Cybersecurity Supply Chain Forum

Security Management Discussion

5/17/2016

Stuart Mitchell
Sprint Solutions Engineering
860-986-7233
Stuart.Mitchell@sprint.com

#gettingbettereveryday

Template Version: 16:9MF1.1
Version Date: 10/23/15

Regarding the recent SS7 hack demo on *60 Minutes*

All the US carriers are getting inquiries on this, and they (including Sprint) are all referring to the CTIA Wireless Association.

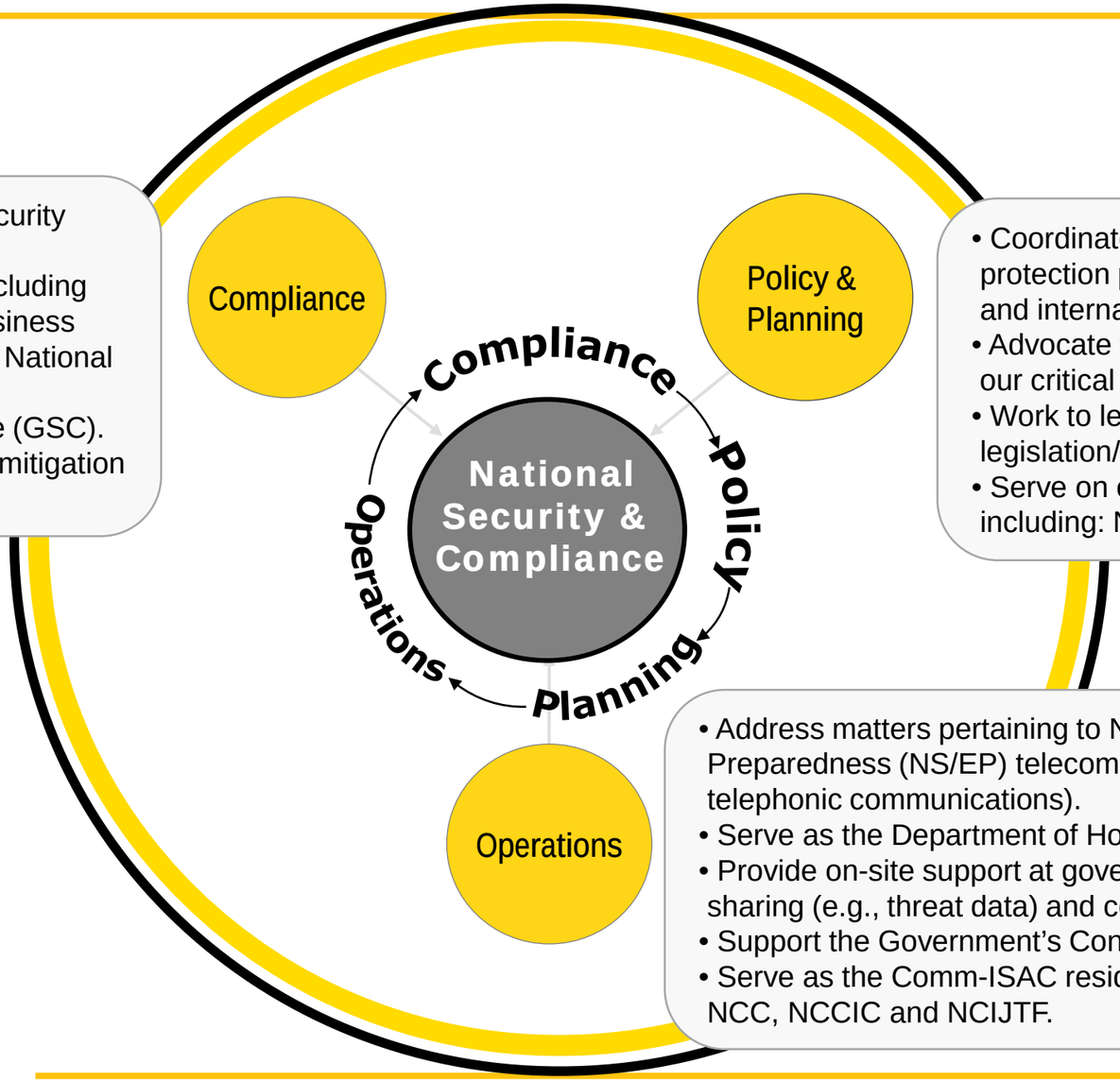
Per the CTIA:

- U.S. wireless providers remain vigilant to protect their networks and their customers," CTIA's vice president of Cybersecurity and Technology John Marinho said.
- "While we are aware of the research hackers' manipulation to exploit SS7 technology in the international wireless networks, it's important to note that they were given extraordinary access to a German operator's network.
- That is the equivalent of giving a thief the keys to your house; that is not representative of how U.S. wireless operators secure and protect their networks. We continue to maintain security as a top industry priority."

