

Who am I?

Breaking things since I was 12

Consulting Security Architect

I get to break things and help fix them

Other interests: traveling, hockey, snobby
beer, and my bulldog

#cyberspice

Networks are Failing Us

They work too well
We have a global network of interconnected devices that can communicate with each other in a way that is almost instantaneous. This is a double-edged sword. While it allows us to connect and share information, it also makes it easier for attackers to spread malware and launch attacks.

They don't work well enough
Networks are complex and fragile. A single point of failure can bring down an entire network. And even when they do work, they often do so at a cost. Network congestion, latency, and security vulnerabilities can all impact the performance and reliability of our networks.

...And how often do all of these things happen in the night?

Software Defined Networking

Abstraction of the network plane and data plane from the hardware. The control plane is moved to a centralized location, and the data plane is distributed across the network devices.

What's out there and how does it work?

So why do we care?

Networks control the way we interact with the world. They are the backbone of our society. If they fail, our lives are disrupted. We need to understand how they work and how to protect them.

Let's Connect to Blue

Let's talk dynamic security...

Location-based access control
- Mobile devices are always connected to the network.
- Consider which user applications connect and where they connect.
- Monitor network. Application controls in security and regulation.

Proactive measures based on patterns using machine learning
- Detect and respond to threats in real-time.
- Monitor network traffic.
- Monitor user behavior.
- Monitor device health.

Where are all the SDN Talks?
Because Skynet can defend itself now!

Jon Medina
protiviti
Take the Future with Confidence

Who am I?

Breaking things since I was 12

Consulting Security Architect

I get to break things and help fix them

Other interests: traveling, hockey, snobby
beer, and my bulldog

#cyberspice

Networks are Failing Us

They work too well!
They don't work well enough!
...And how does this all come together in the cloud?

Software Defined Networking

And what about the cloud?
The cloud is not a magic box.
The cloud is not a magic box.
The cloud is not a magic box.

What's out there and how does it work?

So why do we care?

...And how does this all come together in the cloud?

Let's talk dynamic security...

...And how does this all come together in the cloud?

Where are all the SDN Talks?
Because Skynet can defend itself now!

Jon Medina
protiviti
For the Future with Confidence

Who am I?

Breaking things since I was 12

Consulting Security Architect

I get to break things and help fix them

Other interests: traveling, hockey, snobby
beer, and my bulldog

#cyberspice

Networks are Failing Us

They work too well

- Things are talking that shouldn't be
- We have to actively PREVENT systems from talking to each other
- Have you seen a firewall rule list lately?

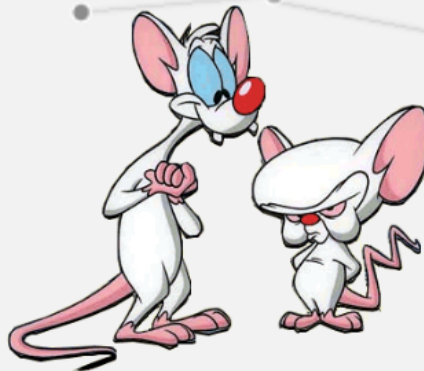
They don't work well enough

- Applications have no network visibility
- Network hardware is getting complicated
- Infrastructure deployment is costly and inefficient
- Network devices are expensive

...And how does this all come together in the cloud?

Software Defined Networking

- Abstraction of the control plane and data plane from devices.
- The brains of network device functions are moved to a centralized location.
- This is *not* NFV



Switch Controller

ctions are

What's out there?

- Companies with closed source implementations:
 - Cisco Application Centric Infrastructure (ACI)
 - VMware NSX
- Companies with Open Source OpenFlow implementations:
 - Juniper
 - HP
 - Arista
 - Big Switch
 - ...and dozens more

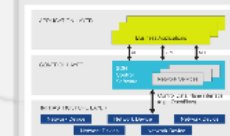
This is not a new technology
Google, Amazon, Facebook, NSA, most telcos have been using it for years

What's out there and how does it work?

Go with the flow



SDN Architecture



Core Concepts

- Controller sends flows (think ACLs) to switches
- Switches forward traffic based on flows
- If a switch doesn't have a flow that matches a packet, it asks the controller
- The controller either sends a new flow to the switch, or the packet is dropped



What's out there?

