Beyond Firewalls: The Future Of Network Security
Security Trends Today

Network security landscape has expanded
CISOs “Treading Water”

- Pouring money in security, yet not any more secure
  - Average of 4000 nodes with 5 security vendors
- Risks posed by threats vs risks to business outcomes
- Success measured by total number of attacks stopped vs reduction of risk
- Attackers are always innovating to stay ahead
Threats are Everywhere

Perimeter security isn’t enough. Malware defeats network security through many vectors.

Stop Threats. Faster.

- Cyber criminals are always uncovering new vulnerabilities
- Attacks are more diverse and variable
- Threats are already inside and are likely unknown
- Data security across networks is crucial
Traditional security strategies focus on the perimeter only—outside in.

And...it is not enough.

Today’s network security must be dynamic, automated and intelligent to effectively detect and stop evolving threats.

Perimeter security model

- Layered on top of the network – not an integral function
- Designed to trust activity that’s already inside the network
- Relies mostly on traditional firewalls for data and insight
A Change in Mindset
Start thinking about Secure Networks

- Adjust your tactics – re-examine point technology
- Recognize perimeter security isn’t enough
- Enable Detection and Enforcement anywhere
- Security is everyone’s problem – horizontal and vertical. Work with DevOps and NetOps
Everything on Your Network is a Potential Threat

Normal and Abnormal Behavior

Normal operation: call home beacons, energy utilization

Anomalous behavior: bursting traffic, abnormal high data download rate

Is this normal? How to mitigate risk?
The Software Defined Secure Network

Operate the network as single enforcement domain – Every element becomes a policy enforcement point

**POLICY**

- Create and centrally manage intent-based policy directly aligned to business objectives

**DETECTION**

- Gather and distribute threat intelligence from multiple sources – find exploits faster
- Leverage cloud economics for real time analysis – identify risks sooner

**ENFORCEMENT**

- Apply policy enforcement to threat intelligence in real time – and adapt the network in real time
Software Defined Secure Network: Policy, Detection and Enforcement

Bottoms Up and Tops Down Approach –

Leverage *entire network and ecosystem* for threat intelligence and detection

Utilize *any element* of the network as an *enforcement point*

Dynamically execute policy across all network components including third party devices
The Right Policy for the Right Job

Different threat levels need different policies

Anomalous lightbulb: quarantine and create new policy for correct behavior

Compromised core switch? The right policy for the right level of threat
Juniper’s Security Vision

From Network Security to Secure Networks

Unique in the industry with building blocks for tomorrow’s Software Defined Secure Network

• **Simplified Policy and Management** across all network elements

• **Dynamic Solution** fueled by real time threat intelligence for protection against ever evolving cyber crime

• **Efficient Detection and Enforcement** leveraging the entire network to deliver protection

*The Juniper Software Defined Secure Network automatically adapts to the evolving threat landscape so that our customers don’t have to.*
Thank you