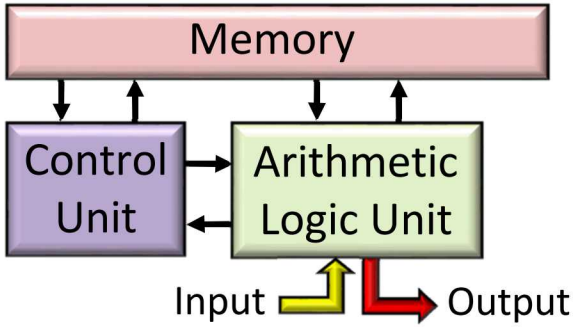
Imagine

- Orders of magnitude lower power, size, weight & cost
- Linearly scalable to arbitrary bandwidths
- Scalable to 10's of 1,000's of expressions
  - Efficient scaling with pattern complexity
- Deterministic; ie. robust to stream(s) content
- Scalable to millions of parallel contexts (sessions)
- Dynamically reconfigurable

Neuromorphic Processors are Disruptive

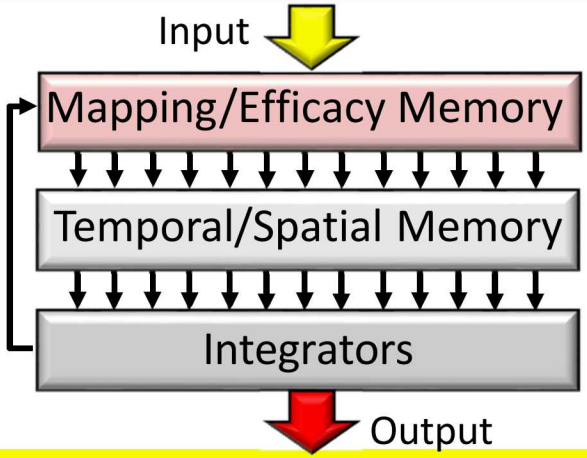
Neuromorphic is very Different

Legacy Von Neumann Architecture (CPU)



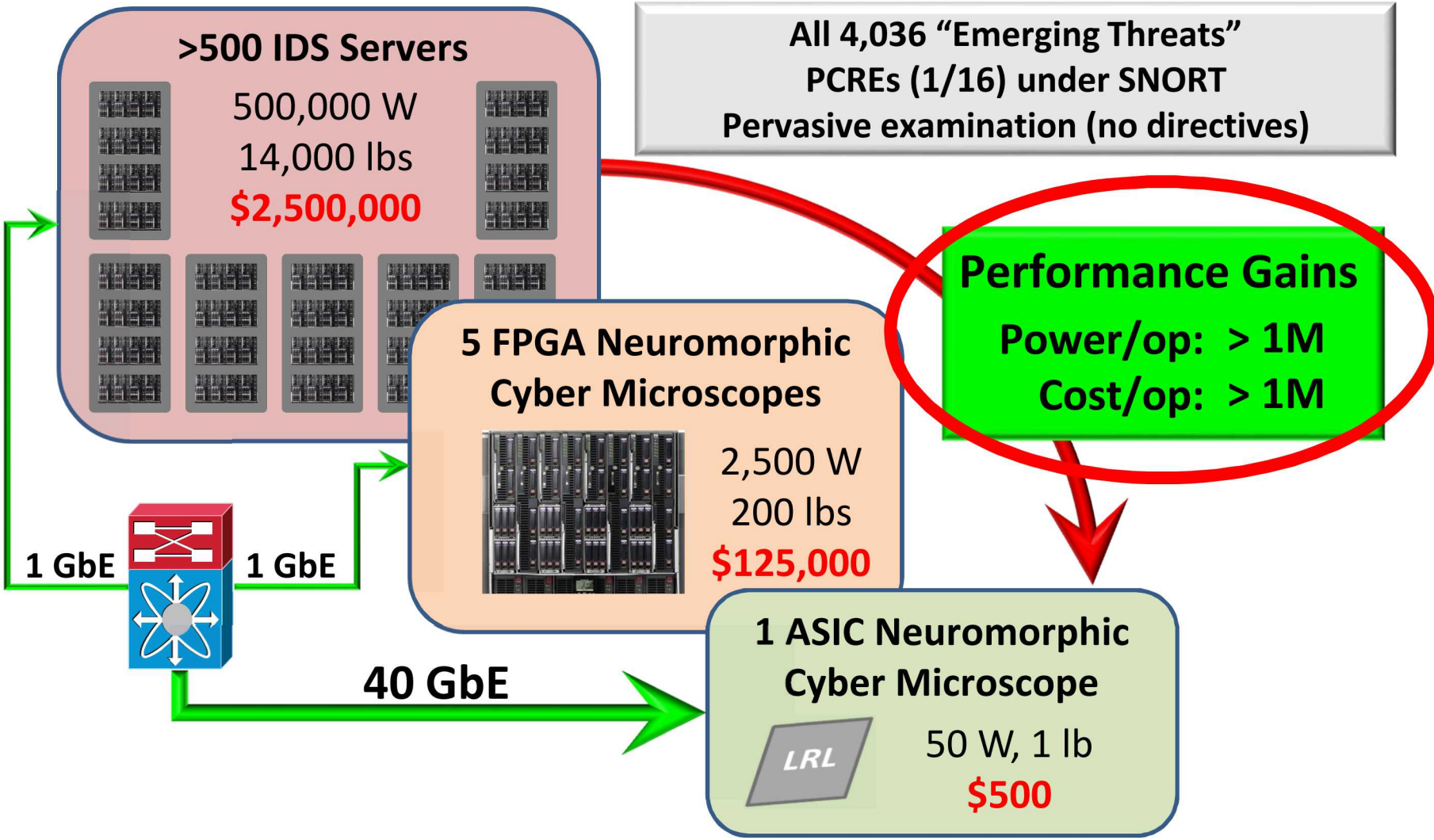
- **Complex processor**
  - Extraordinarily flexible
  - Data processing via sequential instructions
- **Simple memory**

Neuromorphic Processing Unit (NPU)

