ARMADA

Your data. Anywhere. Protected.

THE MOST SECURE & FASTEST VPN TO CONNECT THE PUBLIC SECTOR TO THE WORLD

WHY GOVERNMENT ORGANIZATIONS ARE REQUIRED TO HAVE STRONGEST CYBERSECURITY?

REMOTE WORKING: A PRACTICE BECOMING PART OF YOUR PUBLIC ORGANIZATION'S EVERYDAY LIFE

The pandemic crisis has pushed **Public Sector workers** to use their **personal devices** and **unsecured networks** to **work remotely**. Such a shift from the **physical to the virtual environment** is both a real **opportunity**, as it takes part of a **global digital transformation**, and a **threat**, as it significantly exposes your organization to a **growing cyberthreat landscape**, making it an ideal target for **cyberattacks**, as it is a goldmine of information that is **rarely protected** by the same level of cybersecurity practices used by many private enterprises.

As **distance working** becomes a part of your **organization's daily life and as** the **Public Sector** continues to make progress on its **digital transformation journey**, **cybersecurity** is becoming increasingly important in dealing with the **rise of hacktivism**.
Besides, a $1.2 trillion infrastructure package was signed into law by President Biden in November 2021, including $1 billion over four years to fund state and local cybersecurity efforts, an area where money has been lacking, particularly during the COVID-19 pandemic.
That decision truly confirms that cybersecurity has become a major concern for US Government and that it became necessary to fund security priorities after a year of escalating cyberattacks on key organizations.

YOUR PUBLIC ORGANIZATION: A PRIME TARGET FOR CYBERCRIMINALS

From ransomware attacks to data breaches, here are the major reasons why numerous public entities have fallen victim to cyberattacks in recent years:

1. **Lucrative targets for ransomware** - Cybercriminals, often state-funded, seek to disrupt critical infrastructure and operations that depend heavily on the Internet or internal networks for operation. Another category of cybercriminals is also emerging: the hacker who has political or social motives and who seek to draw public attention to an issue by throwing an unflattering light on the target, usually by releasing sensitive information to the public. Hackers also attempt to compromise confidential information and national secrets for spy purposes or to resell them on the Dark Web.

2. **Open technological environments** - Hackers seek to exploit any weak point in your systems to gain access to other critical systems and databases, and with so many devices purchased, security teams don't have the ability to ensure that every device is secure.

3. **Very valuable data** - Public sector cyberattacks are particularly destructive because they impact many lives considering how much government bodies facilitate our everyday life. From passports and driving licenses through social care, education to waste collection, the true scale of the threat becomes very apparent. While private entities are repeatedly told to put their security first, that level of urgency seems to be lacking in the Public Sector.

4. **Low tolerance for downtime** - For Public Sector organizations, there is no room for service disruption. When faced with a cyberattack, they need to continue running mission-critical applications to power essential platforms such as call centers, patient and judicial databases. But a disaster recovery (DR) strategy is necessary to be there for their communities.

REAL FACTS - WHAT WOULD HAPPEN IF YOUR SENSITIVE DATA WAS INTERCEPTED

Here are some alarming recent cyber attacks that underline the dismal state of cybersecurity in the public sector and the need for you, as institution, to build cyber resilience:

October 2021: An American company announced that the Russian Foreign Intelligence Service (SVR) launched a campaign targeting resellers and other technology service providers that customize, deploy and manage cloud services.

September 2021: The U.S. Department of Justice sentenced Ghaleb Alaumary to more than 11 years in prison for aiding North Korean cybercriminals in money laundering. His assistance included ATM cash-out operations, cyber-enabled bank heists, and business email compromise (BEC) schemes. These attacks targeted banks, professional soccer clubs, and other unnamed companies in the U.S. and U.K.

Nobody is ever 100% immune from daily-evolving cyberthreats, but with awareness of the issues and with our technologies at the helm, Public Sector organisations can rest assured that the risks they face can be reduced. The **need for security to strengthen data protection** across various devices, networks, and other collaboration tools **has never been greater in the sector**.

Don't wait anymore! Meet the security and mobility challenges with Armada.

ARMADA, THE MOST SECURE AND FASTEST VPN TO CONNECT YOU TO THE WORLD

Trust us to develop a robust cybersecurity strategy for your organization by investing in the **proactive Armada mobile VPN**. It's a must to keep your workers connected, safe and secured.
Let's work together to ensure your critical data, applications and systems are truly protected!

WHY CHOOSE US?

Our **mobile VPN Armada** is dedicated to **smartphones** and **tablets** using the **Android and iOS operating systems**.

It offers:

- **Secure remote access** to the organization's network resources.
- **Application and session persistence** even in the event of loss of connection, and **no user intervention** required if it happens.
- **Universal Content filtering**: limit access to non-compliant sites, block the internet, except for the approved sites or URLs.
- **Secure data transmission** over different unreliable wireless networks of all types (WiFi, LTE and Cellular).
- **Strong and rigorous authentication** of connected devices.
- **Public organization network extend**: mirrors your network no matter what network an employee connects. It allows staff to access information remotely while being controlled by IT securely.
- **Any device and applications compatible:** use smartphones to type on as a small computer instead of your traditional laptop. Turn it into a modem to connect your laptop.
- **Video Bonding:** patented solution allowing better video viewing or transmitting such as a teams or zoom session, where up to 40% packet loss will not affect the session.
- **Simple integration, Cloud compatible** or on premise deployment.
- **Easy and centralized administration** of the device fleet.
- **Seamless roaming** between WiFi and Cellular networks.
- **Simple and intuitive mobile user experience**, fast and reliable access to information, increasing the efficiency and productivity.
- **Reduced costs:** fewer calls to the IT department, fewer support tickets.

Image: wayhomestudio - freepik.com

ARMADA IS CUSTOMIZABLE!

Additional designs and button layout can be configured according to the customer need:

- Data Usage Reporting
- Content Filtering
- Organization Cloud Access
- Easily Managed
- Rugged
- Unlimited Data

TECHNICAL CHARACTERISTICS

- Technology developed according to open standards: Mobike, IKEv2
- Simplified integration into your architecture and deployment
- Linux Gateway
- Supports multiple hypervisors
- Supports multiple authentication standards (LDAP, Radius, AD, etc.)
- Supports PKI systems
- Compatible with Mobile Devices Management solutions (MDM)

Need more information about Armada? Looking for a solution with Android and iOS?
Contact us today to find out more:

NEWCOM | 781-826-7989
sales@newcomglobal.com | www.newcomglobal.com

NEWCOM

Radio IP
Redefining Secure Mobility