Companies with closed-source implementations:

- Cisco Application Centric Infrastructure (ACI)
- VMWare NSX

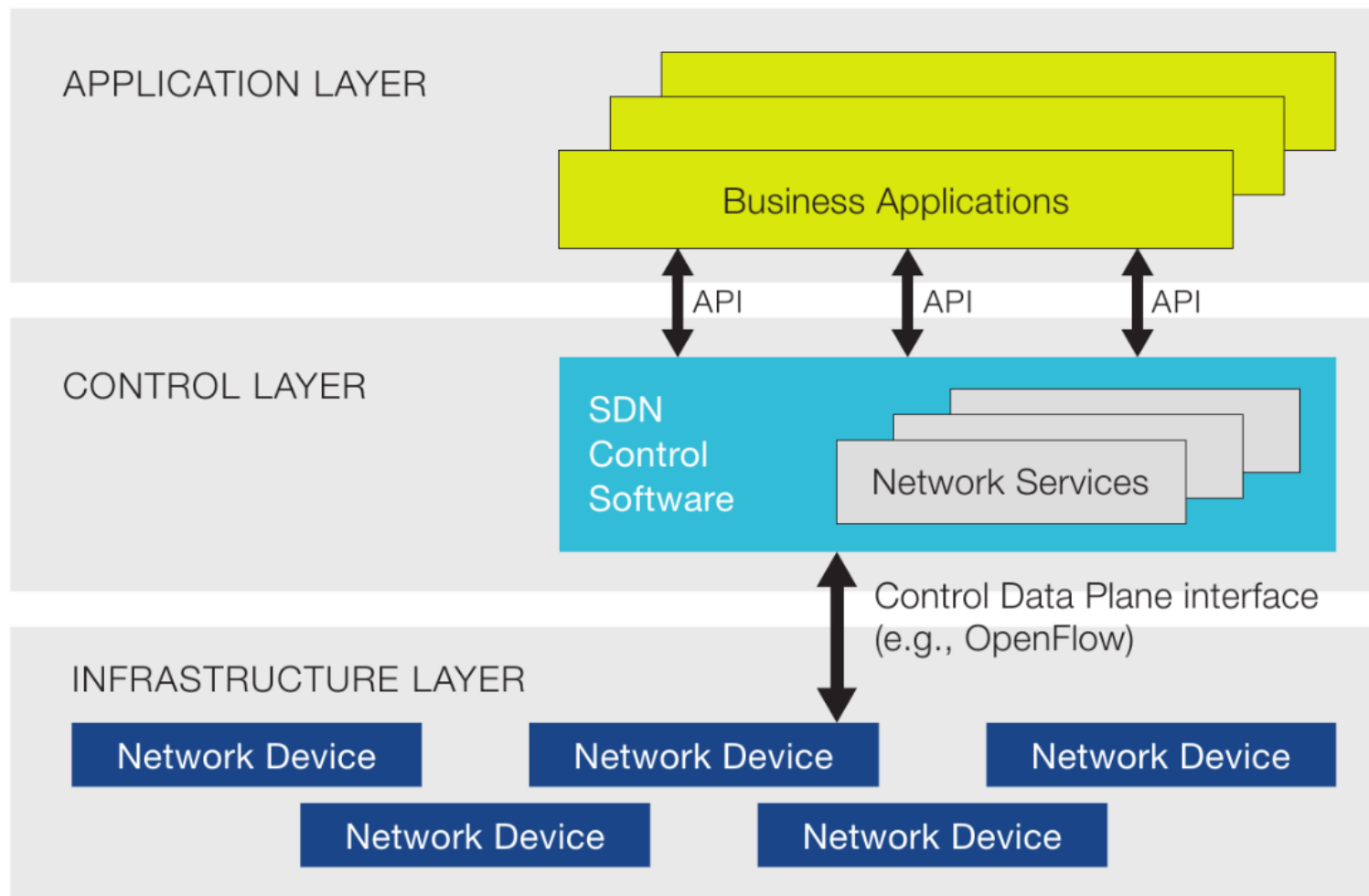
Companies with Open Source Openflow implementations:

- Juniper
- HP
- Avaya
- Big Switch
- ...and dozens more

This is not a new technology

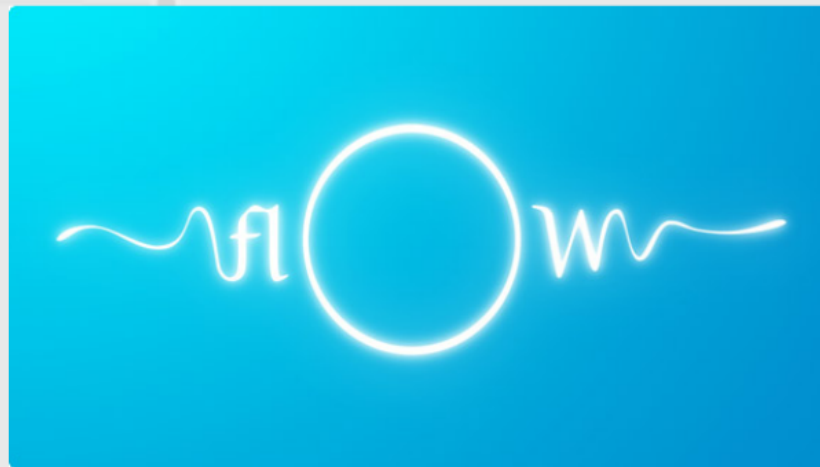
Google, Amazon, Facebook, NSA, most telcos have been
using it for years