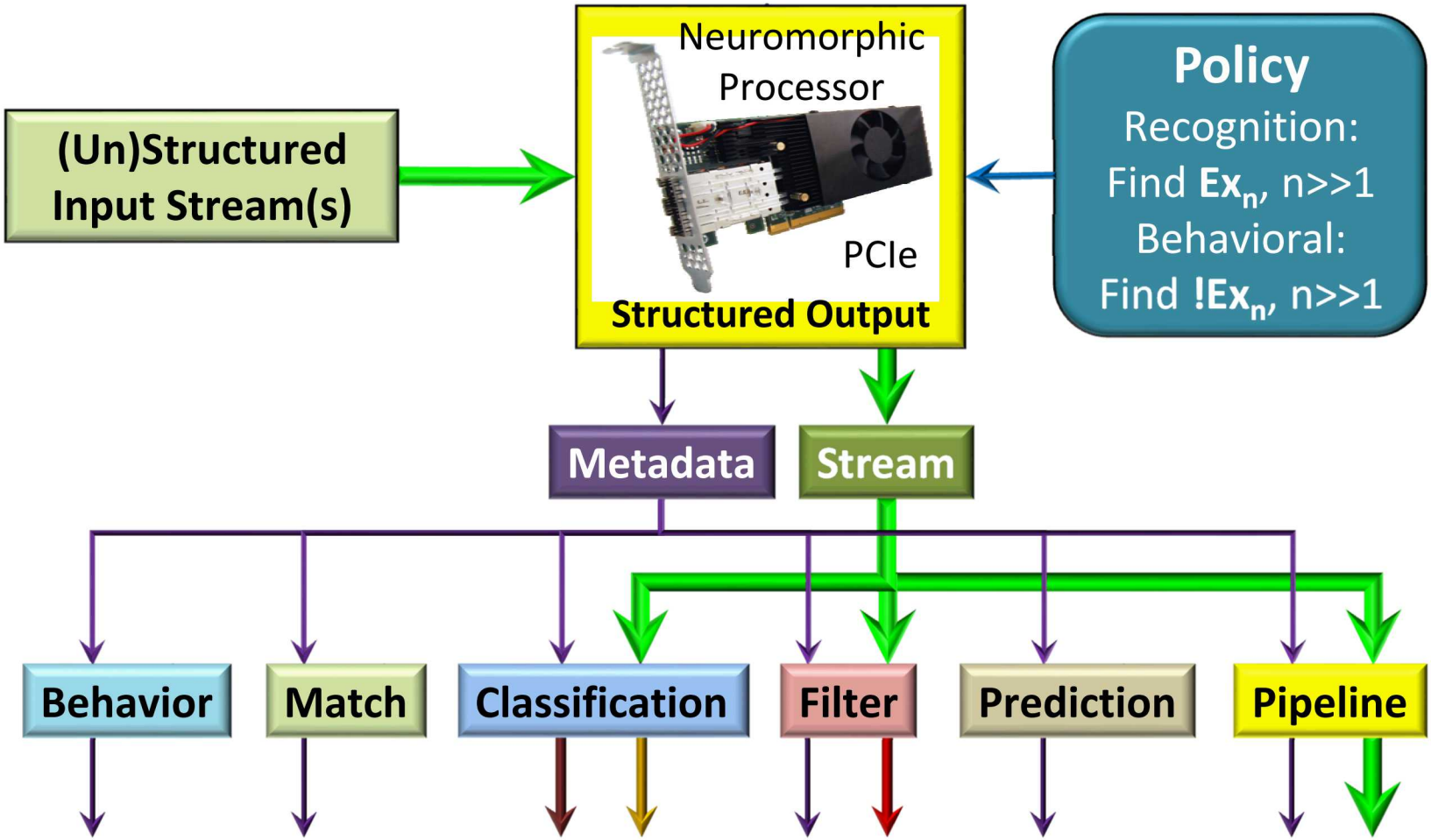


- **Simple processor**
  - Massively parallel integrators
- **Complex memory**
  - Data processing via efficacy & temporal/spatial mapping
  - Processing is multi-dimensional

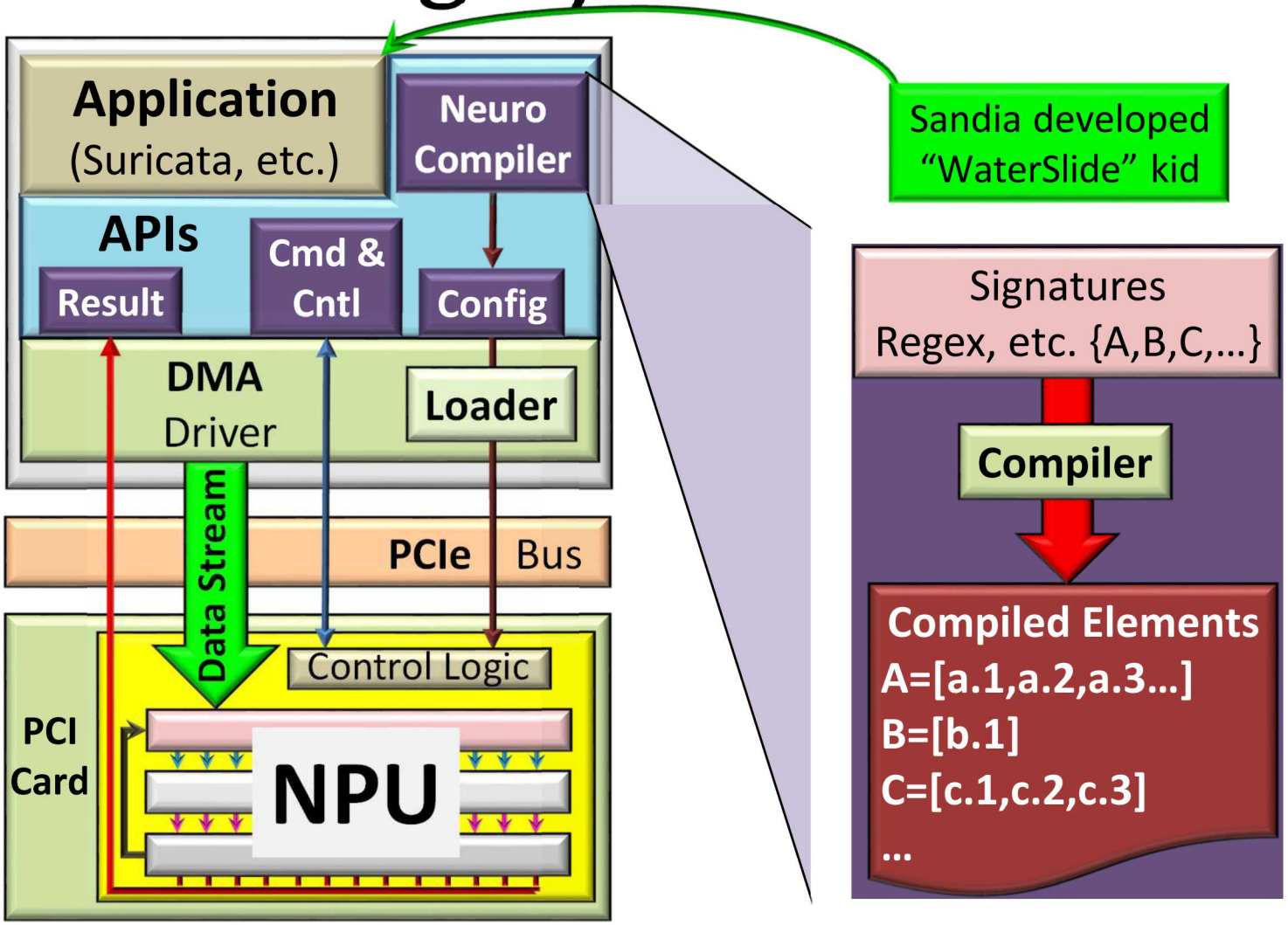
Power/op & Cost/op



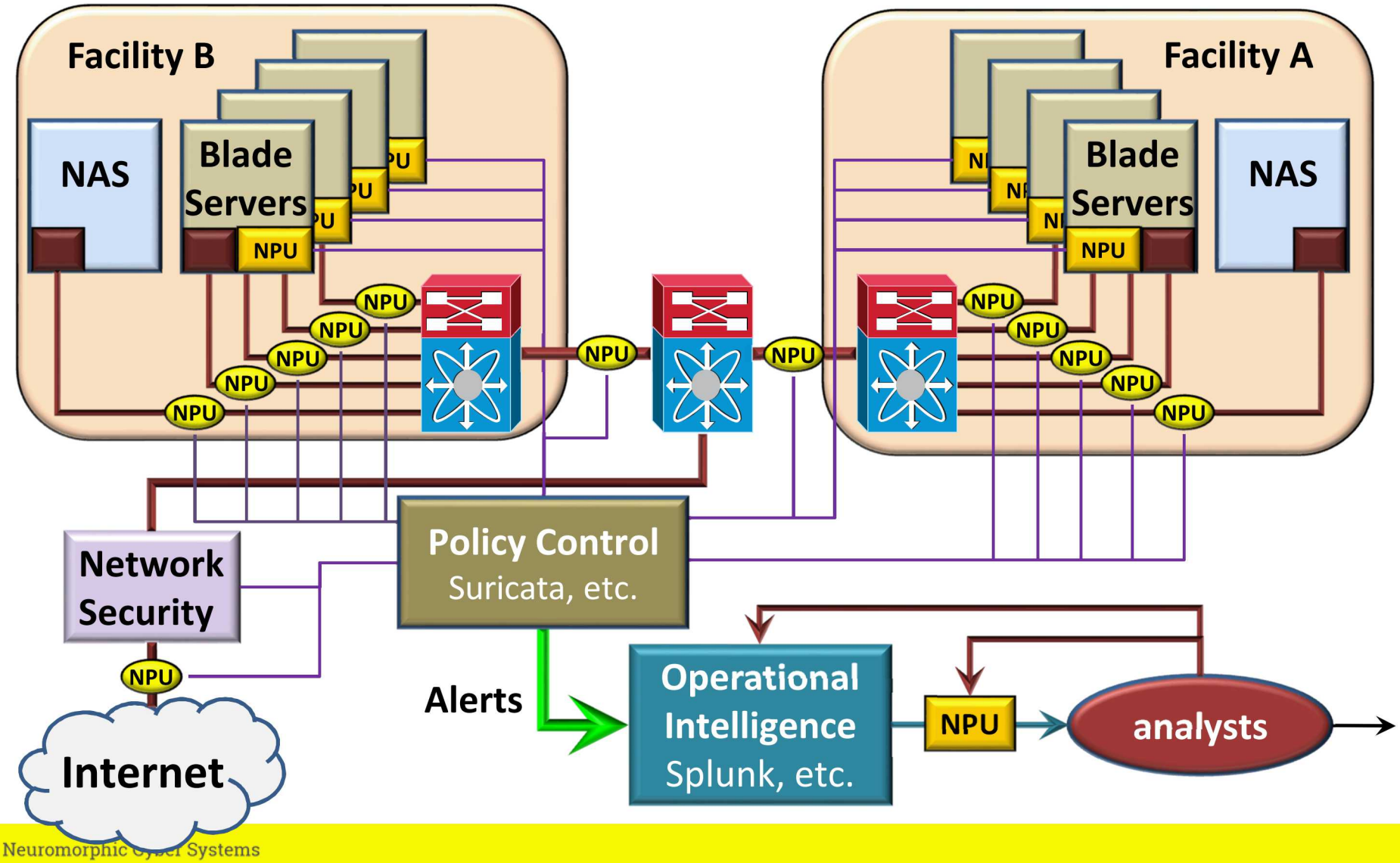
Neuromorphic Processors are Pattern Matchers



