AVAYA

GOVERNMENT
SOLUTIONS

GUIDE TO SECURING THE EVERYWHERE PERIMETER

SECURING THE EVERYWHERE PERIMETER

The days of a fixed network edge are gone. Digital transformation, cloud computing, Bring Your Own Device (BYOD) and the Internet of Things (IoT) have fragmented the traditional government network perimeter, making it nearly impossible to determine where an agency's secure perimeter lies.

AVAYA GOVERNMENT SOLUTIONS

THE BIG PROBLEM

Detected security incidents are growing at an alarming rate and posing significant threats to today's network security model.

38%
Increase in Security Incidents

25+%
Enterprise Attacks will be IoT

25B
IoT Devices

256
Days to Identify Attacks

6.7M
Cost Per Data Breach

48%
Breaches were Malicious

> *By 2020, over 25% of identified attacks in enterprises will involve IoT*
> **Gartner, 2016**

Sources: PwC, "The Global State of Information Security® Survey, 2016; Gartner – "Predicts 2016: Security for the Internet of Things"; Cost of Data Breach Study: Global Analysis Benchmark research sponsored by IBM independently conducted by Ponemon Institute, LLC

SOLUTIONS

Inherently Safer: Stealth Networks and Hyper-Segmentation

Traditional, hierarchical architecture simply is not built to support new technology trends and protect against the increased risk of exposure inherent in them. This article explores how hyper-segmentation delivers much-needed safety to networks.

Read the article

The New World of Network Security

This white paper takes a look at elements of IoT security and offers a roadmap for implementing smart, multilevel security capabilities.

Read the white paper

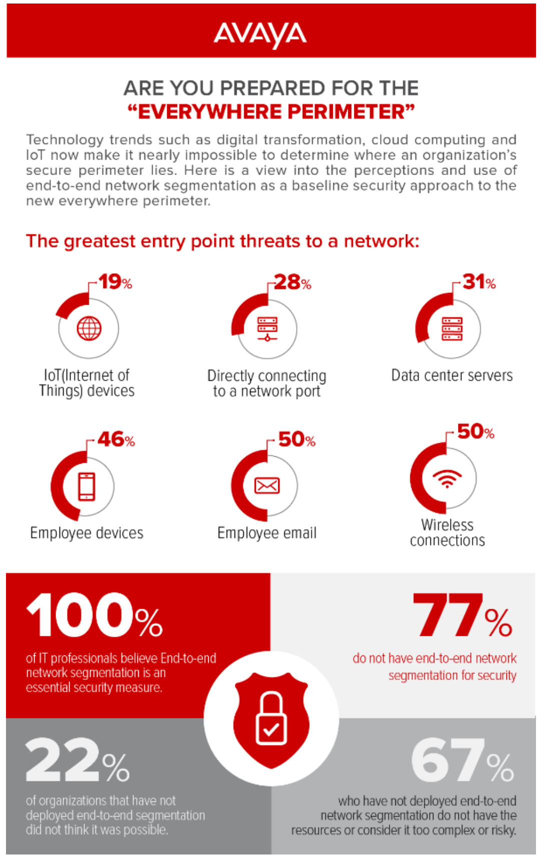
ARE YOU PREPARED FOR THE EVERYWHERE PERIMETER?

There are thousands or even millions of endpoints that must be secured to prevent hackers from accessing agency networks, stealing sensitive data, and causing significant infrastructure damage.

In addition to an increasingly distributed and mobile workforce, government leaders also are challenged by a number of complex legacy systems that must be integrated into the new borderless network. The government needs an effective security strategy that is comprehensive, pervasive and automated to protect “everywhere perimeters” from malicious cyberattacks.

AGENCIES MUST

- Safeguard critical applications and information
- Contain breaches and isolate hackers
- Meet compliance and regulatory obligations
- Protect people, places, and assets
- Manage and secure IoT



AVAYA

ARE YOU PREPARED FOR THE
“EVERYWHERE PERIMETER”

Technology trends such as digital transformation, cloud computing and IoT now make it nearly impossible to determine where an organization's secure perimeter lies. Here is a view into the perceptions and use of end-to-end network segmentation as a baseline security approach to the new everywhere perimeter.

