



NEW-AGE MOBILE NETWORKS: THREATS AND SOLUTIONS

Nitin Vig
Senior Systems Engineer
Juniper Networks



AGENDA

1 Mobility Trends

2 Attacks and their impact

3 Thwarting the attacks

4 Summary

SECURITY IS IMPACTED BY TWO TRENDS

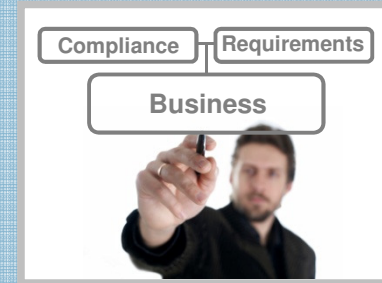
Industry Trends



Workforce Behavior



IT Infrastructure



Business Drivers

Security Trends



Attacker Behavior



Evolving Threat Vectors



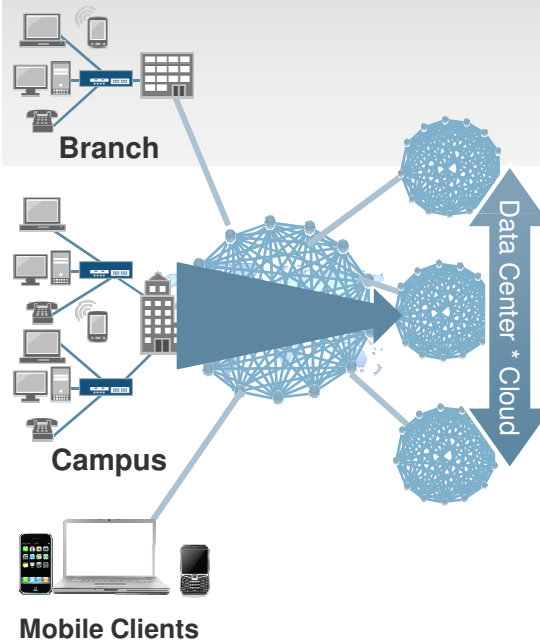
New Attack Targets

INDUSTRY TRENDS

Workforce Behavior



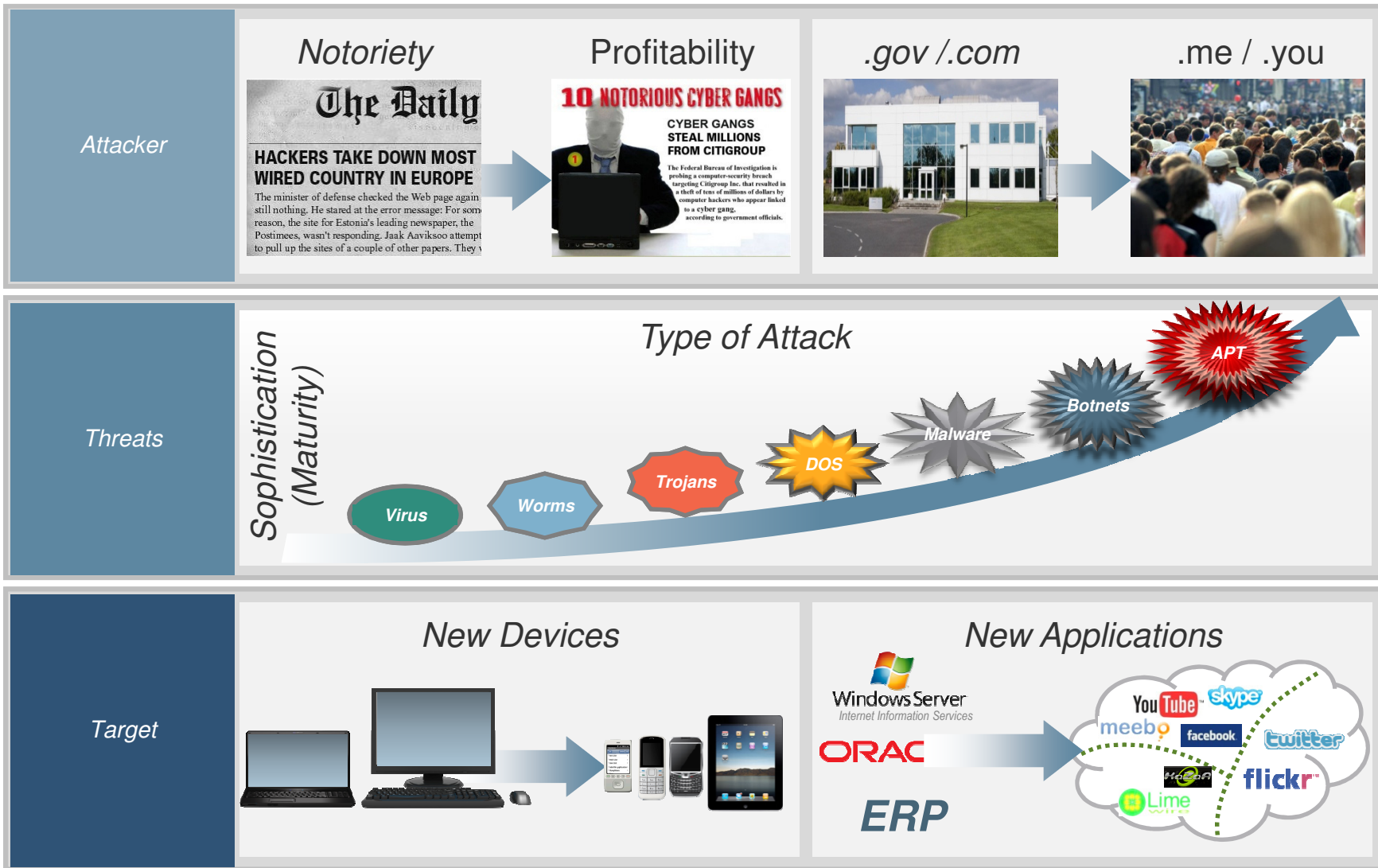
IT Infrastructure



Business Drivers