Template Version: 16:9MF1.1
Version Date: 10/23/15

Security Compliance

- Work to ensure compliance with National Security Agreement (NSA) obligations.
- Operate CFIUS Compliance Office (CCO) including program governance, coordination across business units and communication with USG to ensure National Security Agreement obligations are met.
- Support the Government Security Committee (GSC).
- Foster collaborative relationship with CFIUS mitigation agencies.



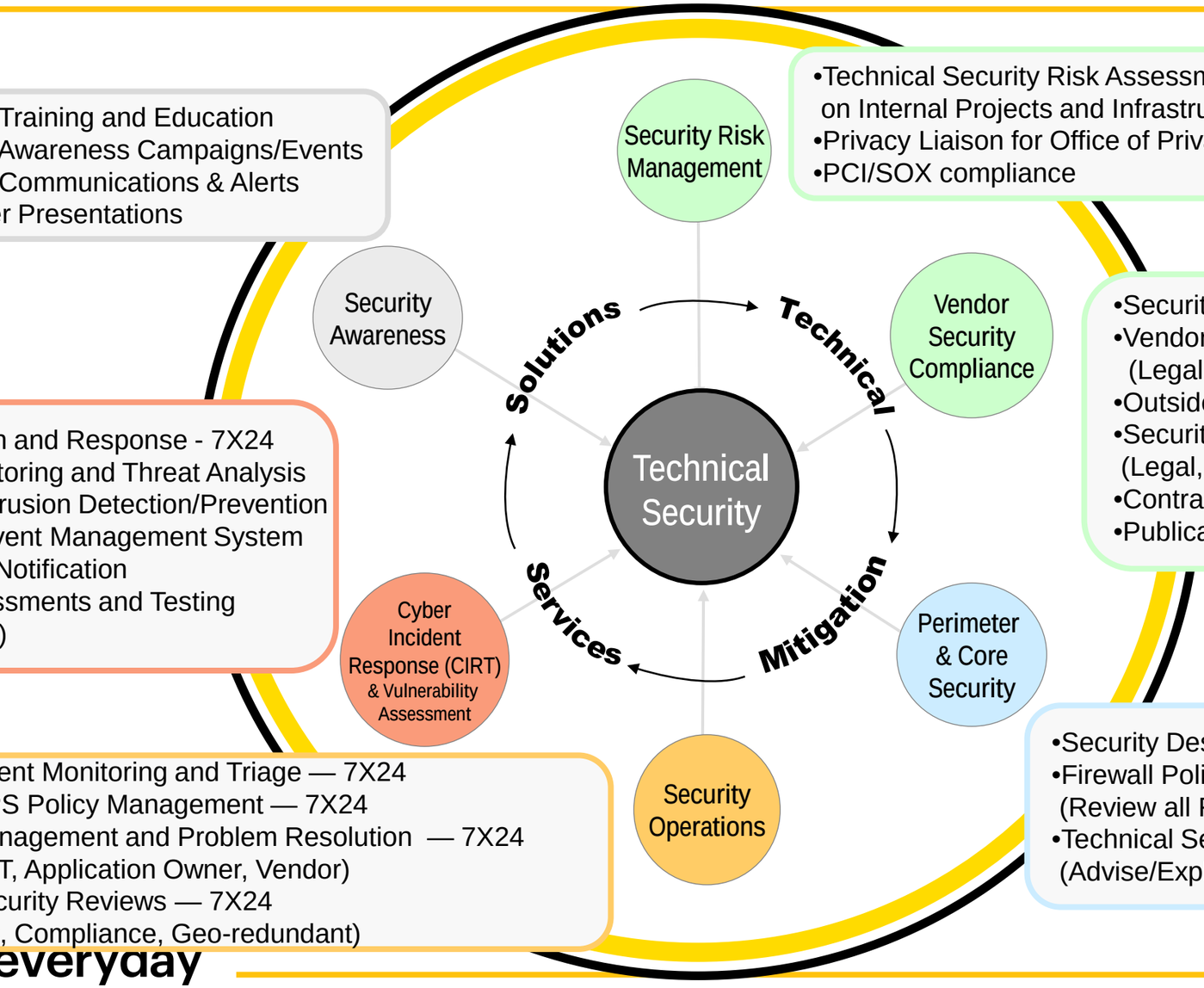
- Coordinate national security and infrastructure protection planning activities with government partners and internal organizations.
- Advocate the company's commitment in protecting our critical infrastructure and key resources.
- Work to lessen the risk of security legislation/regulation
- Serve on or assist with various security committees including: NSTAC, SCC, CSRIC, CTIA.