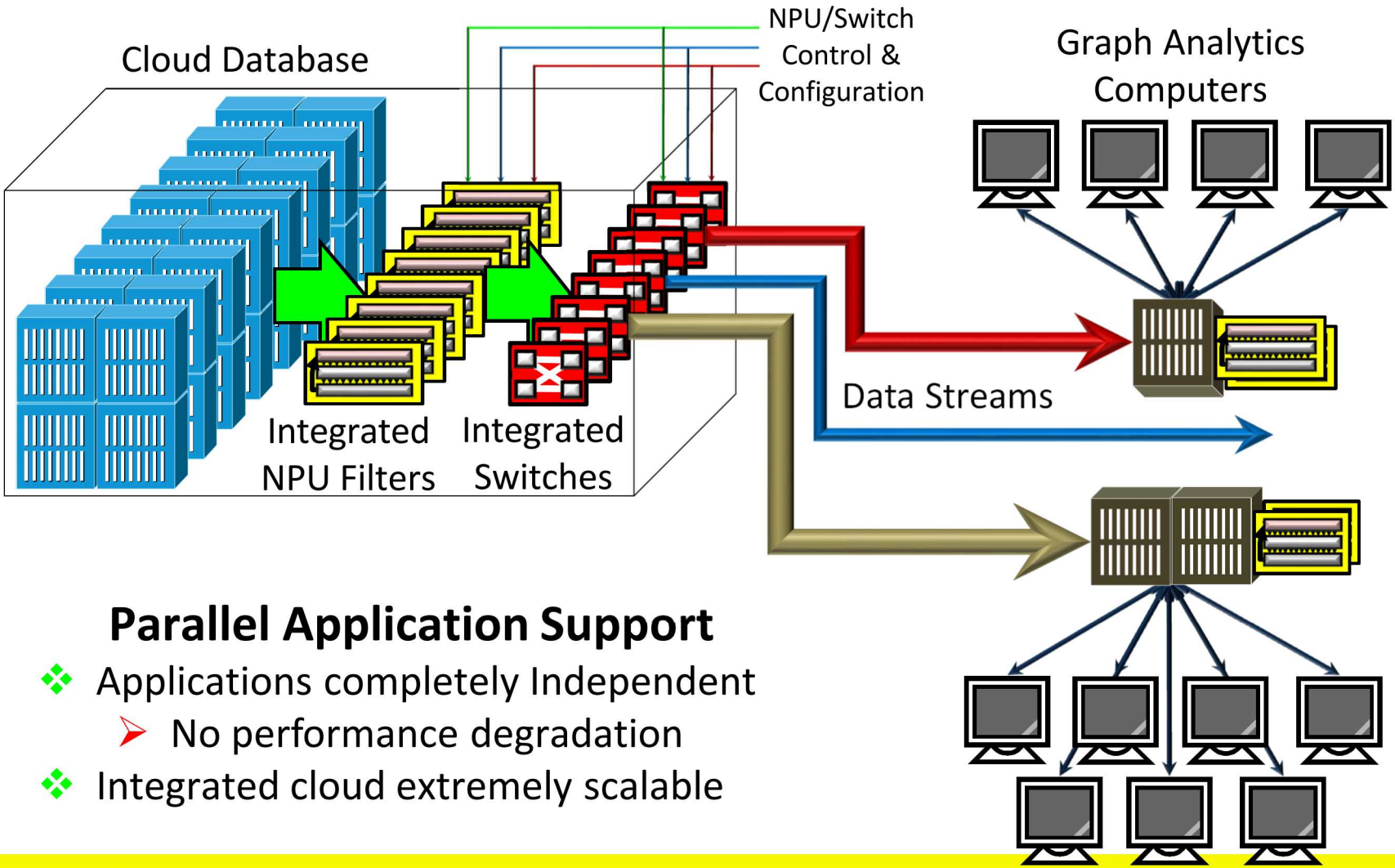
Highly Portable



Cyber Analytics Example



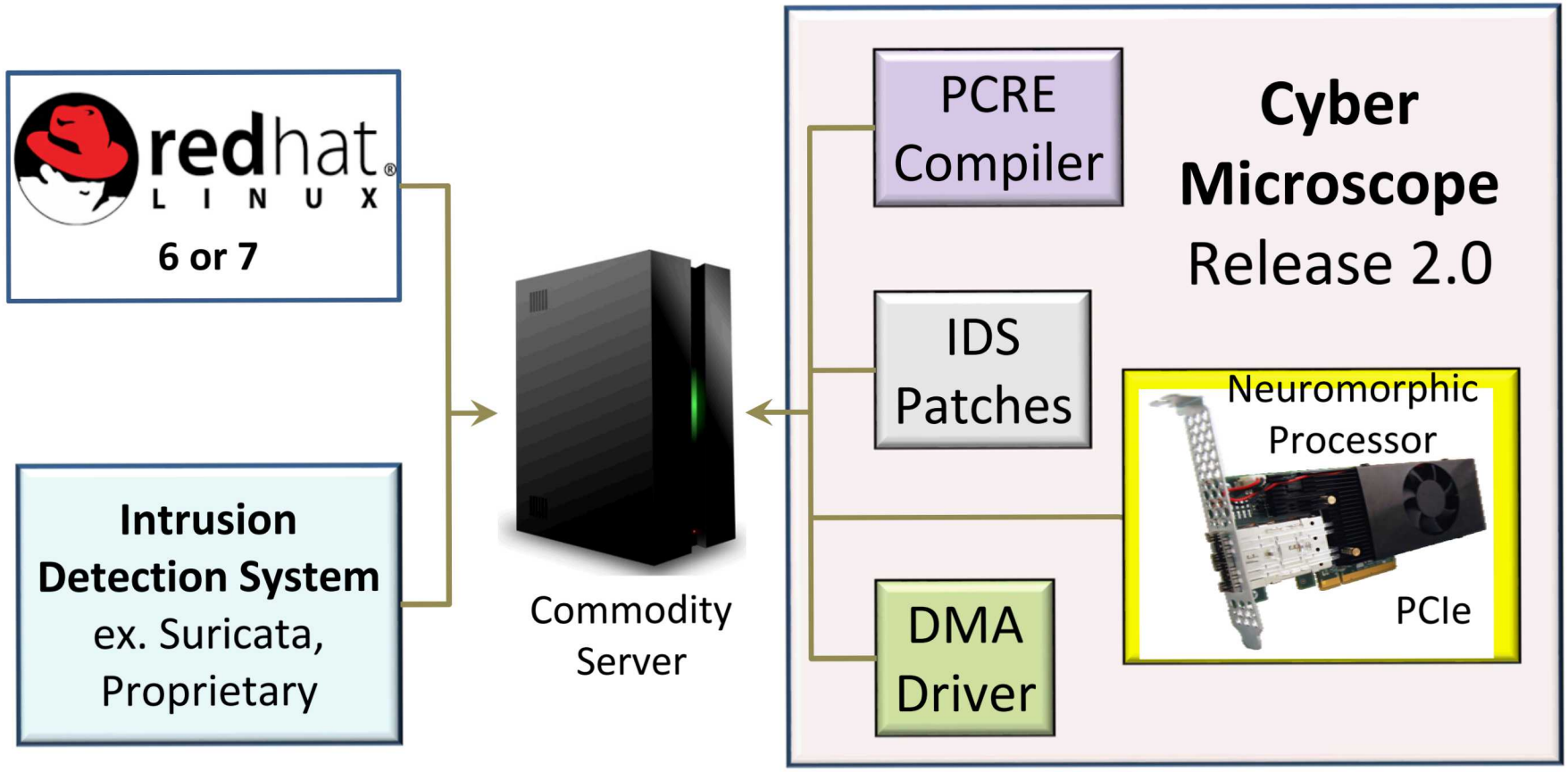
Graph Analytics Example



Parallel Application Support

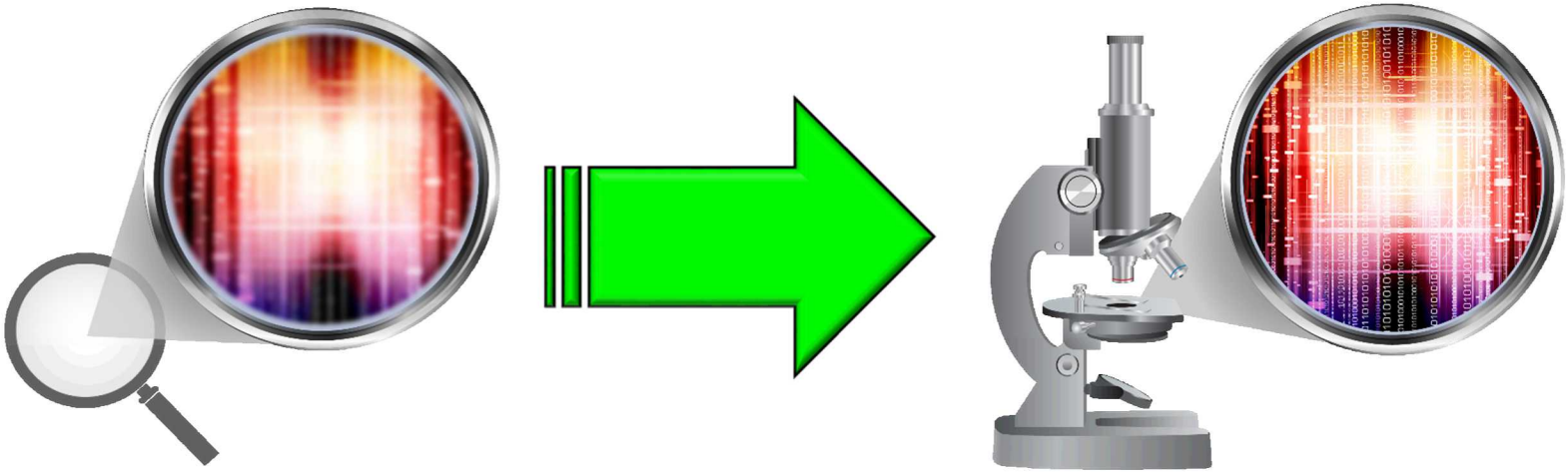
- Applications completely Independent
  - No performance degradation
- Integrated cloud extremely scalable

First Product: Cyber Microscope



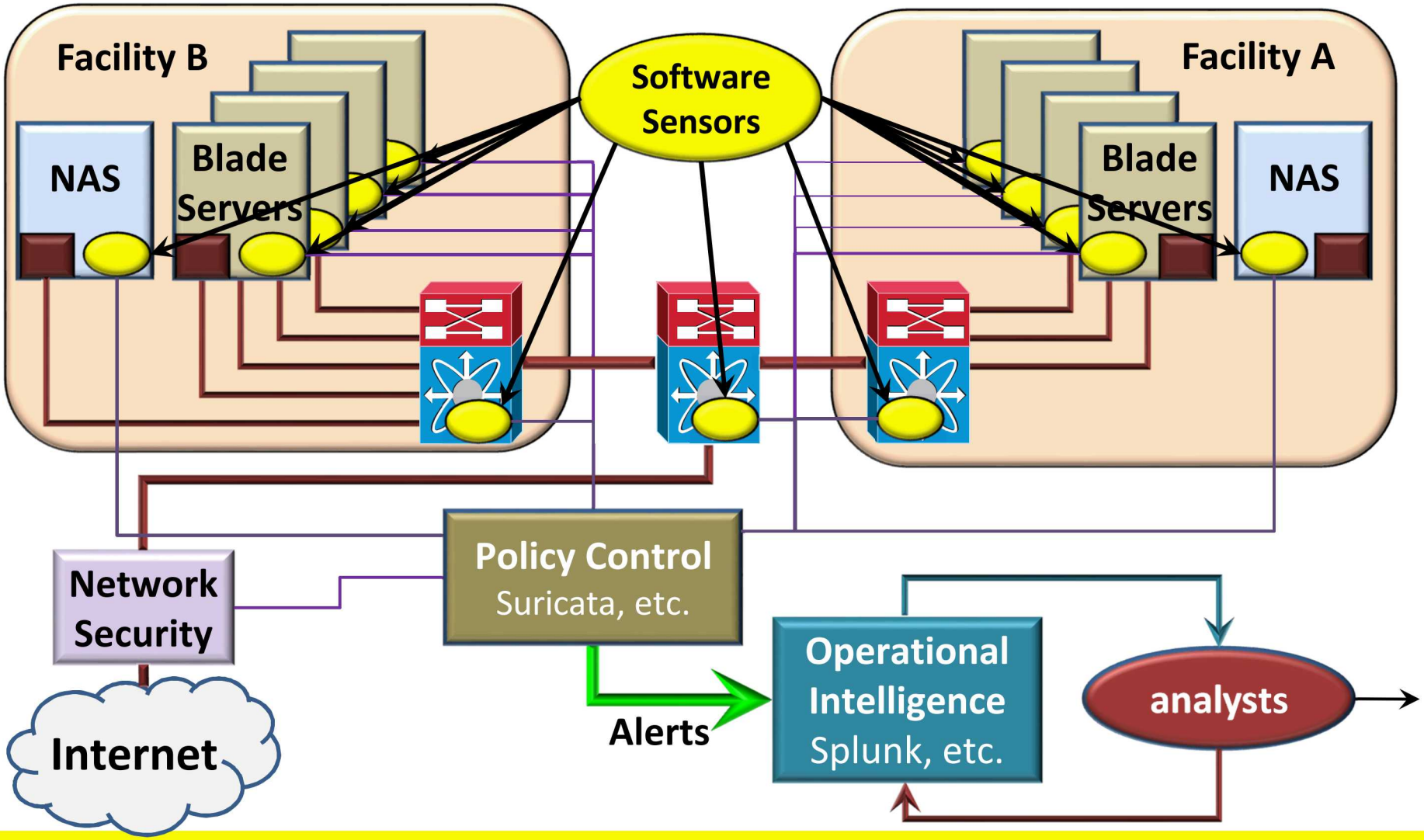
Some Interesting Features

- NPU integrates key mission requirements, ex.,
  - Context switching
  - Dynamic programmability
  - Behavioral characterization
  - Time & Order invariance
  - Pervasive analysis
  - Basic statistical operations
- Current device uses a single neuron type
  - Can extend HW architecture through novel neurons
  - Example: more complex statistical operations