SECURITY TRENDS





ATTACKS AND THEIR IMPACT

THE THREAT OF MOBILE MALWARE IS NOW REAL!

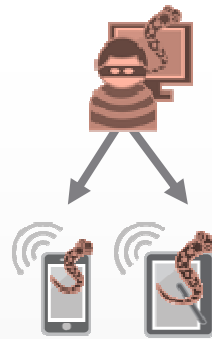
Threats to mobile devices are now a reality!

Mobile device threats reach FAR beyond simple viruses and SMS exploits...

...to include malware, loss/theft, data comm interception, exploitation and misconduct, and direct attacks.



EVOLUTION OF MOBILE MALWARE



Criminals now using PC-style malware attacks to infect mobile devices

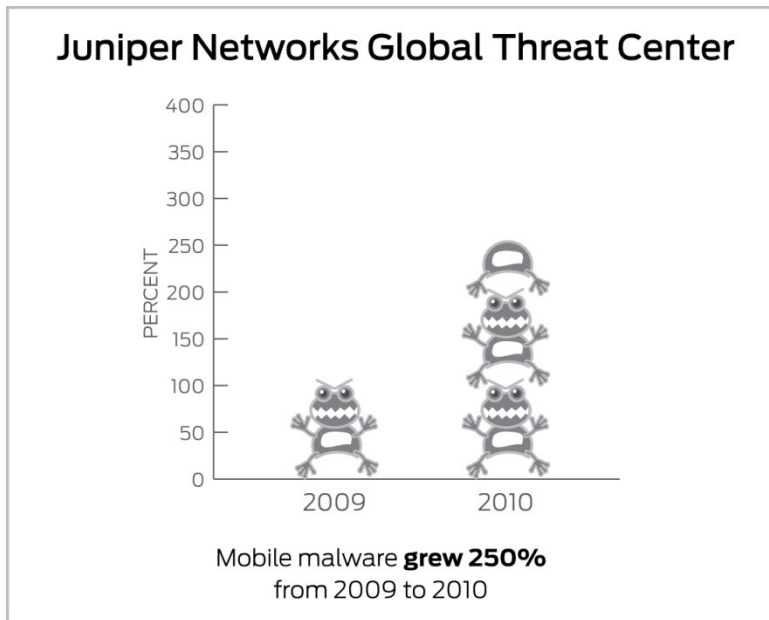


Greatest mobile malware risk comes from rapid proliferation of applications in app stores