The greatest entry point threats to a network:

19% IoT(Internet of Things) devices

28% Directly connecting to a network port

31% Data center servers

46% Employee devices

50% Employee email

50% Wireless connections

100% of IT professionals believe End-to-end network segmentation is an essential security measure.

77% do not have end-to-end network segmentation for security

22% of organizations that have not deployed end-to-end segmentation did not think it was possible.

67% who have not deployed end-to-end network segmentation do not have the resources or consider it too complex or risky.

View the infographic

DEPLOYING AN IOT-READY ARCHITECTURE

The changing nature of networks now requires a different approach to security. By leveraging Avaya technology, the government can now make what was once complex, simple. The three key emerging challenges—implementing scalable segmentation, managing the double-edged nature of IP reachability, and securing edge configuration and attachment—are addressed by the three pillars of Avaya's securing the everywhere perimeter:

Hyper-Segmentation

addresses the challenge of implementing scalable segmentation

→

Native Stealth

addresses the challenge of managing the double-edged nature of IP reachability

→

Automatic Elasticity

addresses the challenge of securing edge configuration and attachment

→

AVAYA GOVERNMENT SOLUTIONS

HYPER-SEGMENTATION

Avaya's hyper-segmentation greatly improves upon traditional segmentation by scaling to millions and seamlessly spanning the entire organization from data center to device. Once hyper-segments are created, organizations experience a reduction in the attack surface, a quarantine function if a segment is breached, improvement of anomaly scanning, and greater firewall efficiency.

LEARN MORE

An Exploration of End-to-End Network Segmentation—Part I: Hyper-Segmentation

Hyper-segmentation—the ability to create stealth segments that span the entire network—enables network security tools to perform with greater efficiency, offering full transparency into network activity.

Read the article

Divide & Conquer: Cybersecurity Through Hyper-Segmentation

Hyper-segmentation creates dead ends for hackers. If one segment of the network is attacked, hyper-segmentation prevents uncontrolled access everywhere. And, in the age of IoT, scalability is important: you can set up any number of isolated segments quickly and easily.

Read the white paper

AVAYA GOVERNMENT SOLUTIONS

NATIVE STEALTH

Unlike traditional technology, Avaya delivers hyper-segments that are not exposed to the vulnerabilities of Internet Protocol. In the event the organization is breached—for example, through an IoT network segment—the hacker is unable to see anything outside that segment, keeping them contained. Because intermediate networking nodes are ignorant of the content and do not rely upon IP-based reachability, they cannot be used as launch points for exploiting a breach.

LEARN MORE

An Exploration of End-to-End Network Segmentation—Part II: Native Stealth

Native stealth—the characteristic of a hyper-segment that's invisible—keeps hackers in the dark.

Read the article

Cybersecurity, Stealth and the Internet of Things

Have you ever considered how a true security practice could be implemented for an IoT framework? You are not alone. Quite frankly its still the wild west out there. There are scarce standards on IoT and security and the practice is not well understood. But there is a way to create a network that is 'dark' to IP topology discovery techniques.

Watch the video

AVAYA GOVERNMENT SOLUTIONS

AUTOMATIC ELASTICITY

Avaya has pioneered the concept of network elasticity as an enabler for securing the everywhere perimeter. An elastic hyper-segment automatically stretches services to the edge, only as required and only for the duration of a specific application session. As applications terminate, or end-point devices close down or disconnect, the now-used networking services retract from the edge. It simplifies the deployment of hundreds of segments for tens of thousands of endpoints.

LEARN MORE

An Exploration of End-to-End Network Segmentation—Part III: Automatic Elasticity

With automatic elasticity, attackers can't hack what they can't connect to, therefore they can't penetrate your network without the necessary level of authentication.

Read the article

Smarter Networking with Automatic Elasticity

While static configuration is technically valid, it is increasingly seen as sub-optimal. Integrated elasticity delivers multiple benefits to the information-centric organization: service agility is enhanced, access control can be effectively enforced, any unused or redundant configuration is rolled back, leaving the network edge "clean".

