The Future of Threat Prevention

Bricata is the leading developer of Next Generation Intrusion Prevention Systems (NGIPS) technology, providing innovative, disruptive, high-speed, high-performance network security and data protection solutions.

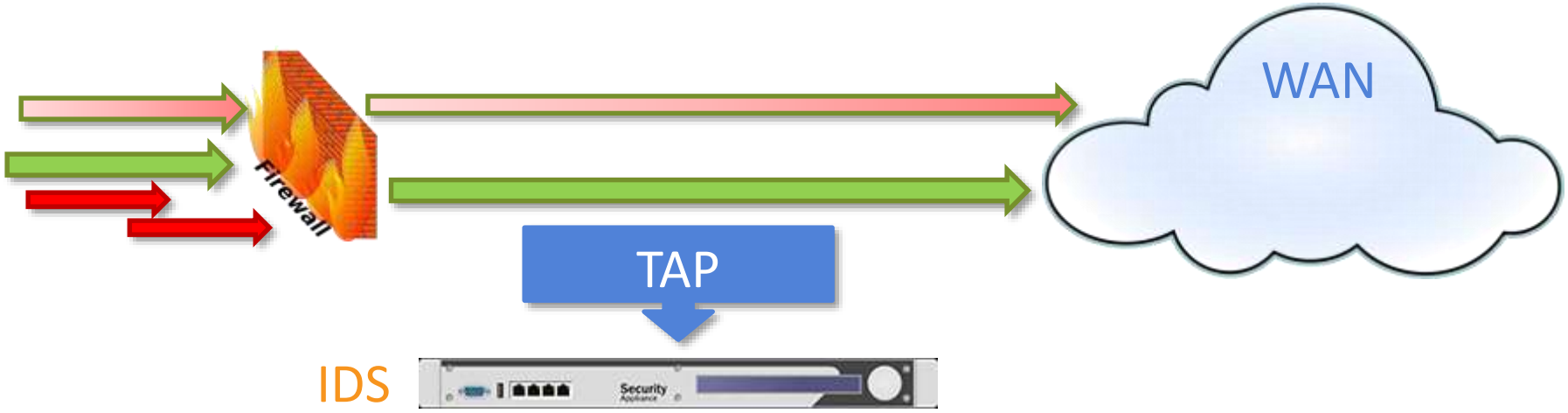
Yasser Mohamed| Senior Sales Engineer

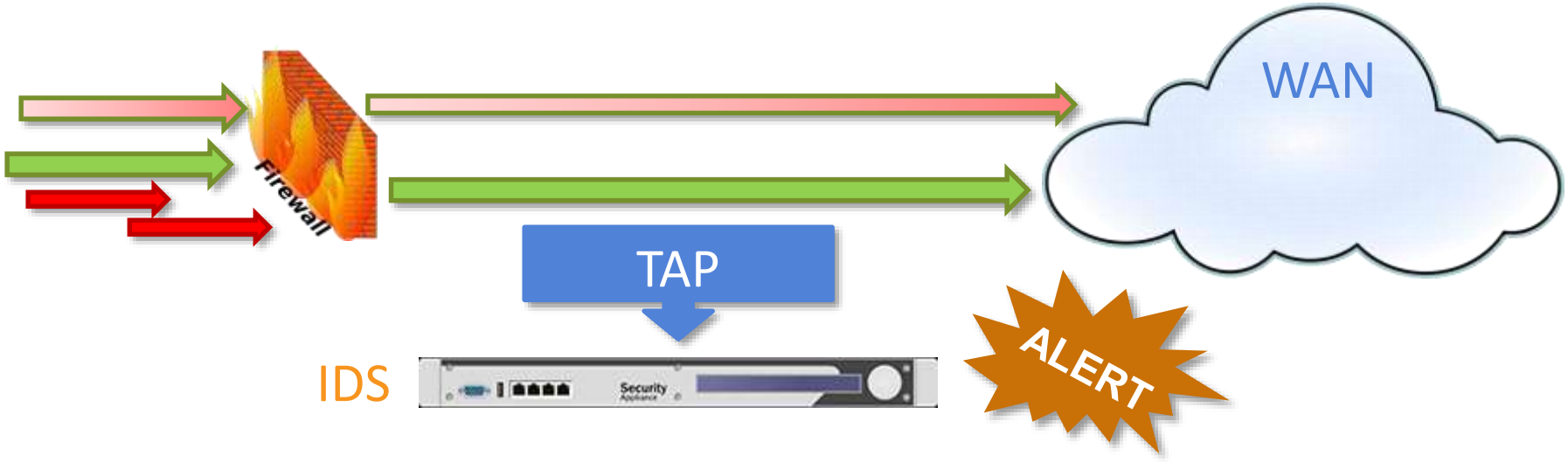
About Bricata - Overview

- Where IDS came from
- How IPS is different
- Current threat landscape and challenges
- How Bricata is different
- Live demo