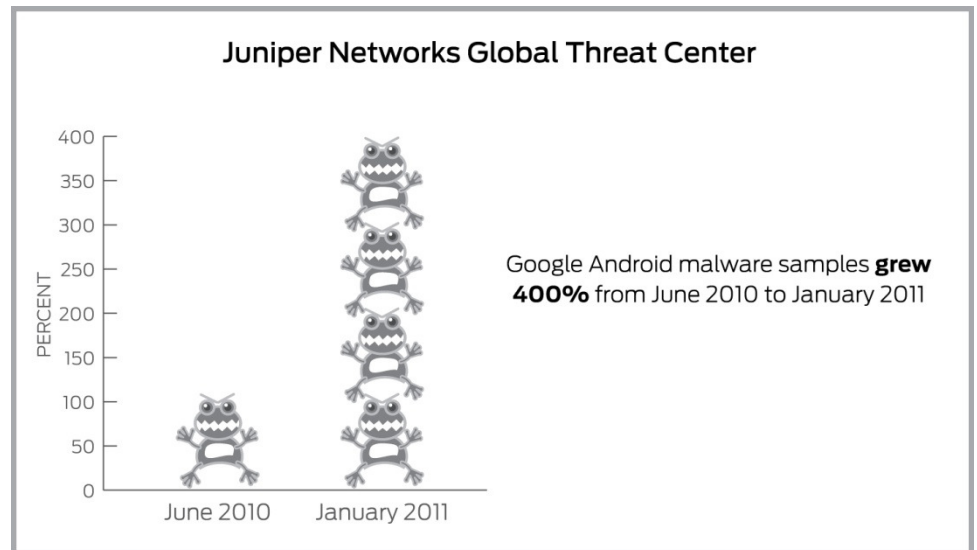
Mobile spyware is prevalent and now commercialized

THE MOBILE MALWARE EXPLOSION



While mobile malware grew quickly between 2009 and 2010...

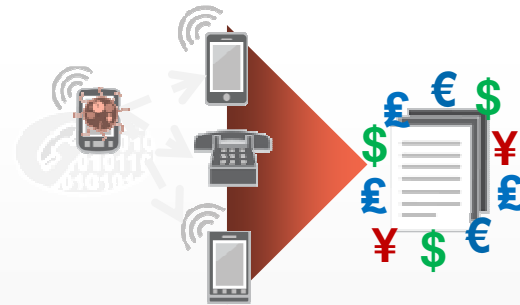
...malware samples for Google Android grew even faster!



MOBILE MALWARE EXAMPLES

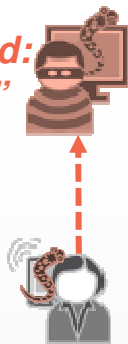


Trojans that send SMS messages to premium rate numbers



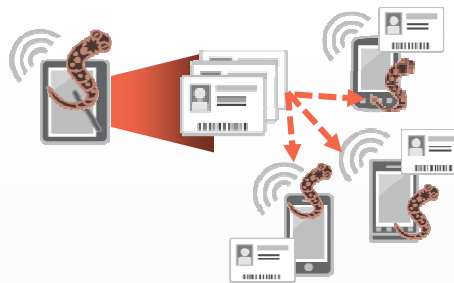
Background calling apps that rack up exorbitant long distance bills

*“Credit Card:
1-2-3-4-5...”*

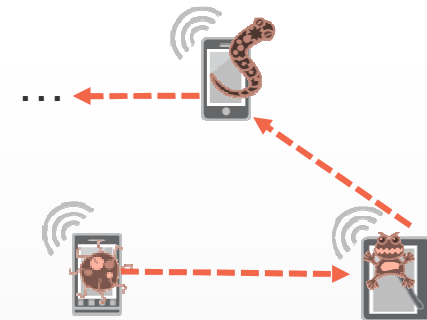


*“Credit Card:
1-2-3-4-5...”*

Keylogging applications that compromise passwords and credit card or bank account numbers