Read the data sheet

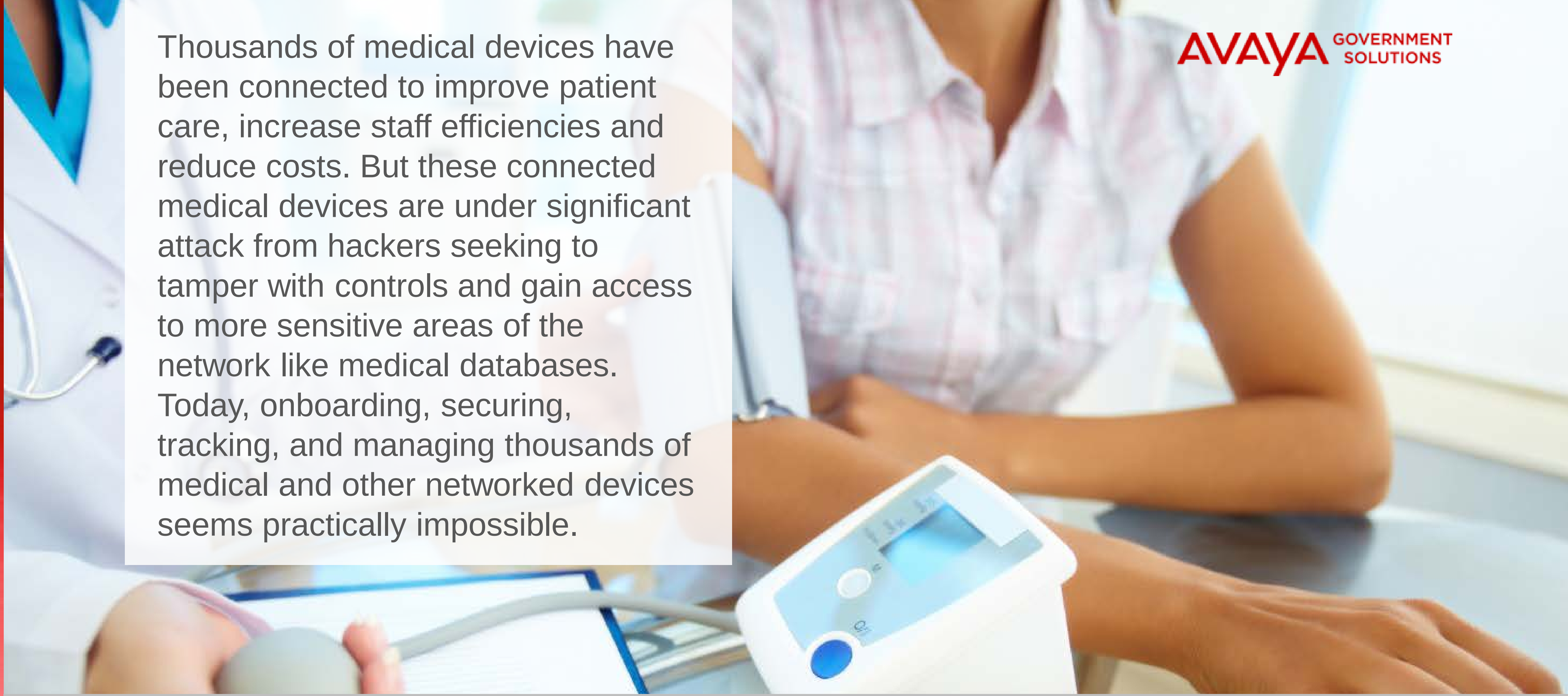
GOVERNMENT HEALTHCARE

Challenges:

- o Securing medical devices
- o Cannot add software code to devices
- o Device tracking

Solution:

- ✓ Automates secure access process
- ✓ Inserts intelligent device proxy
- ✓ Offers device tracking and flow control



Thousands of medical devices have been connected to improve patient care, increase staff efficiencies and reduce costs. But these connected medical devices are under significant attack from hackers seeking to tamper with controls and gain access to more sensitive areas of the network like medical databases. Today, onboarding, securing, tracking, and managing thousands of medical and other networked devices seems practically impossible.