CYBER APPLICATION

Exemplar Intel Community IDS

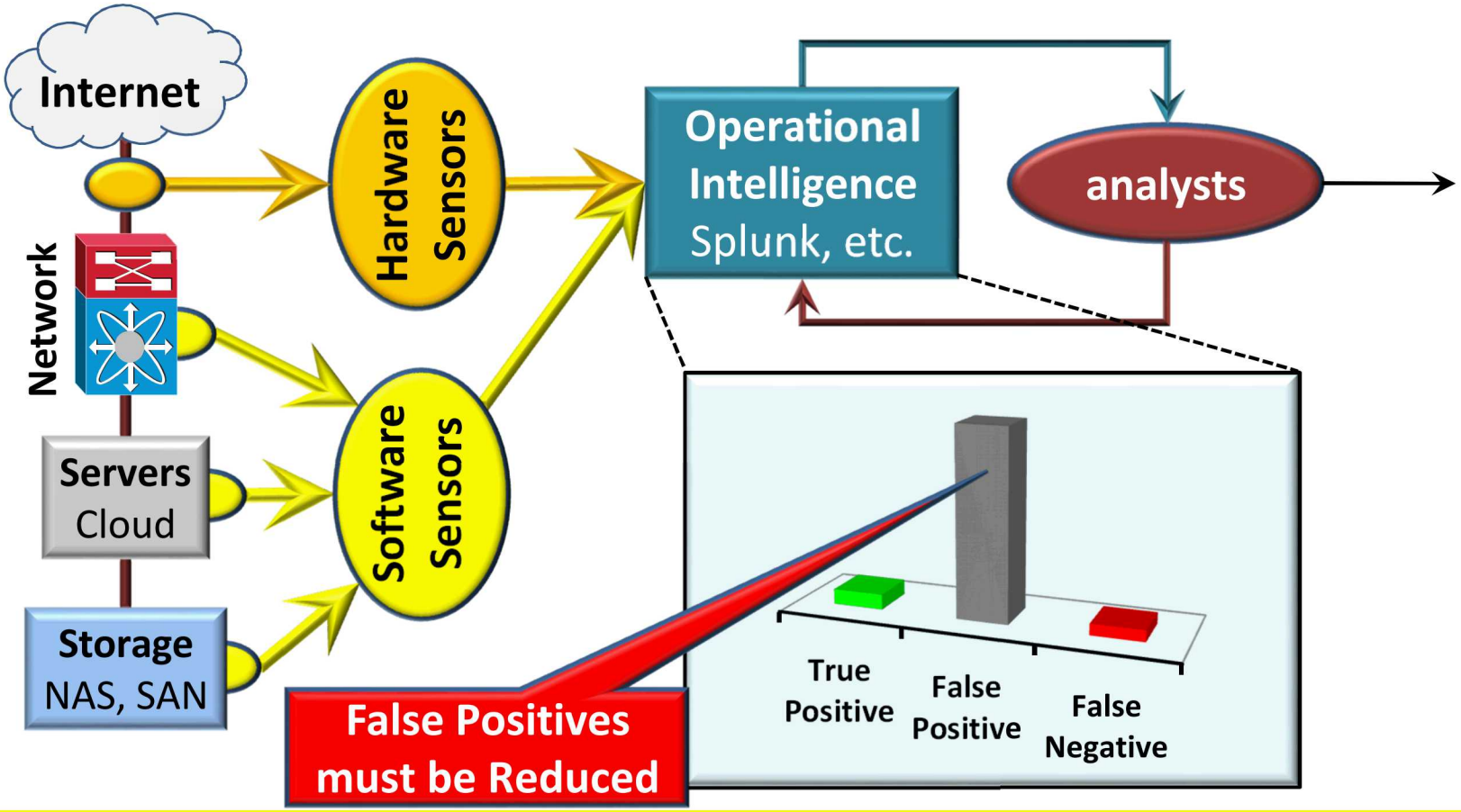


Practical Considerations

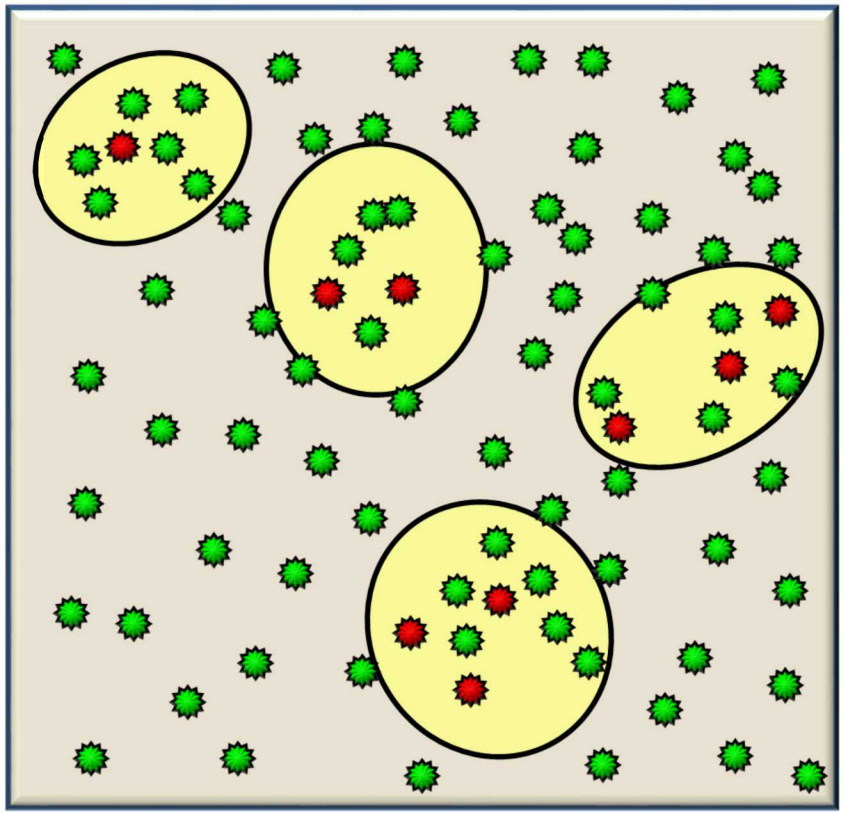
- Hardware sensor cost extremely high
  - ex. 10GbE IDS >$100k
  - Cost limits number & resolution of HW sensors
- Software sensors often resource intensive
  - ex. ROP detectors require most of the CPU
  - Cost limits number & resolution of SW sensors
- Analyst's priority, reduce False Negatives
  - Achieved by detuning sensors, ie. large # of False Positives
  - Major source of noise, direct result of sensor cost
- Detuned sensors are more vulnerable to attack
  - Spoofing & Flooding are common

Analyst's Top Priority

Signal/Noise is killing analyst community



Root Cause: Resolution



True Positives (**TP**)
Potential False Positives (**FP**)
Expression Coverage

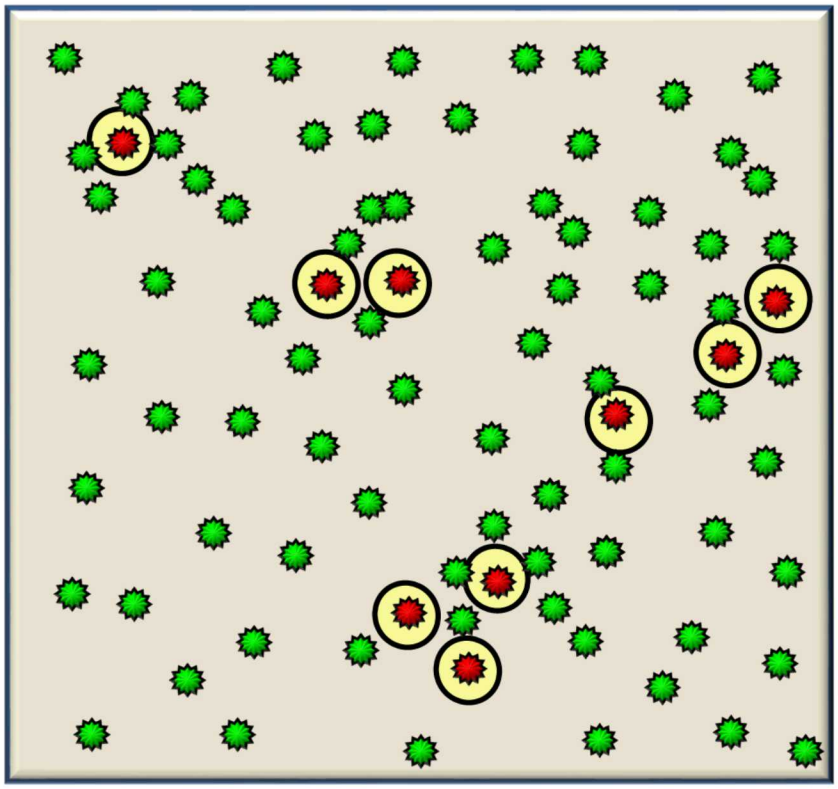
State-of-the-Art Sensors

ex. **Suricata**

- **Cost** limits resolution
- **TP**s identified but
- Many **FP**s captured
- Splunk database,
  - Low Accuracy
  - Poor signal/noise ratio
  - It's still a haystack
- **S/N** is killing the analysts