Self-propagating code that infects devices and spreads to additional devices listed in a user's address book



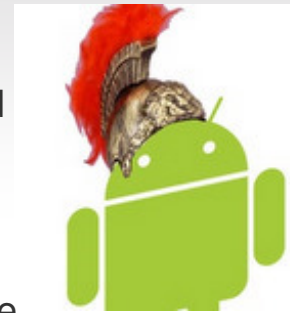
Malware growing more sophisticated, now with polymorphic attacks

MOBILE MALWARE EXAMPLES AND TARGETS

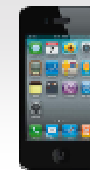


'Most Sophisticated' Android Trojan Surfaces in China –
December 30, 2010

- Geinimi, highly sophisticated botnet-like Trojan, detected in Android devices in China
- Sends location information, device identity, even stored contacts to unknown server
- Found in apps, mostly games, infected and repackaged to resemble legitimate apps, then uploaded onto Chinese third-party app stores



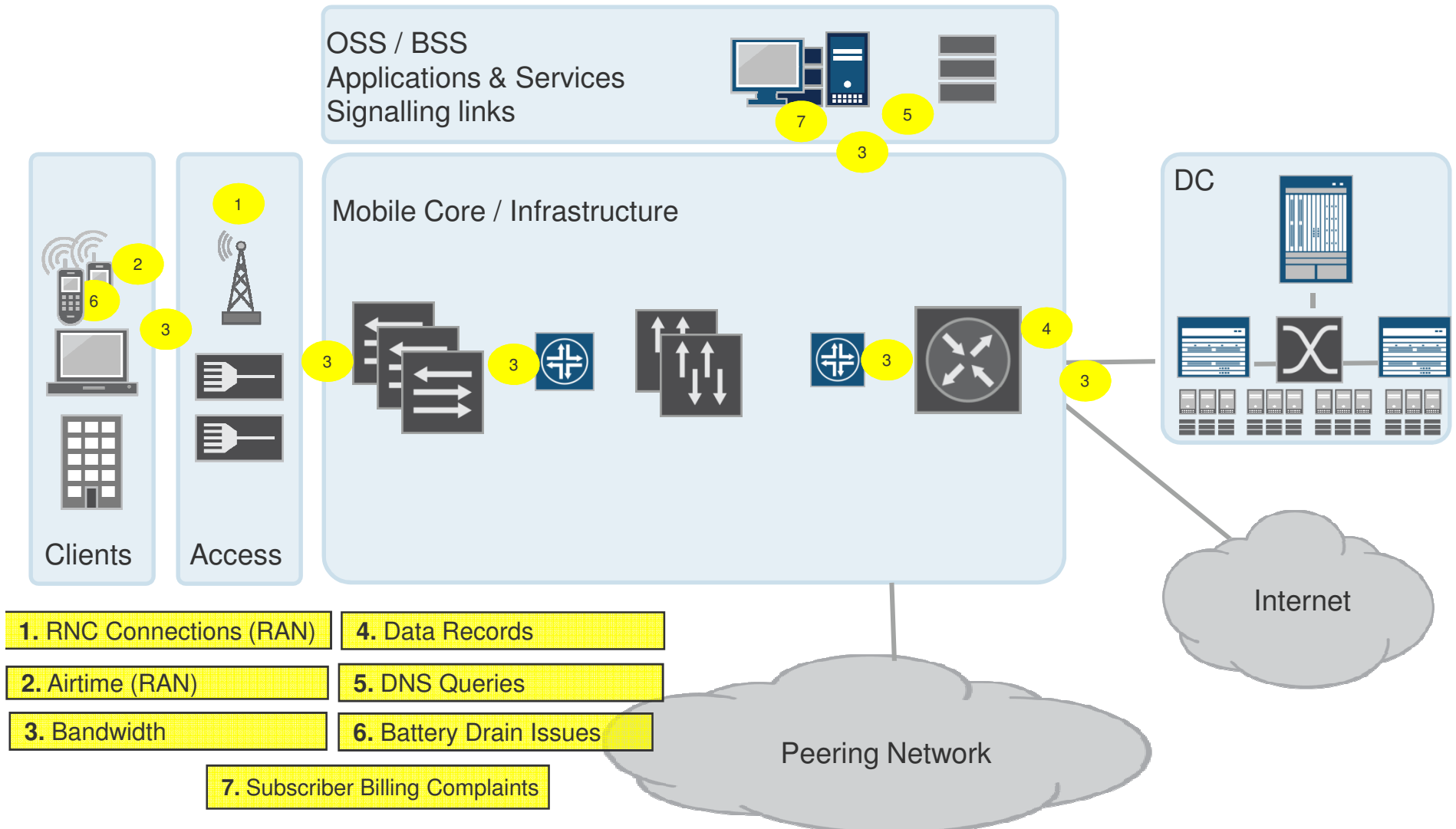
2011 Cyberattack Targets: iPhone, Facebook, Foursquare –
December 29, 2010