- Address matters pertaining to National Security/Emergency Preparedness (NS/EP) telecommunications (including both cyber and telephonic communications).
- Serve as the Department of Homeland Security Operational Liaison.
- Provide on-site support at government locations to facilitate information sharing (e.g., threat data) and coordinate requests for support.
- Support the Government's Continuity of Operations (COOP) function.
- Serve as the Comm-ISAC resident member and the primary lead to the NCC, NCCIC and NCIJTF.

#gettingbettereveryday

Template Version: 16:9MF1.1
Version Date: 10/23/15

Technical Security



- Security Training and Education
- Security Awareness Campaigns/Events
- Security Communications & Alerts
- Customer Presentations

- Technical Security Risk Assessment and Policy Compliance on Internal Projects and Infrastructure
- Privacy Liaison for Office of Privacy on new projects
- PCI/SOX compliance

- Security Policy Management
- Vendor/Business Partner Security Compliance (Legal, Regulatory, Contractual)
- Outside Resource Committee (ORC) Facilitator
- Security Compliance for external projects (Legal, Regulatory, Contractual)
- Contract support with Supply Chain Mgmt.
- Publication of Residual Risk Report

- Cyber Incident Identification and Response - 7X24
- Proactive Intelligence Monitoring and Threat Analysis
- Security Architecture for Intrusion Detection/Prevention
- Security Information and Event Management System
- Security Vulnerability Alert Notification
- Security Vulnerability Assessments and Testing (Applications and Systems)

- Security Event Monitoring and Triage — 7X24
- Firewall / IPS Policy Management — 7X24
- Firewall Management and Problem Resolution — 7X24 (Network, IT, Application Owner, Vendor)
- Firewall Security Reviews — 7X24 (Migrations, Compliance, Geo-redundant)