SDN Architecture

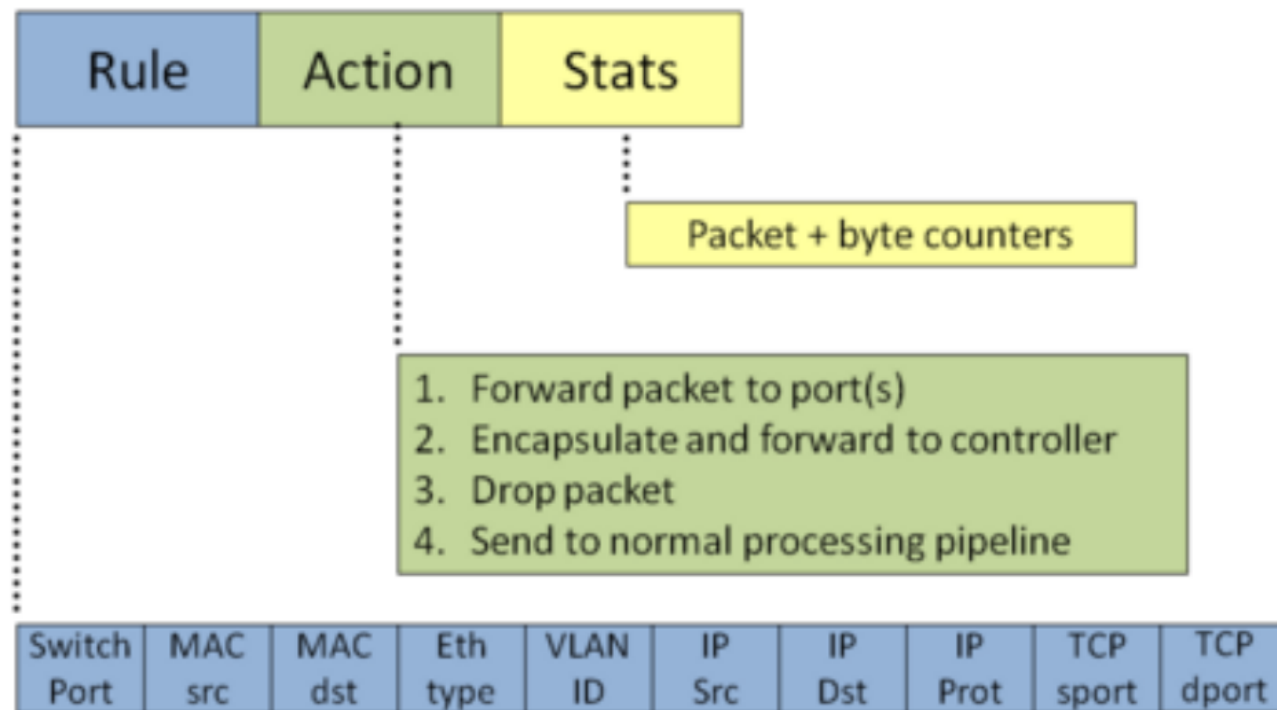


Core Concepts

- Controller sends flows (think ACLs) to switches
- Switches forward traffic based on flows
- If a switch doesn't have a flow that matches a packet, it asks the controller
- The controller either sends a new flow to the switch, or the packet is dropped



Go with the flow





Let's Check it Out

So why do we care?

- Absolute control over every aspect of network traffic
- Traffic policies can be applied globally to users and systems
- We can make dynamic decisions about how to treat network traffic based on every layer of the OSI model
- Flow tables created within flow tables

The background of the slide features a network diagram with a central circle and a thick gray border. Inside the circle, there are several small gray dots connected by thin gray lines, forming a network structure. The dots are distributed around the circle, with some lines extending towards the edges of the frame.

Security Use Cases

- What network ports are users ACTUALLY using? Do users really need to communicate with each other?
- How do you limit access by vendors and outsiders connected to your network?
- How do you control what devices are connected to your network, and how do you handle BYOD? IOT?

Who am I?