Firewall
WAN


Firewall
WAN

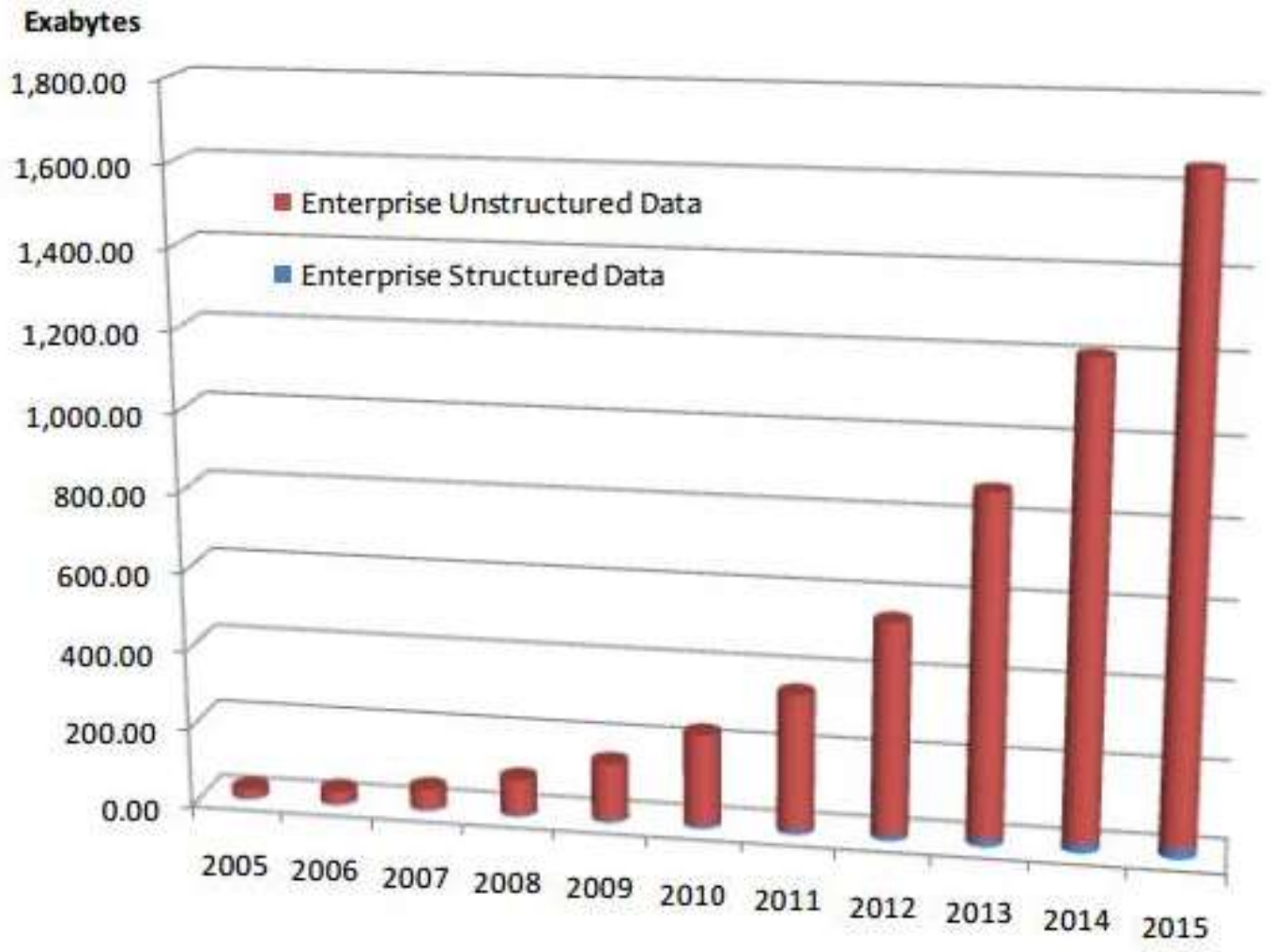

WAN
Firewall
TAP
IDS
Security



- Passive system
- Traffic still passes to destination
- Limited to alerting or TCP resets

- Active system
- Sits in-line and can stop attacks immediately
- Signature based
- Some include heuristic and anomaly detection