'Phishing' Scams Cast Net on Mobile Banking – January 30, 2010

- Developer published an app supposedly for accessing online bank accounts
- After installation, users were presented with their bank's URL and were prompted for login credentials
- After login credentials were submitted, they were then sent to an unknown location, presumably for fraudulent activities

ATTACKS: IMPACT ON THE NETWORK



BUSINESS IMPACT OF NETWORK OUTAGE

Tier-1 European SP suffered a massive network outage (HLRs)

40 million customers unable to make calls or send texts for 4 hours.

Approximately \$100 million in lost revenues to Operator

After a similar network outage back in 2004 at Bouygues Telecom in France, the operator sued its HLR supplier, Tekelec, for \$81 million in damages

http://www.unstrung.com/document.asp?doc_id=175678&piddl_ms_gid=180879

The background of the slide is a complex, abstract composition of overlapping, semi-transparent blue polygons. The colors range from a deep, dark blue to a lighter, almost white-blue, creating a layered, geometric effect. The shapes are irregular and interlocking, filling the entire frame.

THWARTING THE ATTACKS

STATIC SECURITY IS NOT ENOUGH ANYMORE

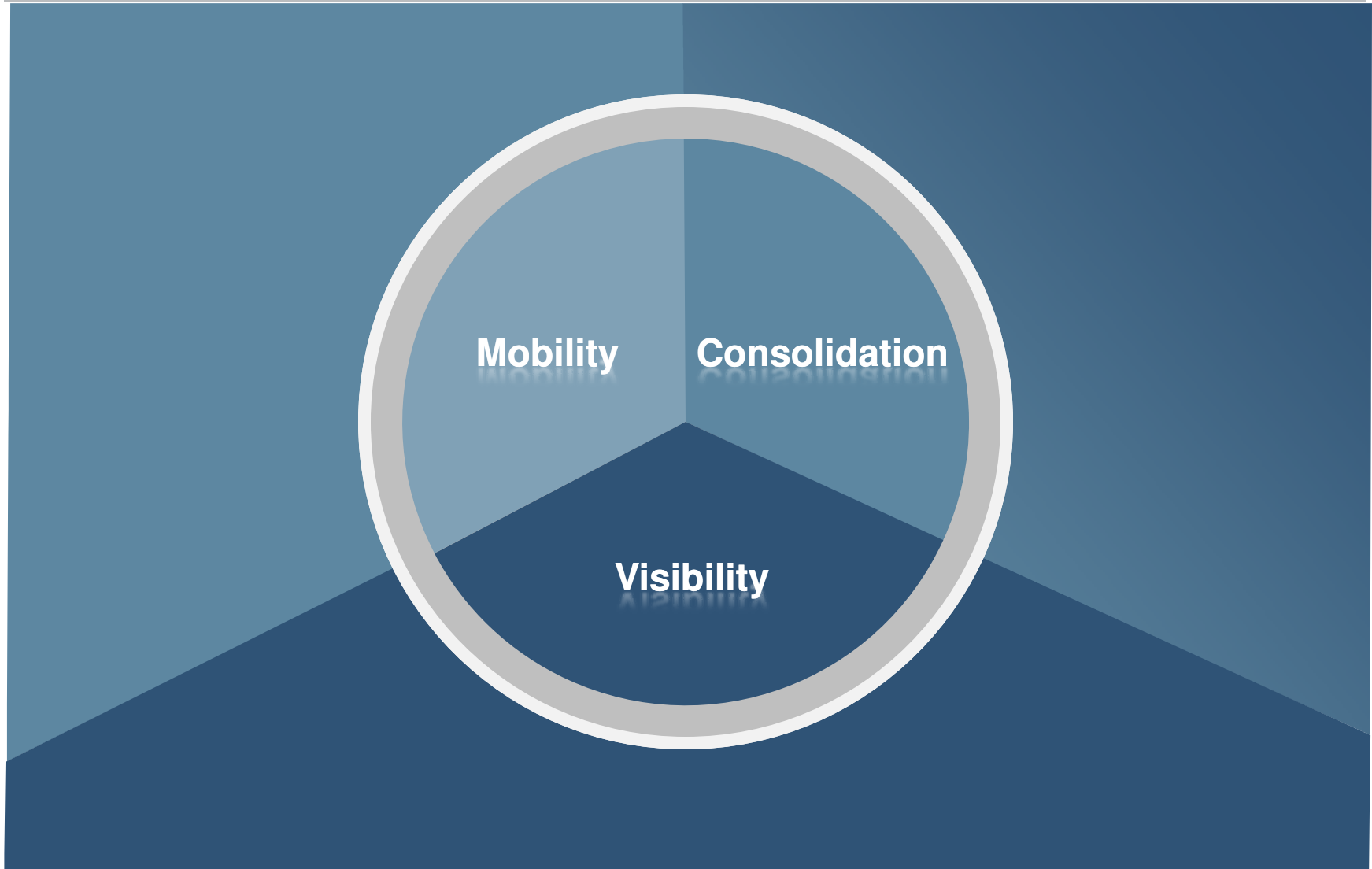
Growing importance of real-time, dynamic security decisions and security policies enforcements