Breaking things since I was 12

Consulting Security Architect

I get to break things and help fix them

Other interests: traveling, hockey, snobby
beer, and my bulldog

#cyberspice

Networks are Failing Us

They work too well!
They don't work well enough!
...And how does this all come together in the cloud?

Software Defined Networking

And what about the cloud?
The cloud is not a magic box.
The cloud is not a magic box.
The cloud is not a magic box.

What's out there and how does it work?

So why do we care?

...And how does this all come together in the cloud?

Let's talk dynamic security...

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

Where are all the SDN Talks?
Because Skynet can defend itself now!

Jon Medina
protiviti
For the Future with Confidence

Let's talk dynamic security...

- Location based access control
- Multi-factor network authentication
- Granular control over application communications and cloud interactions.
- Vendor agnostic deployment assists in security tool-mageddon

Provision resources based on patterns using machine learning

- User and Service Account Behaviors
- Network traffic patterns
- Bandwidth consumption
- Application usage

- **Introducing....
Apache Spot (Incubating)**



What is Apache Spot?

- Spot is a community-driven project providing advanced analytics and comprehensive visibility across all security data using an open, scalable platform.
- Spot expedites threat detection, investigation and remediation via machine learning and consolidation of IT Telemetry into a comprehensive Data Lake.



<https://spot.incubator.apache.org/>

What does Spot Provide?

- Network Flows (nfcapd)
- DNS (PCAP)
- Proxy



TELEMETRY

- Open source decoders
- Load data in Hadoop



PARALLEL INGEST FRAMEWORK



MACHINE LEARNING

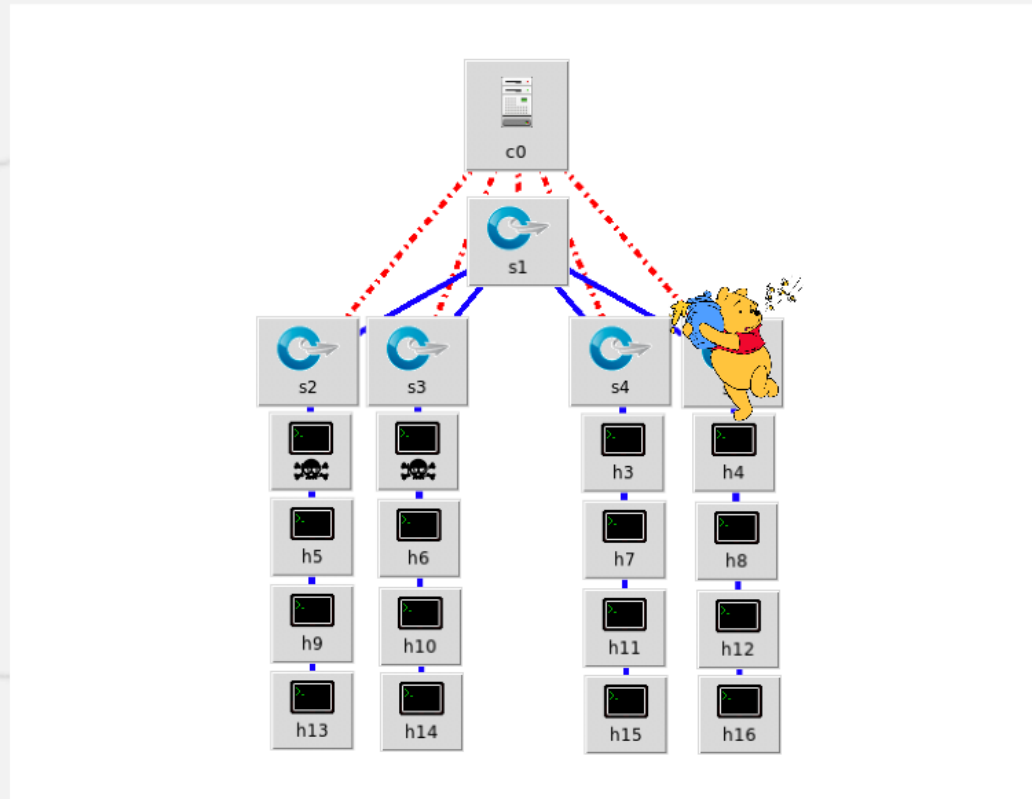
- Filter billions of events to a few thousand
- Unsupervised learning