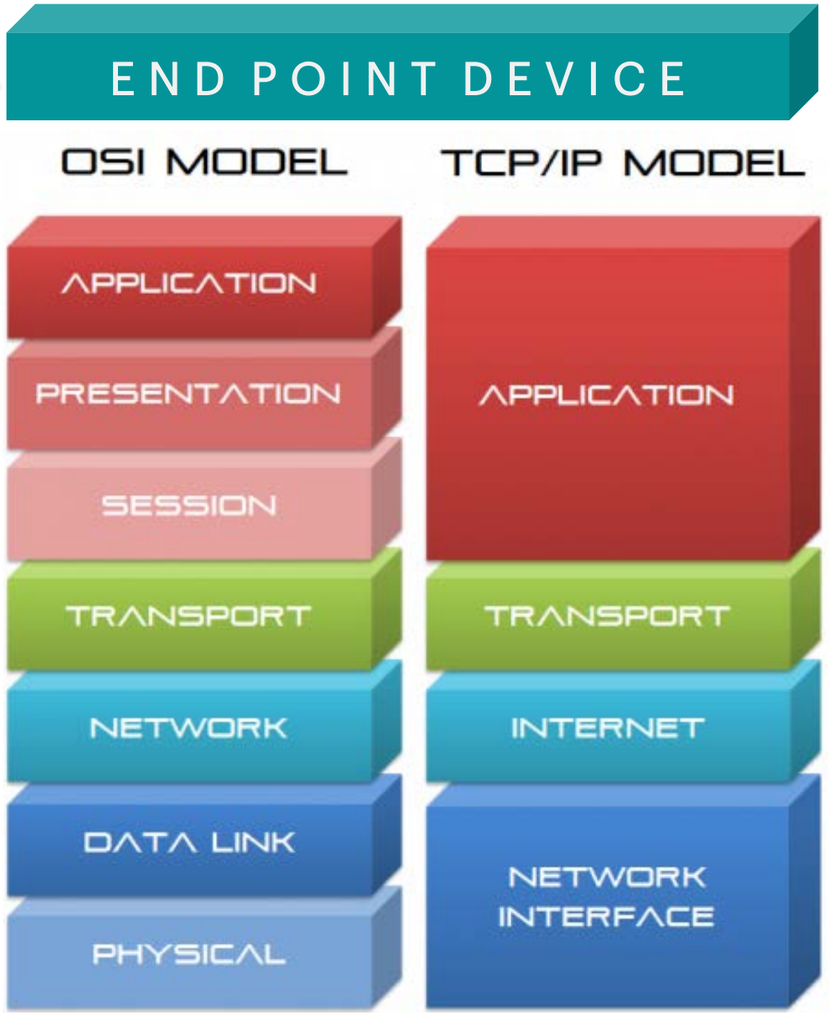
- Security Design (Firewalls, DMZ, Extranet, Intranet)
- Firewall Policy Compliance (Review all Firewall Questionnaires)
- Technical Security Consultation (Advise/Explain Security Issues of Technical Solutions)

Template Version: 16:9MF1.1
Version Date: 10/23/15

Where we play

Secondary function support here

Carrier primarily functions here



#gettingbettereveryday

Best practices for secure architecture

- Layering
- Network segmentation
- Network separation
- Network type

Template Version: 16:9MF1.1
Version Date: 10/23/15

Network Type considerations

	Wireline	Wireless
Public	Internet access - DSL, DSx, OCx, Ethernet, Fiber - DSU's, routers, etc. - Connected to everyone	Internet access - Smartphone data - Wireless gateway (modem) - Machine modules - Connected to everyone
Private	Private Network access - MPLS, PL, FR, ATM - DSU's, routers, etc. - Controlled, internal only	Private Network access - Smartphone data - Wireless Gateway (modem) - Machine modules - Controlled, internal only

Template Version: 16:9MF1.1
Version Date: 10/23/15

Security contrast

General wireless access

- Wireless interface encrypted and encoded
- Device authentication
- Internet network - Shared network with everyone
- IP address – internet potentially accessible

- Potential for intrusion, hacking, malware delivery

Private wireless access

- Wireless interface encrypted and encoded
- Device authentication
- Private network – does not touch the internet
- Private IP address range – not internet accessible
- Static route direct to the Enterprise network
- Your traffic is separated from other traffic using Layer 3 VRF network separation

- Removes external network based risk from
  - Port scanning
  - IP spoofing
  - DNS spoofing
  - Denial of service
  - ...etc.

Template Version: 16:9MF1.1
Version Date: 10/23/15

Secure Private Wireless Network

Productivity gains/ cost savings

Private wireless networks can provide great ROI

- By extending corporate security policy to mobile & remote devices – offering greater control

Rapid deployment

Private wireless networks can be deployed quickly

- Reducing time to market
- Regardless of the end device.

Intranet / Extranet Access

Private wireless network access to the enterprise for:

- Small locations
- Storefront POS
- M2M / IoT
- Business partners

Network continuity

Extend your enterprise network

- Interconnectivity with your wireline network
- Route diversity
- Access diversity