SOLUTION

How Avaya Does SDN Differently

Avaya's SDN Fx Healthcare solution delivers the simplicity needed to help connect, secure and manage the growing number of medical devices and technologies to reduce breaches, implement new healthcare innovation rapidly and improve IT staff efficiency. The solution specifically helps to:

- use advanced network segmentation to reduce catastrophic breaches;
- automate onboarding of new medical devices;
- manage an inventory of thousands of medical devices;
- assign flow priority by device and traffic type.

Read this article on Securing the Everywhere Perimeter in healthcare.

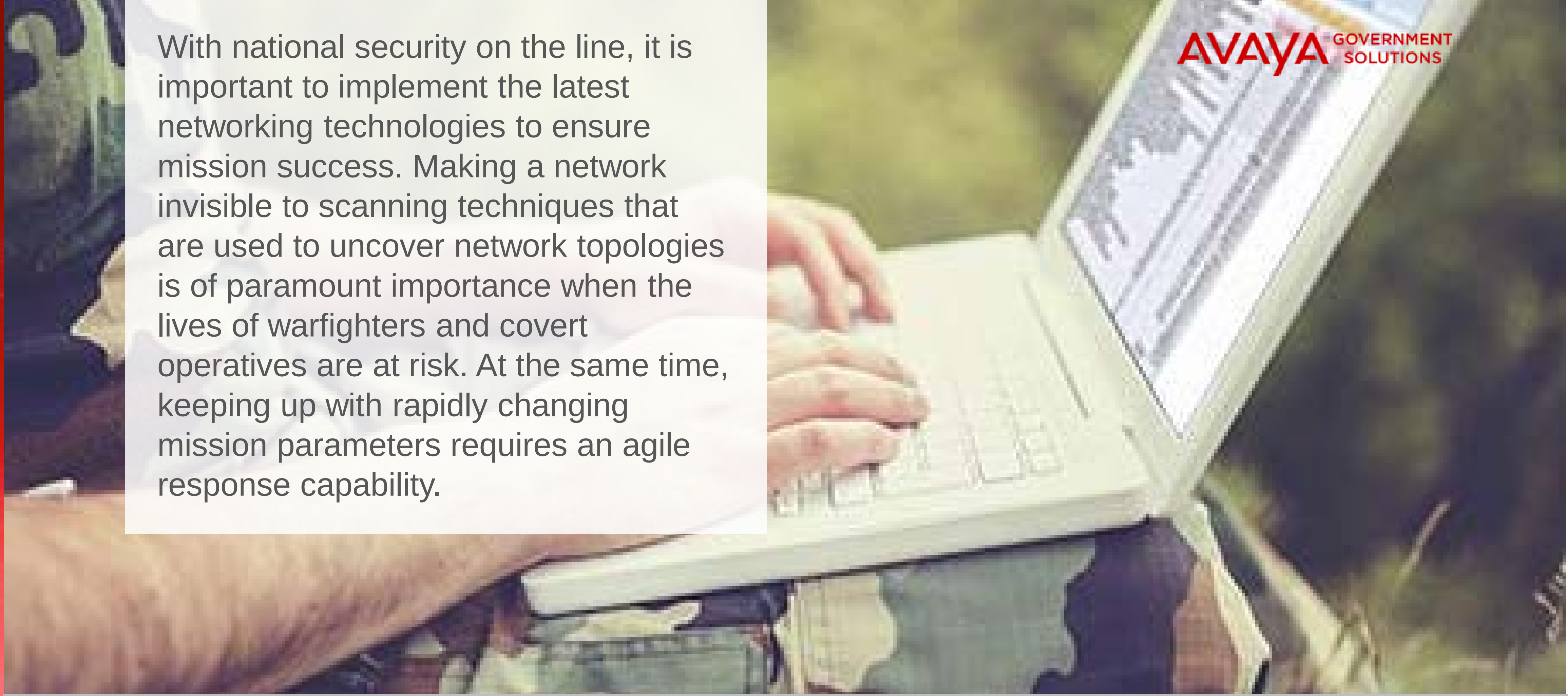
DEFENSE AND INTELLIGENCE

Challenges:

- Highly targeted, globally distributed assets
- Legacy technology and complicated protocols
- Critical performance and recovery time

Solution:

- ✓ Logical network topology enables edge provisioning
- ✓ Single protocol simplifies design, operation, troubleshooting
- ✓ Sub-second recoveries for all Layer 2, Layer 3, IP routing and IP multicast services



AVAYA GOVERNMENT SOLUTIONS

With national security on the line, it is important to implement the latest networking technologies to ensure mission success. Making a network invisible to scanning techniques that are used to uncover network topologies is of paramount importance when the lives of warfighters and covert operatives are at risk. At the same time, keeping up with rapidly changing mission parameters requires an agile response capability.

SOLUTION

Simplicity Enhances Security

Avaya can help defense and intelligence agencies implement a true “stealth” network that protects critical assets and infrastructure from detection. The reliable and easy to manage platform also can grow as the mission expands. With Avaya’s Fabric Connect, administrators can extend services to new facilities and add services without making changes at the network core, allowing them to accomplish in minutes what used to take weeks or months. Fabric Connect also reconfigures itself automatically in response to network traffic and changing conditions, which improves performance while reducing day-to-day operations and maintenance demands.

Watch the Fabric Connect video ▶

AVAYA GOVERNMENT SOLUTIONS

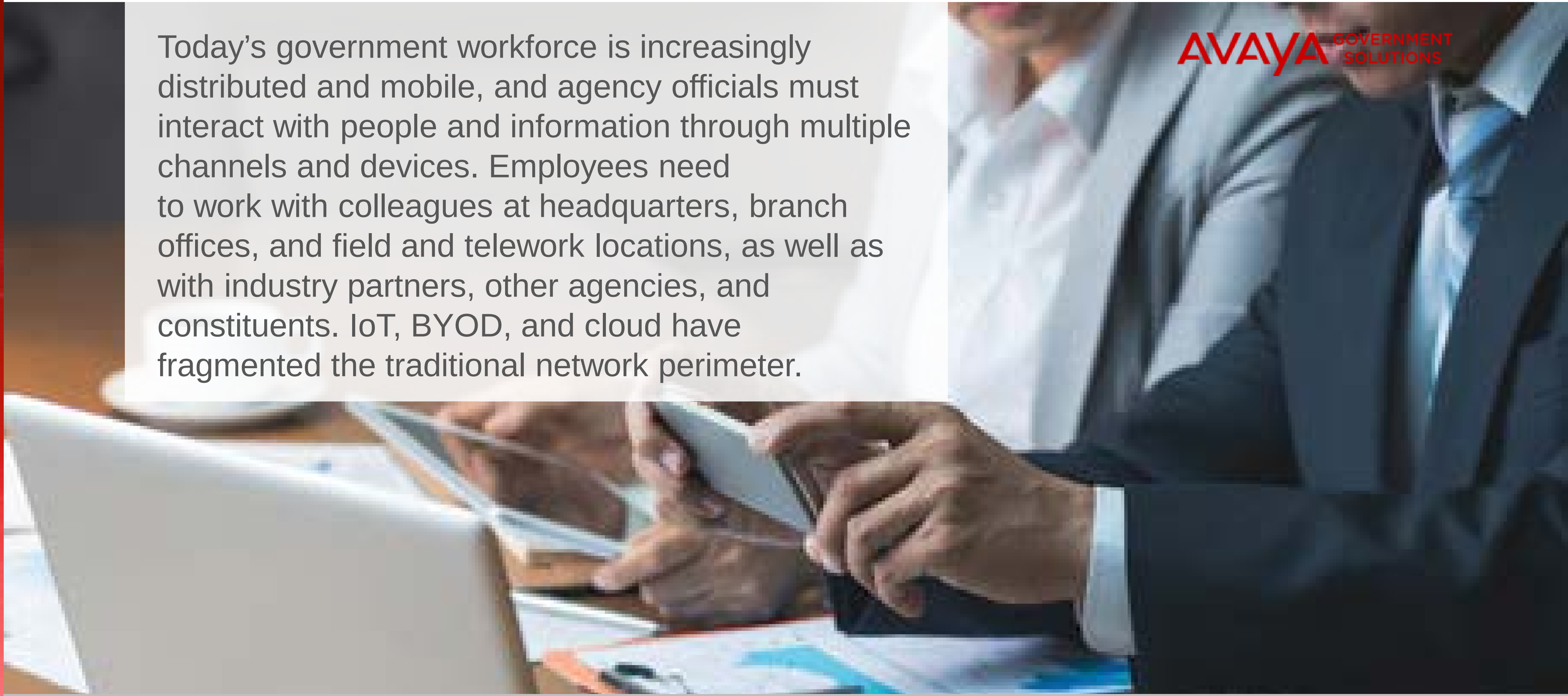
CIVILIAN AGENCIES

Challenges:

- o Leverage existing infrastructure
- o Optimize investments in modern networks
- o Shifting IT resources to enhancing digital services
- o Reduce TCO

Solution:

- ✓ Hybrid/interoperable framework
- ✓ Partition data and applications on the same physical infrastructure
- ✓ Incremental path for digital transformation
- ✓ Simplified design and maintenance reduces IT operating expenses



Today’s government workforce is increasingly distributed and mobile, and agency officials must interact with people and information through multiple channels and devices. Employees need to work with colleagues at headquarters, branch offices, and field and telework locations, as well as with industry partners, other agencies, and constituents. IoT, BYOD, and cloud have fragmented the traditional network perimeter.

SOLUTION

Avaya’s Practical Approach to Securing Everywhere Access