Enterprise Data Growth 2005-2015

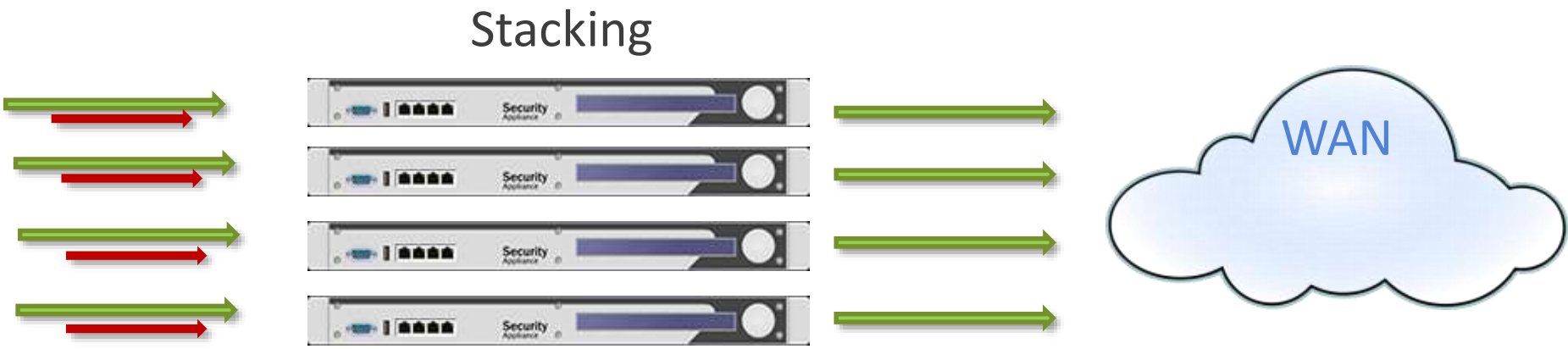


Source: IDC

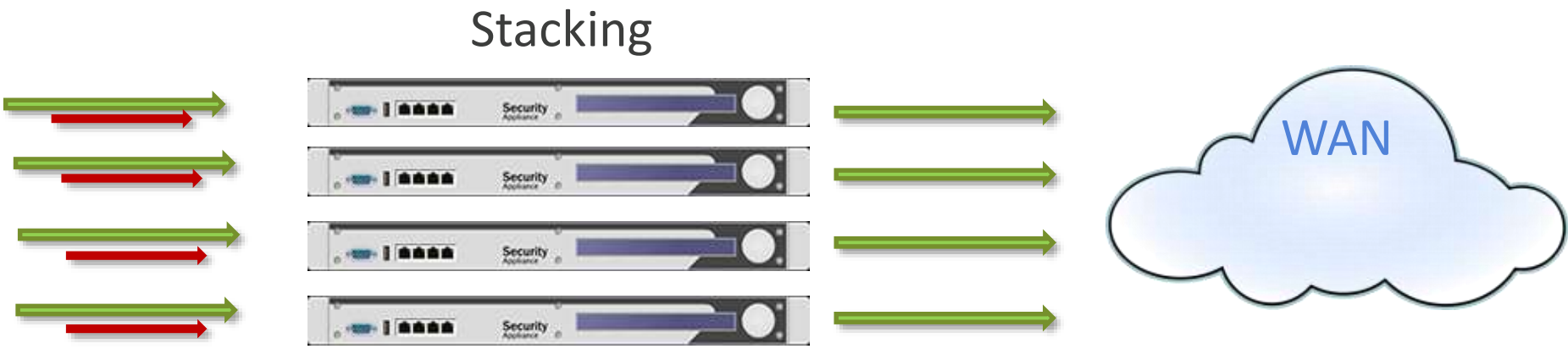
Data Growth means more data to inspect and process.

Legacy IPS solutions cannot handle the traffic alone.

To keep up with traffic flow increases, devices are stacked.

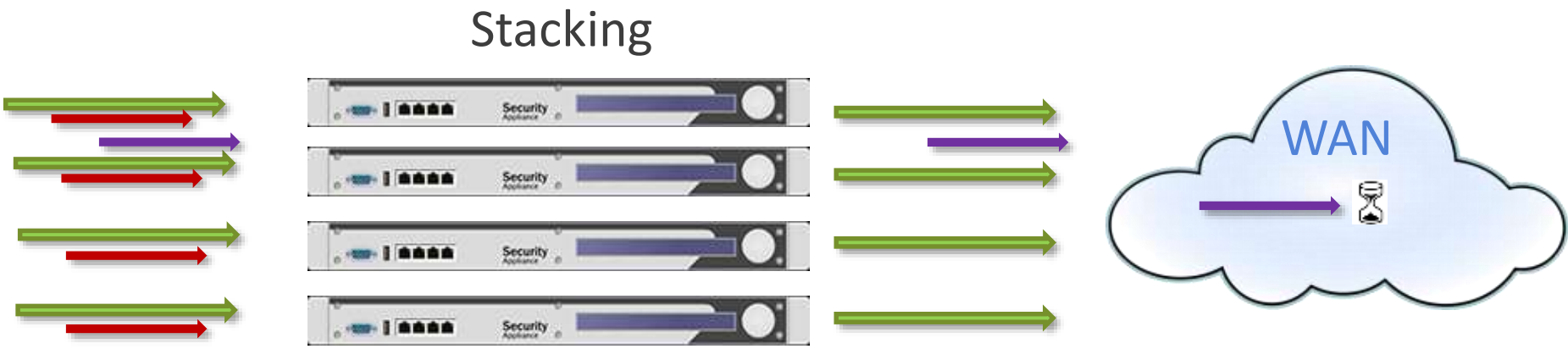


To keep up with traffic flow increases, devices are stacked.