#gettingbettereveryday

Template Version: 16:9MF1.1
Version Date: 10/23/15

Private Wireless Network Benefits

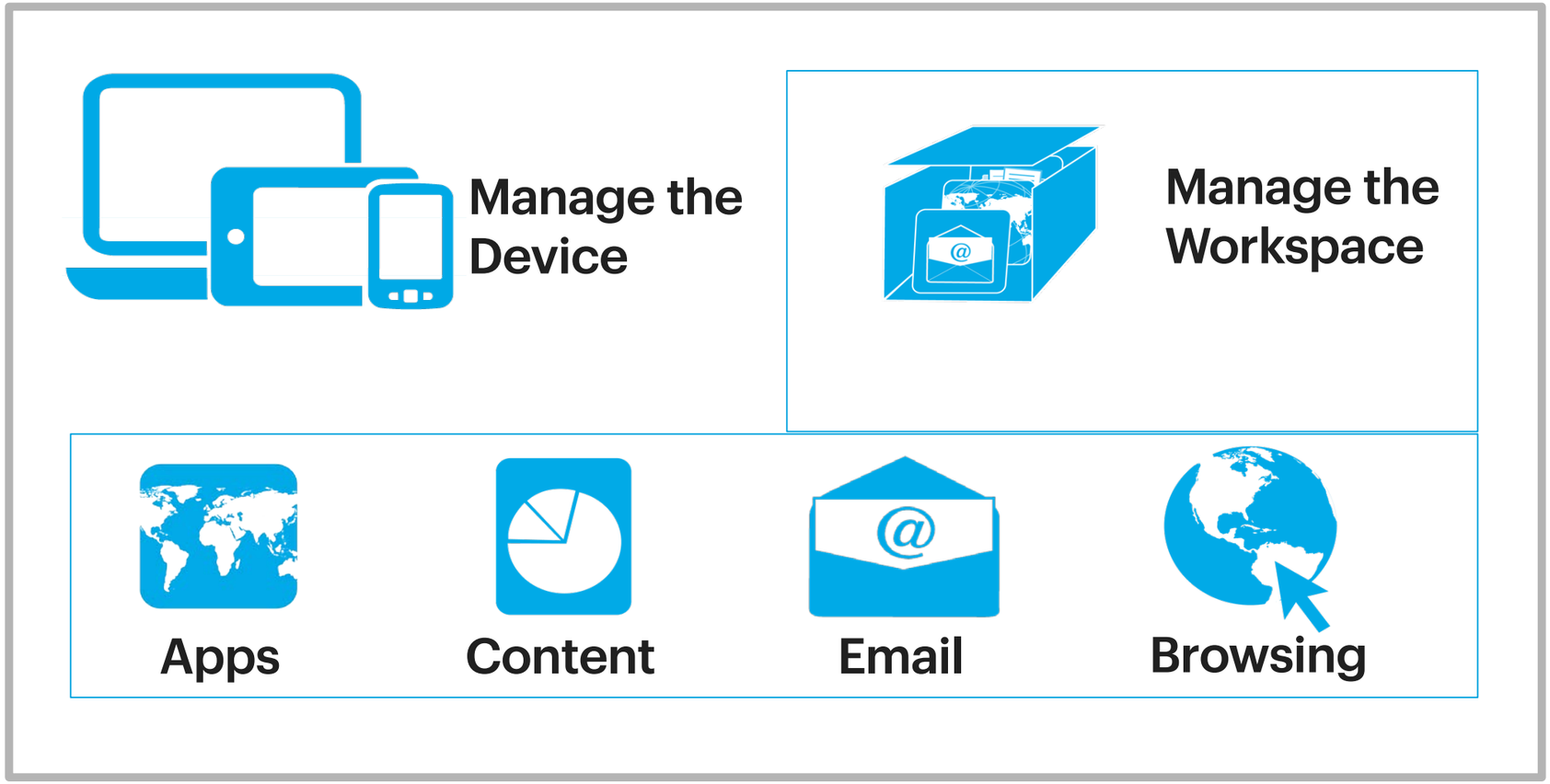
Improve security, increase connectivity and create seamless workflow

- **Enable employees to stay connected while mobile or remote,** with secure wireless access to your enterprise network and applications
- **Further extend corporate security policies and leverage current security investments** to mobile & remote workers.
- **Improve your business processes, supply chain workflow and communications** with secure wireless intra / extra networking.
- **Increase security by removing vulnerabilities**
  i.e.: port scanning of wireless & remote devices,
  Private IP, static destination
- **Support any wireless device** – employee mobility, M2M & IoT