Neuro: Resolution

Cyber Microscope



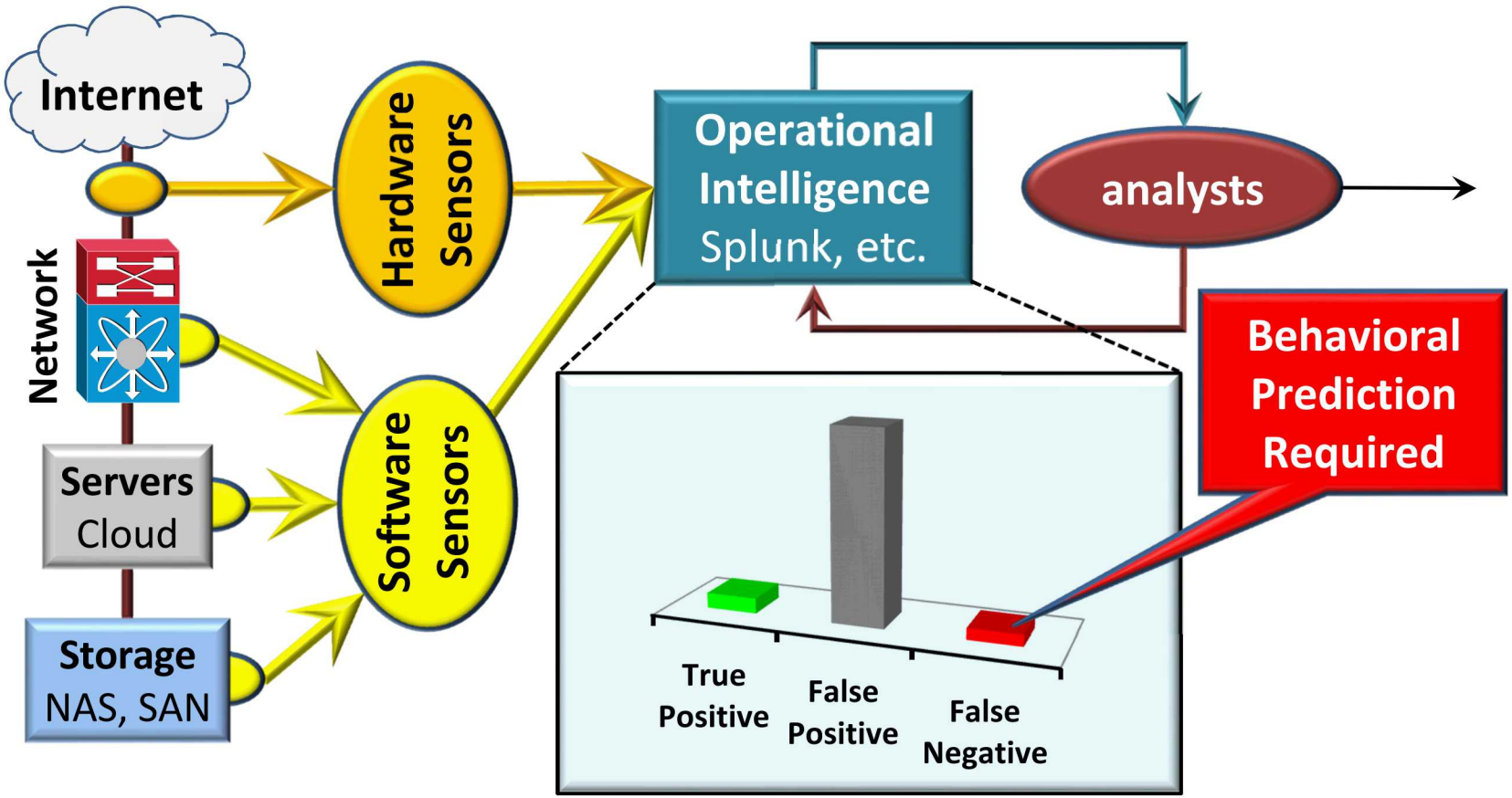
True Positives (**TP**)
Potential False Positives (**FP**)
Expression Coverage

Neuromorphic

- Speed creates resolution
  - Same number of **TP**s
  - Dramatically fewer **FP**s
- Greater Accuracy
- Higher Signal/Noise ratio
- Profound impact on analysts

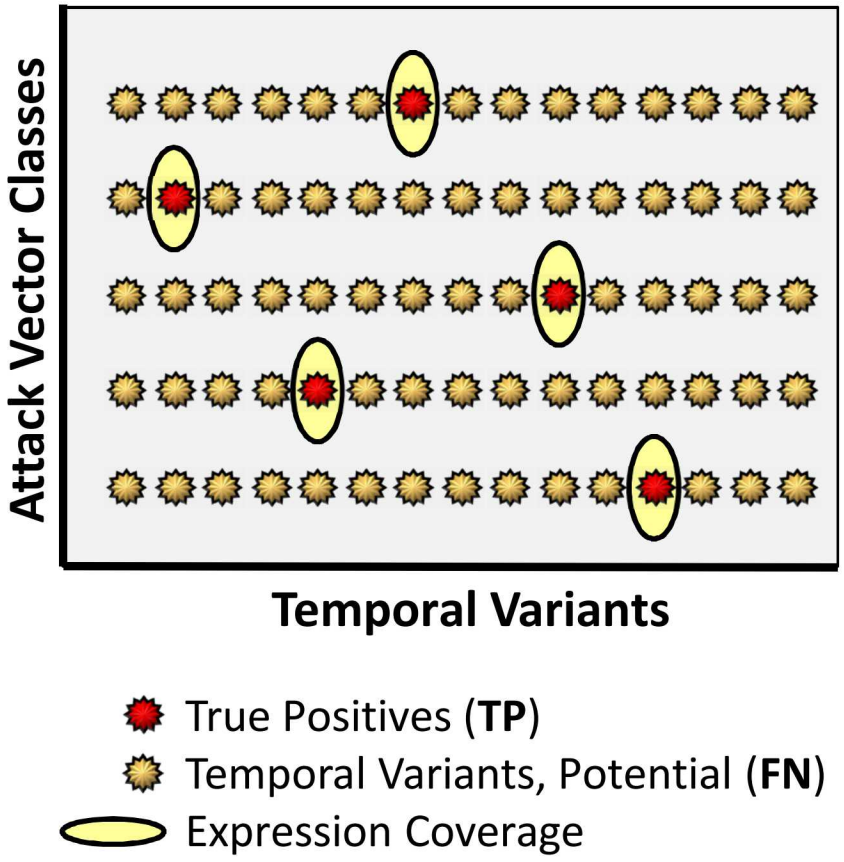
Analyst's Second Priority

Reduce False Negatives



Root Cause: Temporal Variance

Simplest form of behavior prediction

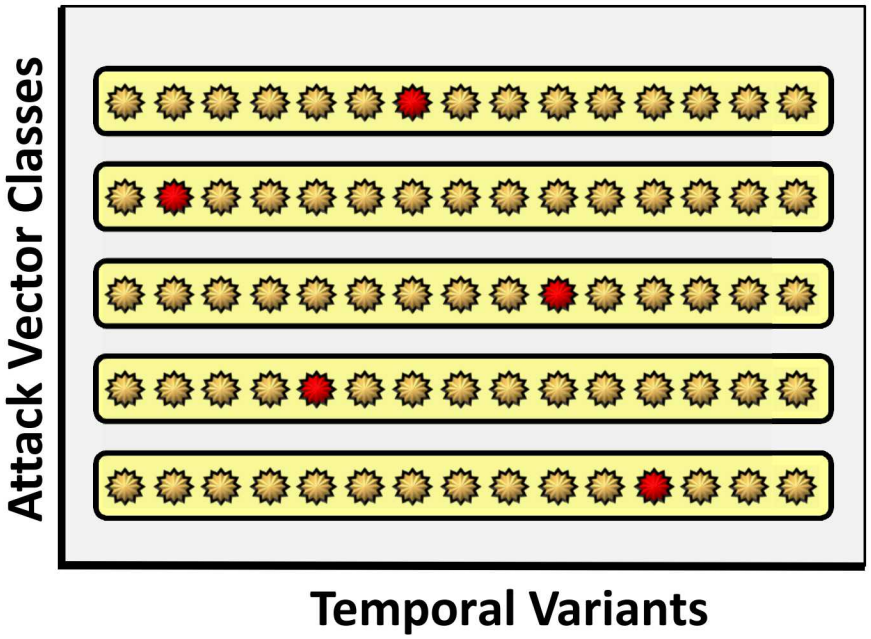


State-of-the-Art Sensors

ex. **Suricata**

- Temporal variance is common
  - Shifting offsets
  - Re-ordering
  - Easily implemented by attacker
- Very **costly** to address
  - Pervasive analysis
  - Associative analysis