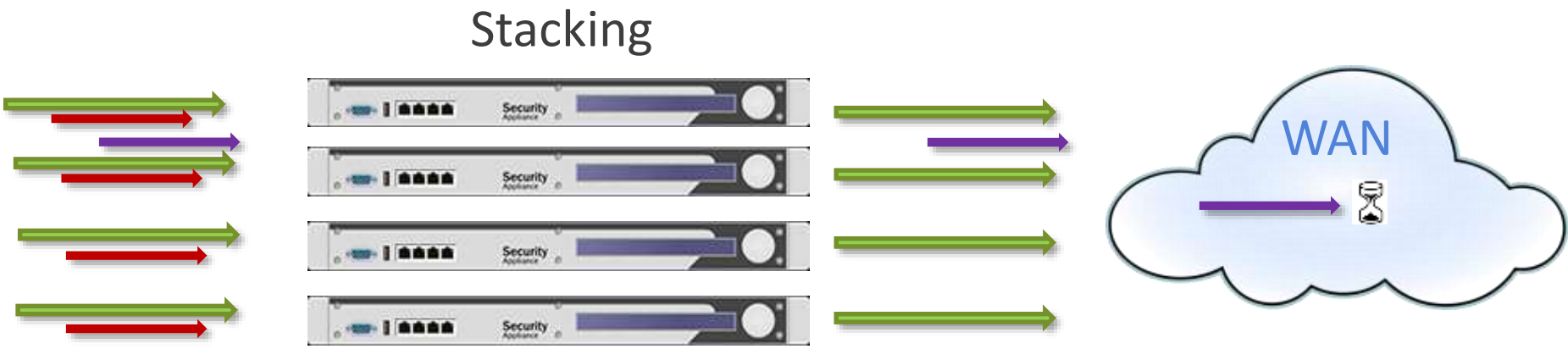


- Expensive
- Hard to manage
- Takes up a lot of space

IPS systems are needed to stop 99% or more of known attacks.
But targeted “Zero-Day” attacks can still compromise organizations.



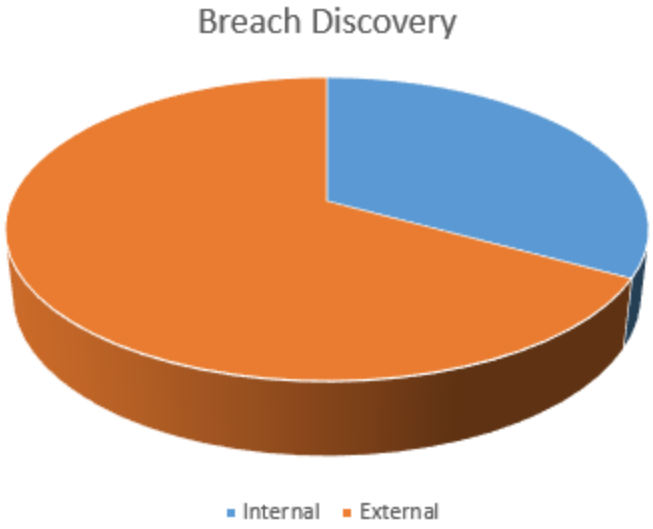
IPS systems are needed to stop 99% or more of known attacks.
But targeted “Zero-Day” attacks can still compromise organizations.



- More sophisticated attackers
- Designed to evade most security devices
- Time-delay execution
- Can persist and grow for months or years