#gettingbettereveryday

Template Version: 16:9MF1.1
Version Date: 10/23/15

Mobile endpoint device security & control



#gettingbettereveryday

Template Version: 16:9MF1.1
Version Date: 10/23/15

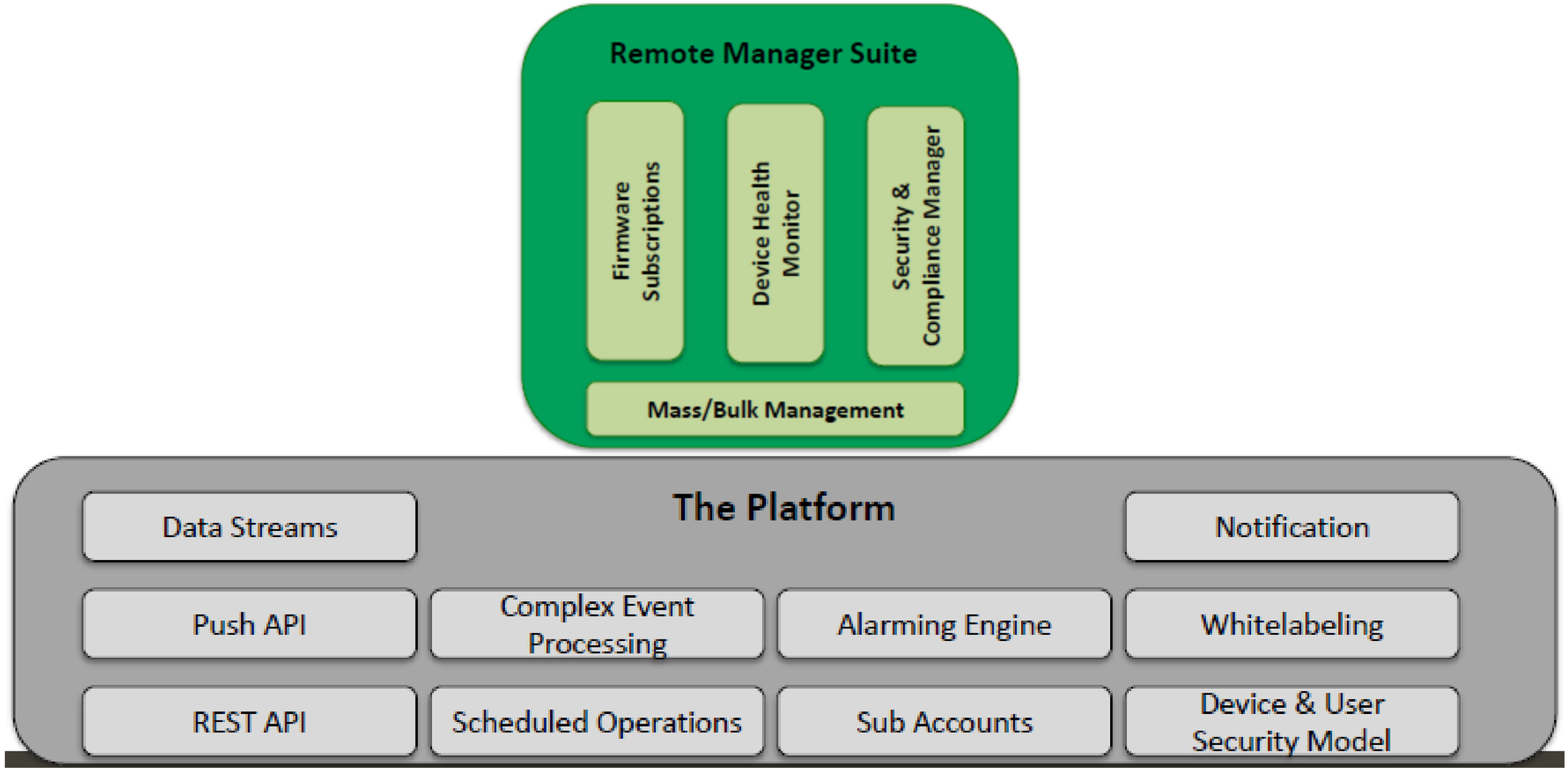
M2M / IoT Network

Comprehensive self-service data transport and device management platform
The ultimate command & control

- Purpose built infrastructure for Machine-to-Machine / Internet of Things
- Separate infrastructure elements from all other networks
- No connectivity to the Internet
- Completely secure
- Discreet closed network address ranges – private dynamic or static address range
- Closed SMS platform – provides additional layer of security
- Device type limitations further support security
- Comprehensive real-time control over provisioning, billing, traffic and device management.
- Greater management flexibility