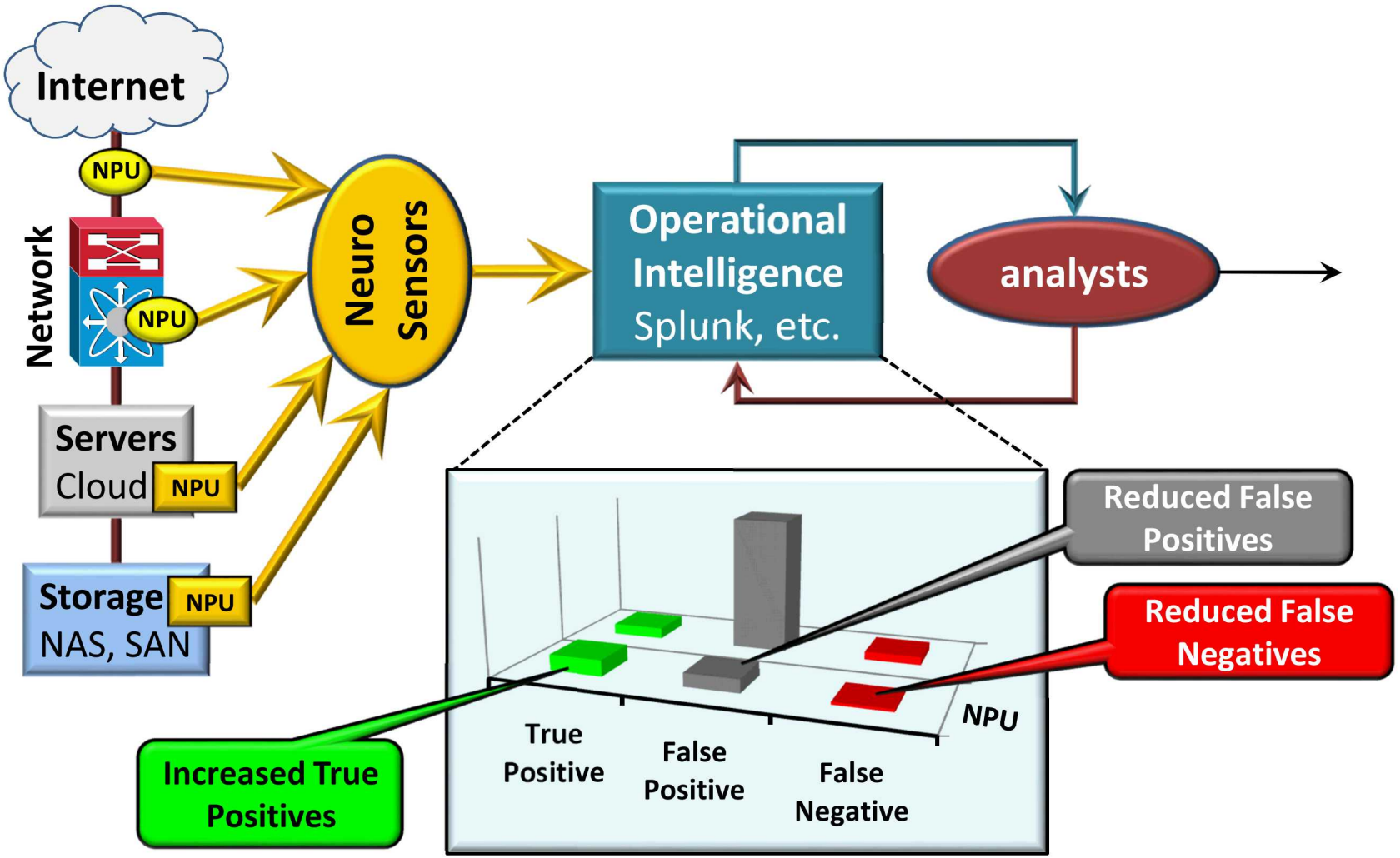
Neuro: Temporal Variance



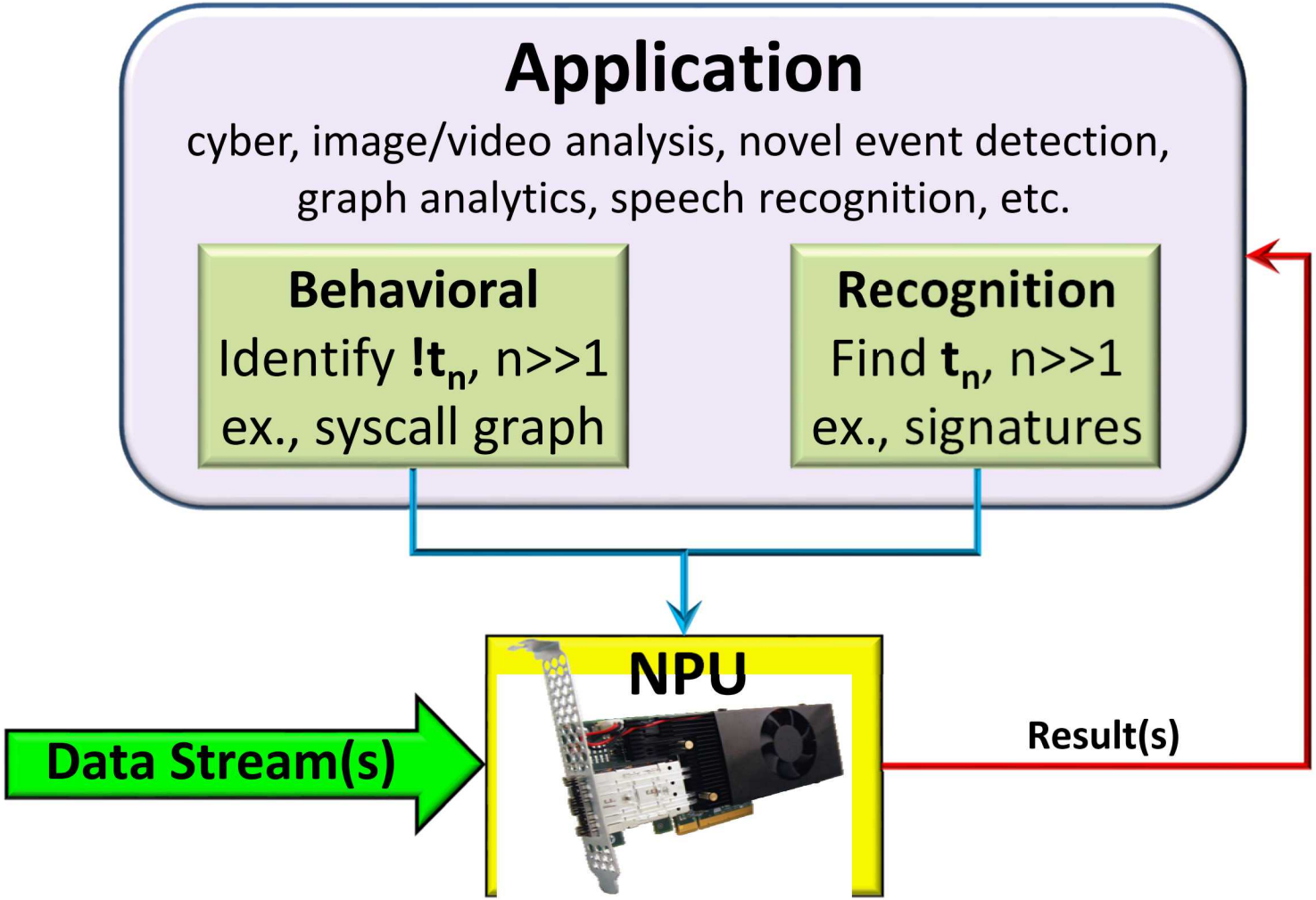
Neuromorphic

- Pervasive analysis is innate
  - Evaluates every byte
  - Limiting this costs resources
- Associative analysis is innate
  - Metadata reordering
- Reduced False Negatives **FN**
  - Behavioral Prediction
- Profound impact on Analysts