2014 Threat Report

66% of organizations were notified of a breach by an *external entity*



229 Days

Median number of days attack groups were present on a network before discovery

Source: Mandiant 2014 Threat Report

The Bricata Difference

Ultra High-Speed Performance

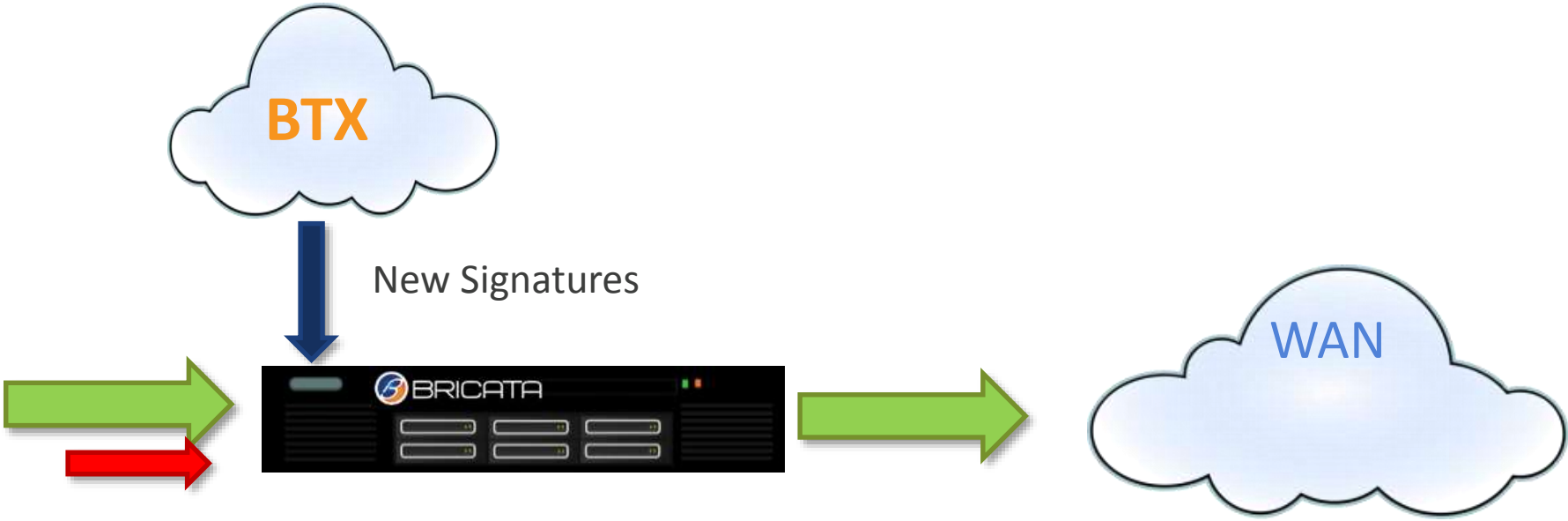
Stacking

8 RU
60 Gbps

4 RU
100 Gbps

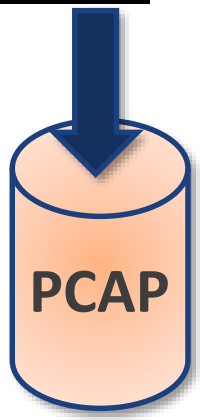
Deployed in-line as an active IPS solution
Speeds range from 500 Mbps to 300 Gbps

- Much smaller footprint
- Lower cost
- Lower operational expenses
- Easier to manage


BTX
New Signatures
BRICATA
WAN

Simplified GUI

New Signatures



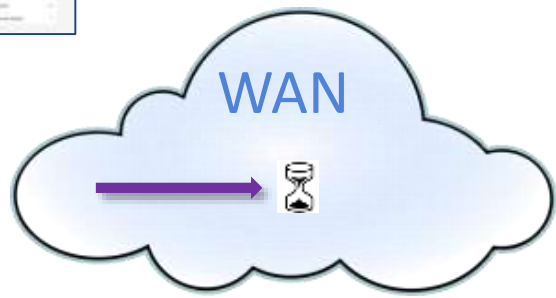
- Full payload and metadata
- 1 click query to pull PCAP
- Rapid investigation
- Open format
- Session reconstruction

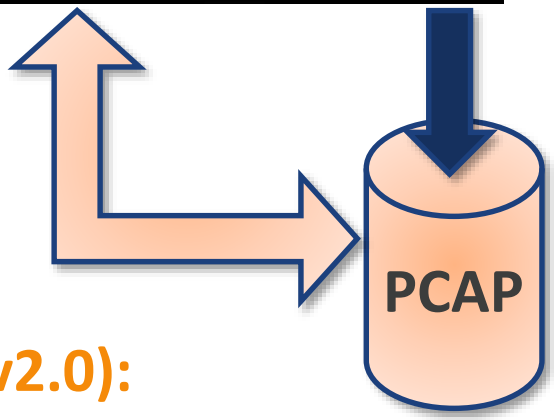
Contextual understanding of security incidents