Template Version: 16:9MF1.1
Version Date: 10/23/15

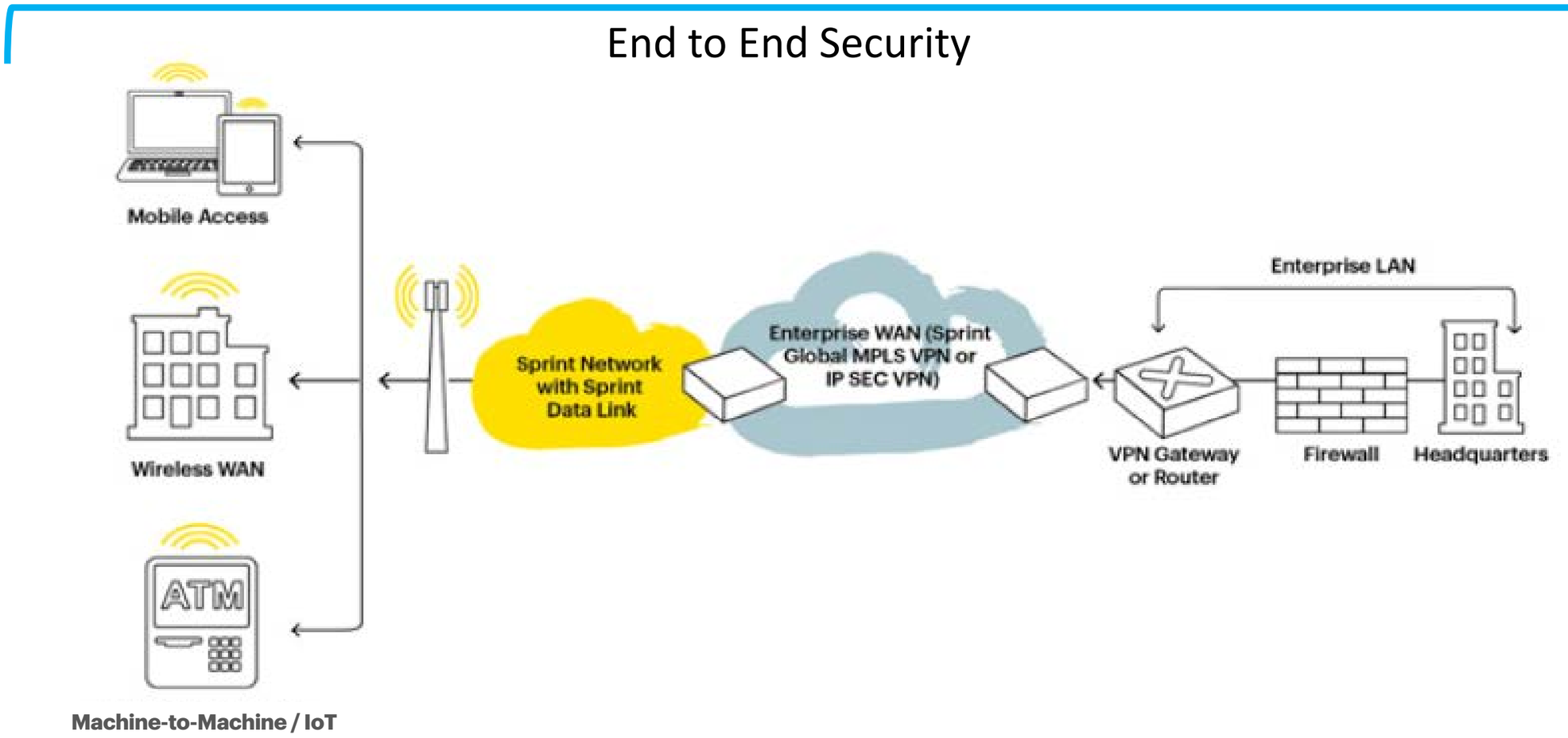
M2M / IoT endpoint device security & control



#gettingbettereveryday

Template Version: 16:9MF1.1
Version Date: 10/23/15

Summary



#gettingbettereveryday

Template Version: 16:9MF1.1
Version Date: 10/23/15


Sprint