By providing a virtualized network that seamlessly manages hyper-segmentation, native stealth, and automatic elasticity across the organization, Avaya provides government agencies a cost-saving path toward secure digital transformation. Wired and wireless, access and core, data center and endpoint, all aspects of network topology are integrated by Avaya’s solutions that emphasize management simplicity, network resiliency, and optimal performance of communications and business applications—all within an integrated, next-generation framework of everywhere access.

Read the article on Securing the Everywhere Perimeter with Network Virtualization.

AVAYA GOVERNMENT SOLUTIONS

IT CAN BE THAT SIMPLE

There are some common misconceptions about what it takes to adopt a new approach to networking. The reality of Avaya's unique approach is simple and proven.

MYTH	VS	REALITY
Solution is limited to VLAN		Can virtualize millions of things; endpoint is the only place that must be locked in/segmented (provisioning at the edge)
Complicated to implement		Fully functional fabric network is achievable in two days; requires less staff and is less prone to configuration errors
Can't work with legacy technology		Hybrid capability/interoperability enables transition from legacy technology; enables multi-tenancy more easily
Increases costs		Reduces IT operating expenses; labor costs reduced by 85% with 25 times less network provisioning for deploying services
Increases work load		Simplified network virtualization solution eliminates cumbersome manual tasks; a single-technology network that reduces complex provisioning of protocol overlays simplifies management and troubleshooting
Issues with compliance		Shortest-path bridging is standards-based; IPv6 compatible

HOW TO ENGAGE WITH AVAYA GOVERNMENT SOLUTIONS

Avaya's unique approach to provisioning at the edge addresses the challenges of the "Everywhere Perimeter." Avaya's solution provides a foundational layer that seamlessly manages hyper-segmentation, native stealth, and automatic elasticity, making it easier and simpler to protect and manage everywhere access across any government agency.

Government agencies in 42 countries, including the national governments of nine out of the 10 largest economies, depend on Avaya solutions to ensure mission critical communications and system security. Contact Avaya Government Solutions today to learn how you can get started on securing your "Everywhere Perimeter."

☎

Contact Federal Government Solutions Team:

703-539-4570 or 1-800-492-6769

Find a Certified Avaya Government Partner:

http://www.avaya.com/usa/partner-locator/

AVAYA GOVERNMENT SOLUTIONS

AVAYA

GOVERNMENT
SOLUTIONS