Simplified GUI

Unknown Threats

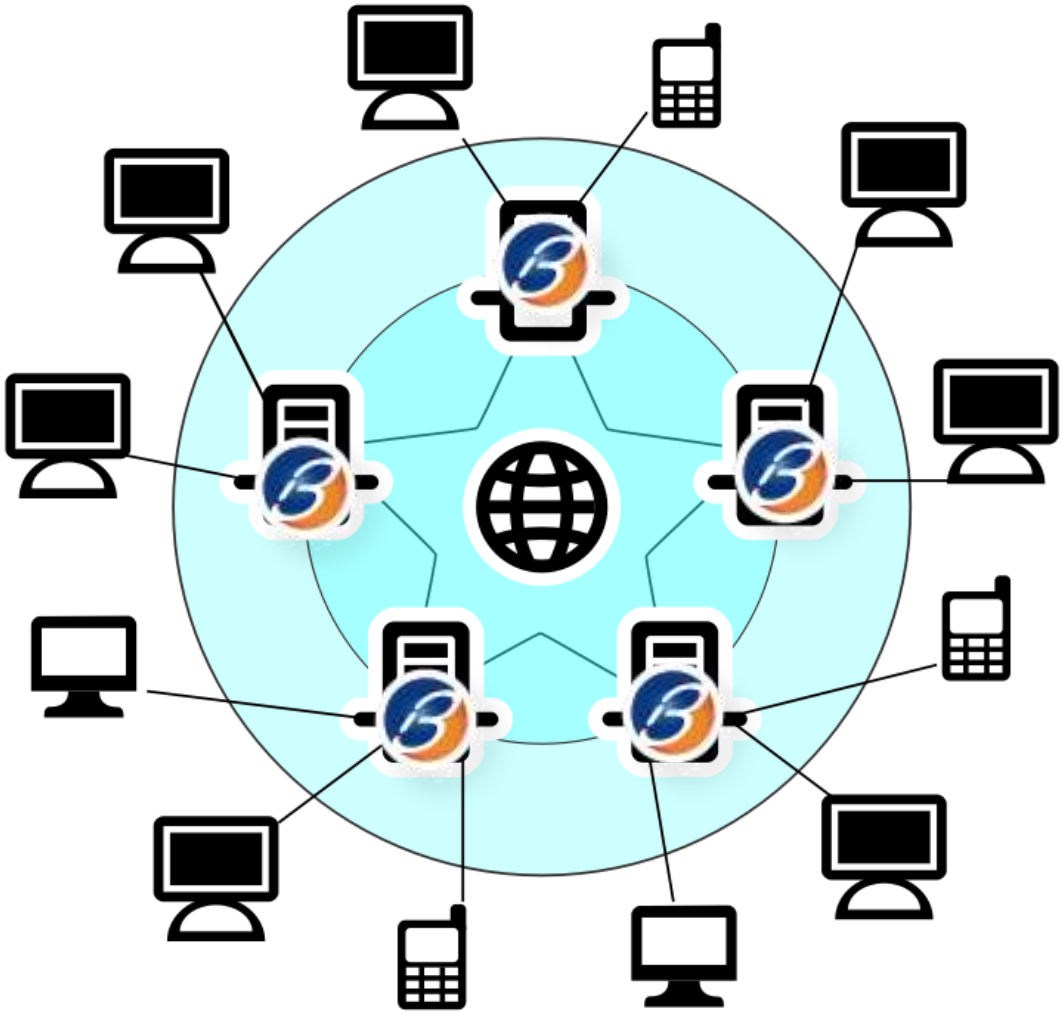
New Signatures

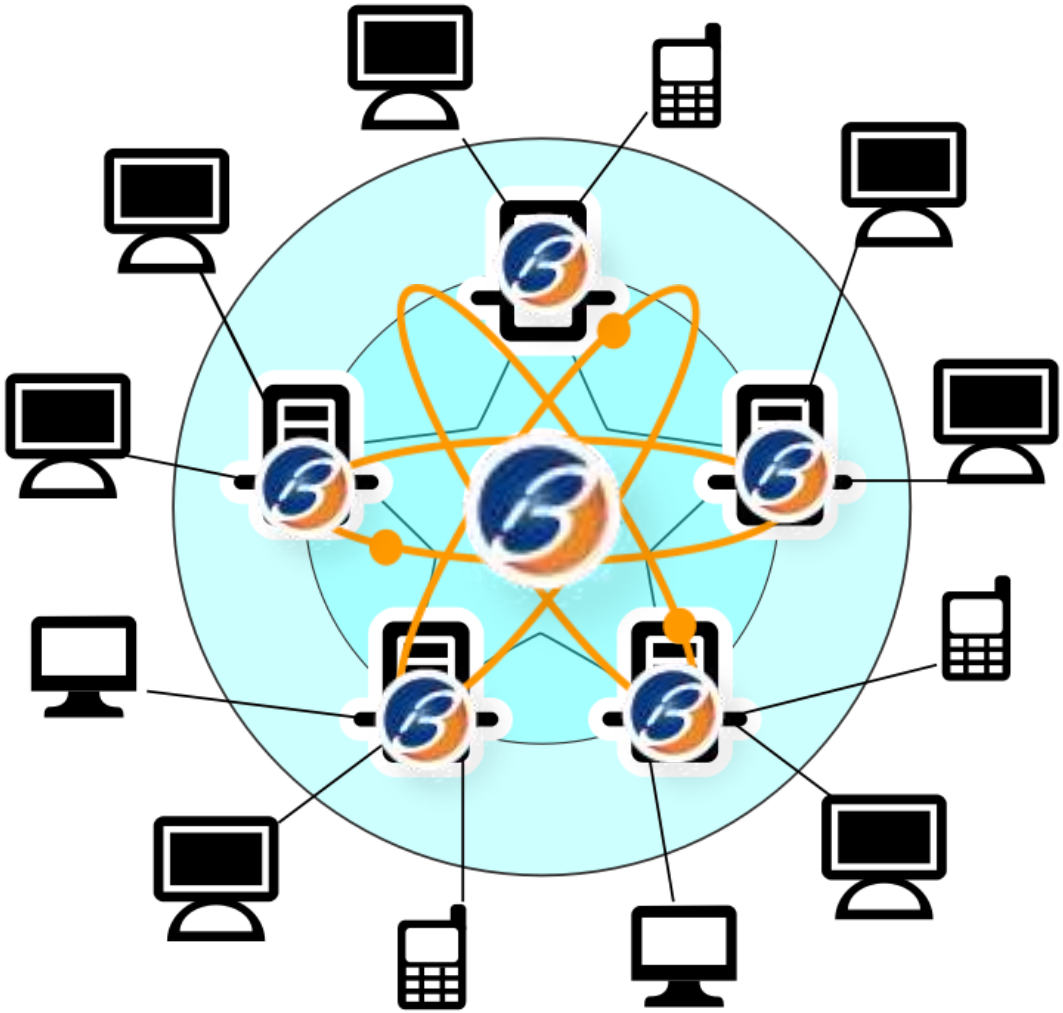


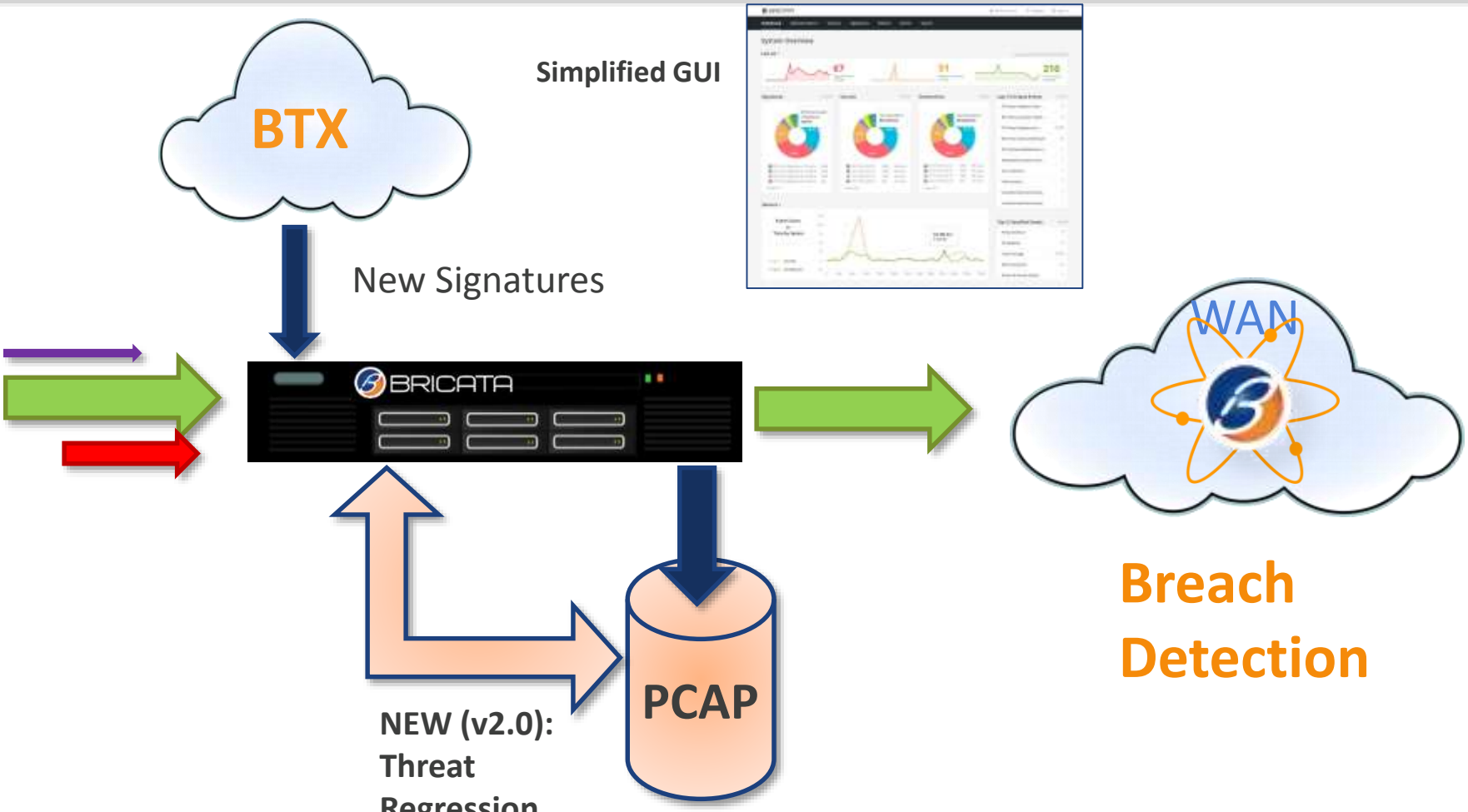


What do we know today that we didn't know yesterday

NEW (v2.0):
Threat Regression

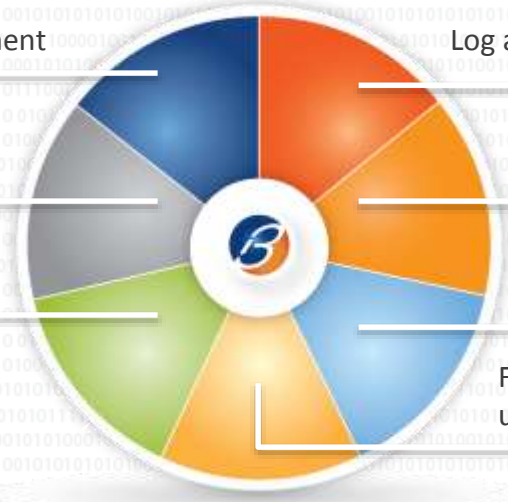





BTX
Simplified GUI
New Signatures
BRICATA
WAN
Breach
Detection
PCAP
NEW (v2.0):
Threat
Regression