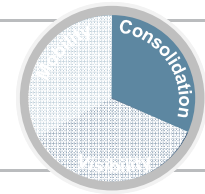
“If you can **detect an attack in the first hour, you have a 90% chance of preventing a data breach,**” said Jonathan Nguyen-Duy, director of Verizon product management.

“By detecting an attack before that packet ever reaches a clients’ perimeter, we can block it, route it or quarantine it”

http://telephonyonline.com/business_services/news/verizon-managed-security-0805/?smte=wl

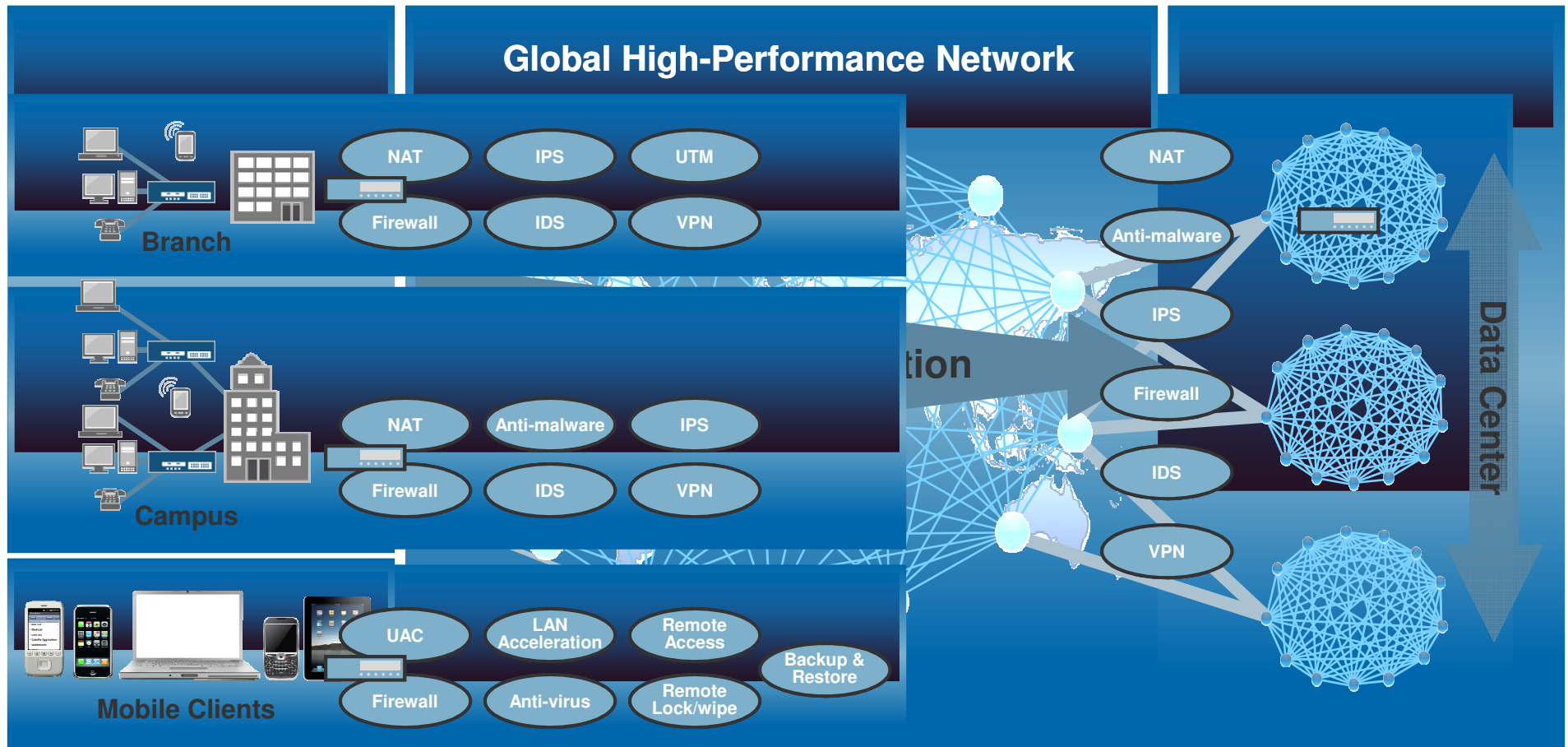
THE FUTURE OF SECURITY





CONSOLIDATION

Consolidation of security services (everywhere)

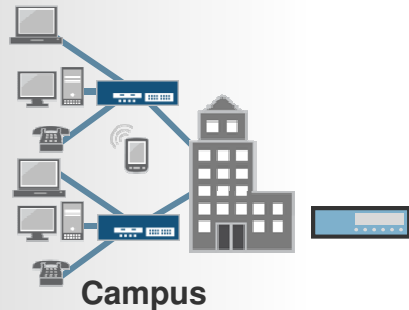




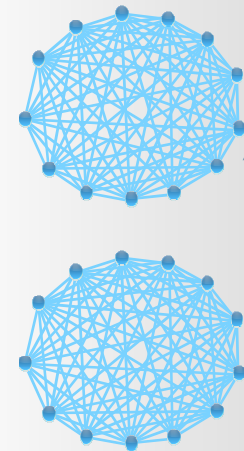
VISIBILITY

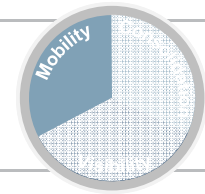
Consolidation of security services (everywhere)
Comprehensive Application Visibility and Control