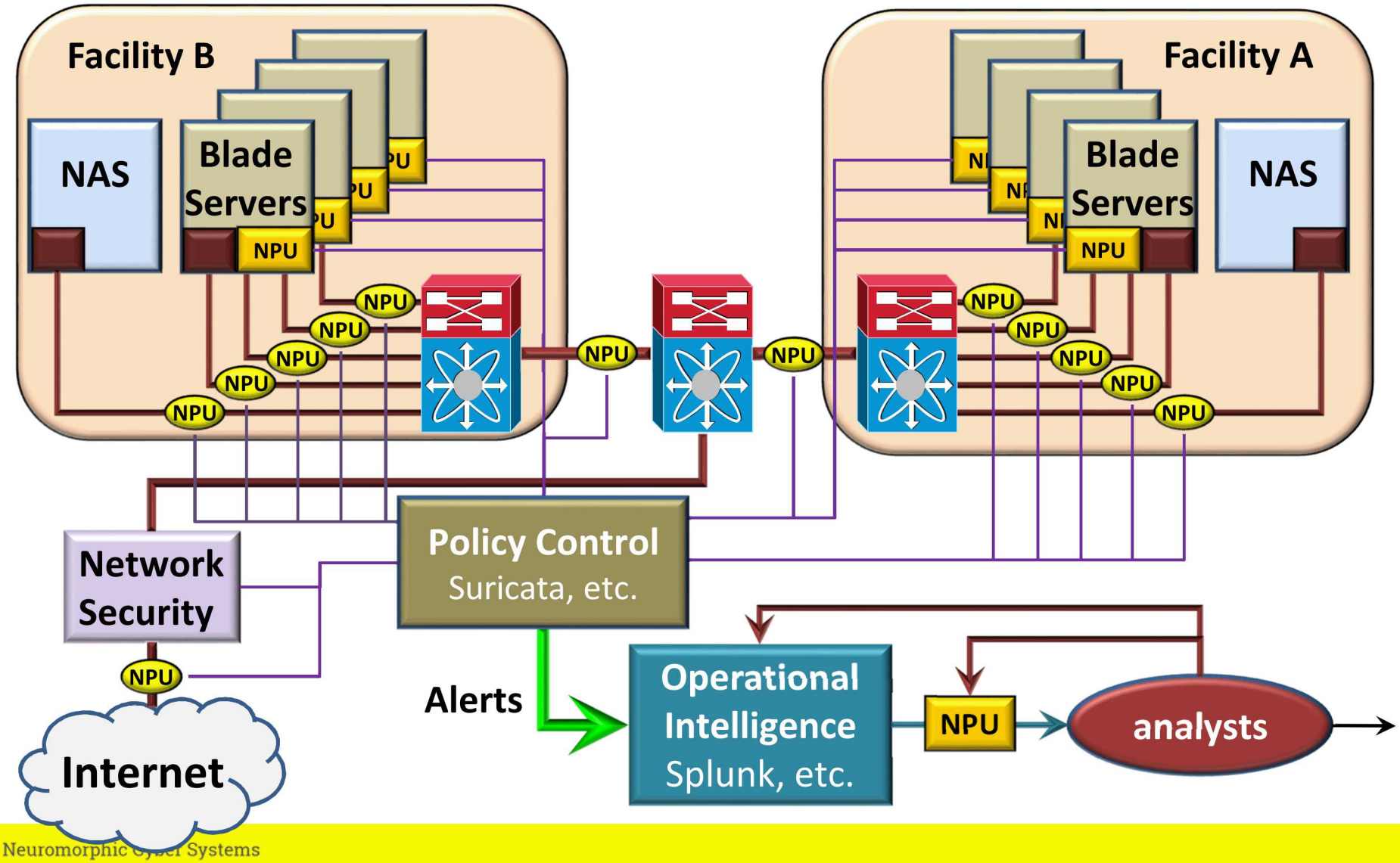
Neuro Addresses Core Issues



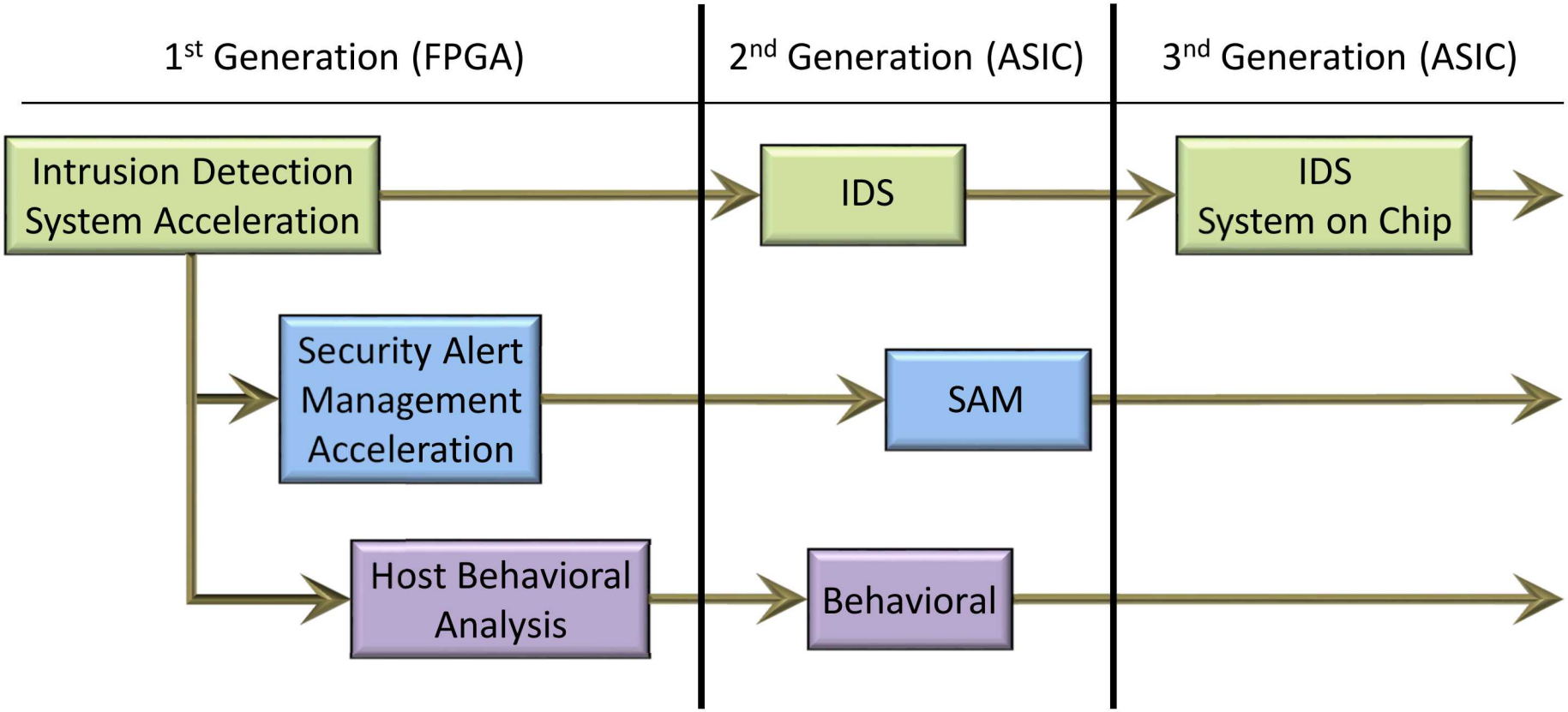
Operational Control



IC Analyst's Vision



Cyber Microscope Product Rollout



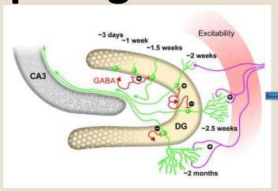
Acknowledgements

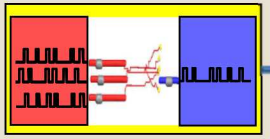
Neuroscience 1998 - 2012

Sandia LDRD 2013 - 2014

HAANA 2015 - 2017

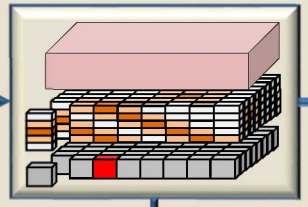
Neuronal Spiking Models

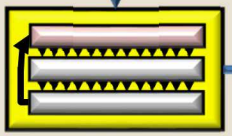




Neuronal Information Theory

STPU



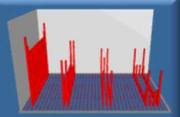


NPU

State Density $(n/m)^m$

Behavior Prediction

Pre-Attentive Processing



PCRE

$/Performance >100,000x
Behavioral Lexicon
Pervasive Analysis
Dynamic Reconfiguration

BECCA

$/Performance >100,000x
Power <100,000x
Weight <1,000,000x

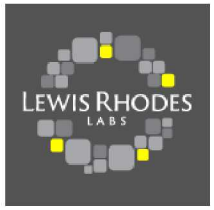
Neuromorphic Signal Processing
Image/video
Mixed Telemetry

Behavioral Analysis
Forensics
(aka *learning*)
Prediction

Neuromorphic Filters/Sensors
->Cyber<-
Big Data
Telemetry

Conclusions

- Neuromorphic will revolutionize cyber defense
  - Dramatic reductions in power/op & cost/op
  - Plethora of powerful novel features
    - Order & time invariant, Sessionization, Behavioral prediction
- Operational readiness
  - Compatible with existing standards & infrastructure
  - 3rd gen FPGA systems available now
  - First 3rd party port, “WaterSlide” Kid



BACKUP

Scalability

Device

Bandwidth x Expressions = Constant

FPGA

2.5 Gb/s x ≈ 1,000 Expressions
5 Gb/s x ≈ 500 Expressions
10 Gb/s x ≈250 Expressions
etc.

ASIC

20 Gb/s x ≈ 20,000 Expressions
40 Gb/s x ≈ 10,000 Expressions
80 Gb/s x ≈ 5,000 Expressions
etc.

System

Arbitrary Depth & Width