Bricata ProAccel NGIPS Feature Set At-a-Glance

Threat Isolation Engine™



Traffic monitoring & event management

Cassandra data analytics engine

Central management console (CMC) for complete dashboard control

Log aggregation, correlation & forwarding to SIEM

Regularly updated signature library & threat intelligence sharing

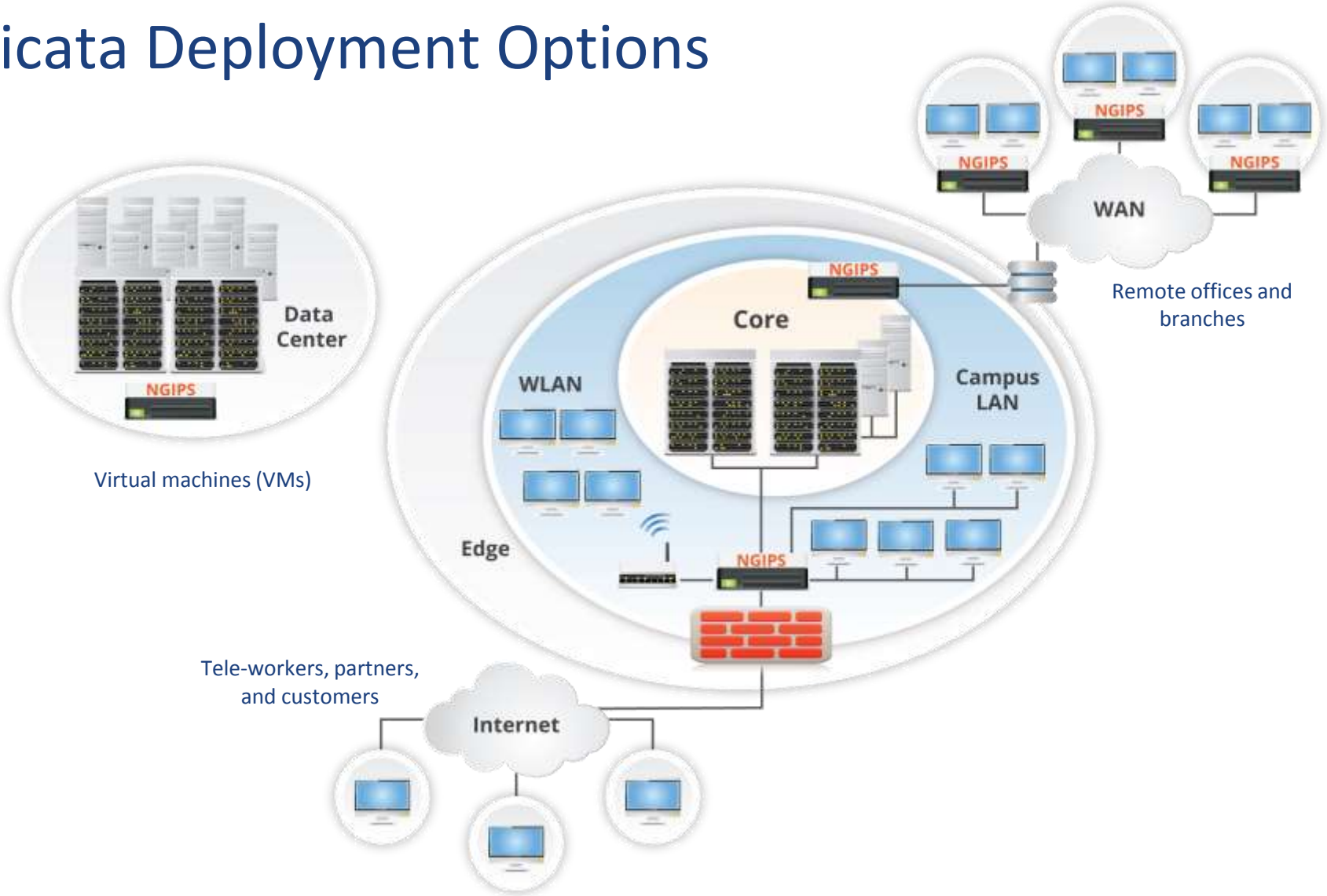
Data exfiltration prevention automation

Full packet capture for complete contextual understanding of security incidents

- Malware, vulnerabilities that are known and unknown
- Threat Intelligence Eco-system
- Port/Protocol independent inspection
- Custom signature creation
- GeoIP reputation & location

- Signature-less detection via Anomaly-based Decision Module
- Application awareness
- Full packet capture, NetFlow and contextual analytics
- Highly scalable global event management
- Event aggregation, correlation and forwarding

Bricata Deployment Options



Why Bricata:

The New, Smarter Breed of Automated Threat Defense

- Reduced costs by as much as 50% over legacy IPS solutions
- Created by leading NGIPS experts in the security industry
- Offers High-speed IPS, full packet capture, and breach detection
- Exceeds feature parity of other leading NGIPS vendors
- Leverages your existing FW investment
- Improves visibility from the core to the perimeter
- Ease of deployment and management
  - All legacy SNORT and Suricata rule sets can be ingested with no rewrite
- Zero Day Threat detection with our Anomaly-based Decision Module

Demonstration