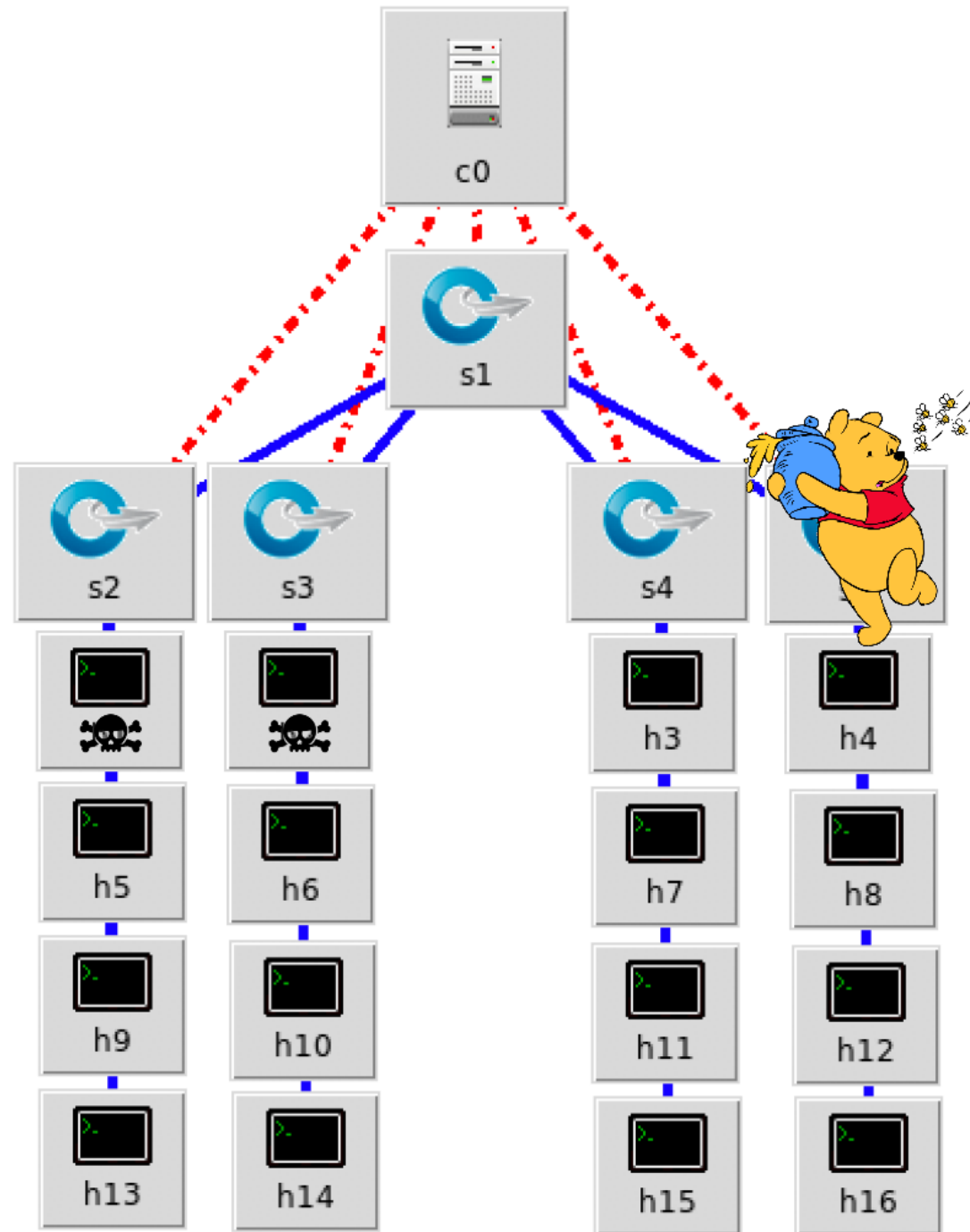


OPERATIONAL ANALYTICS

- Visualization, attack heuristics noise filter

Demo Architecture





Finally..... a helpful SDN tool

(hopefully)

- Takes sFlow information from a network
- Writes it to a mininet topology
- Communicates active flows to SDN controller
- Can be used to model or migrate production or lab environments

....**FloWrita**

github: @acksec

Who am I?

Breaking things since I was 12

Consulting Security Architect

I get to break things and help fix them

Other interests: traveling, hockey, snobby
beer, and my bulldog

#cyberspice

Networks are Failing Us

They work too well!
They don't work
well enough!
...And how does this all come together in the cloud?

Software Defined Networking

And what about the security of the cloud?
The cloud is not a magic box
The cloud is not a magic box
The cloud is not a magic box

What's out there and how does it work?

So why do we care?

...And how does this all come together in the cloud?

Let's talk dynamic security...

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

...And how does this all come together in the cloud?

Where are all the SDN Talks?
Because Skynet can defend itself now!

Jon Medina
protiviti
For the Future with Confidence