Global High-Performance Network



Mobile Clients



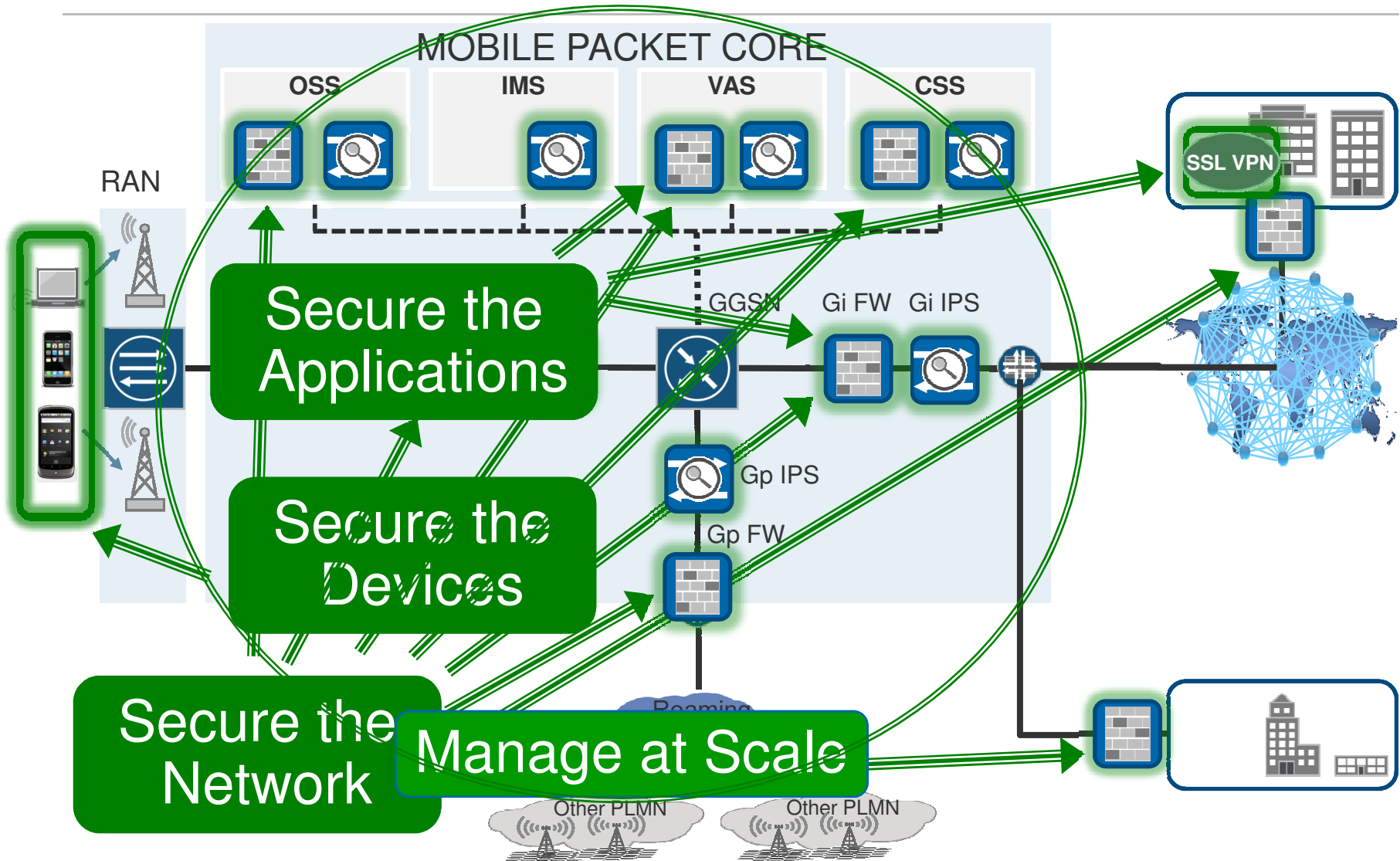


MOBILITY

Consolidation of security services (everywhere)
Comprehensive Application Visibility and Control
Secure Mobility



SECURING THE MOBILE INFRASTRUCTURE



SUMMARY

COMPREHENSIVE SECURITY STRATEGY

Device

Network

Application

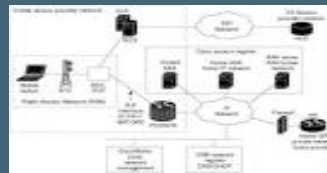
Mobile Device Security



- Security
- Secure Connectivity
- Acceleration



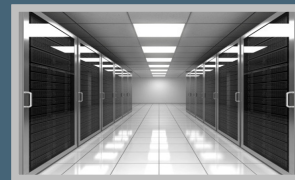
Secure Mobile Infrastructure



- Scale throughput & Sessions
- Signaling and control plane security
- Security for new applications



Datacenter Security



- Virtual security
- Bridge the physical and virtual
- Datacenter scale

Application Security



- AppSecure Strategy
- User mapping to application



Expanded Go To Market



everywhere