HYPORI™
VIRTUAL MOBILITY

How Federal Agencies Face Increasing Cybersecurity Challenges in the Age of COVID-19

WHITEPAPER

Summary

As the global COVID-19 pandemic continues to have an economic, social, and political impact on our nation and the world, businesses, families, and federal agencies face new daily challenges. Initially, predictions were for the virus to be a problematic disruption from which we would recover in the short term. However, COVID-19 and the precautions around it have become part of the fabric of our lives. Today, changes in how we live, work, and serve are becoming new ways of life for the foreseeable future.

Today across the country, federal agencies must continually adjust to the pandemic's impact. The most significant paradigm shift has been to telework and mobile device use by federal employees, contractors, and government officials. To continue providing agency services, conduct national affairs, and protect our country, public servants have to work and need access to agency networks and systems. Given it has been unsafe to gather in offices, many have teleworked on mobile devices.

The Situation

The nationwide shutdown is over, and stay-at-home orders have lifted, but many Americans still work remotely.

Many private businesses have announced long-term remote policies or permanent remote options. While overall, federal agencies may not incorporate 100% telework policies, some agency cyberchiefs now refer to a teleworking intelligence community "federal employee 2.0." Regardless, civil servant mobile device use, already widespread before COVID-19, will continue to rise.

Many civil servants, such as active military, used mobile devices before the pandemic. However, the recent increase in the variety of devices, including personal devices, presents additional challenges. Telework and mobile devices mean federal employees are productive during the pandemic, active service members are in the field with invaluable tools, and contractors maintain their roles. However, this is not without significant security and management concerns.

Telework and associated mobile device use mean multiple points of entry to any network or system. Users need off-site data access, including access to confidential information, and agencies need secure data control. According to a recent Meritalk report, 83% of federal agencies now embrace multi-cloud environments to support COVID-19-related telework needs. Cloud collaboration tools like Google Drive or Dropbox present additional vulnerabilities, but are necessary for daily tasks.

Ultimately, assuring data and networks' security, in many cases of highly classified systems, are imperative. Agencies and institutions need the highest cybersecurity protection while maintaining continued and uninterrupted service and productivity.

The Problem

Since COVID-19, federal agencies have faced large scale transitions like mobile device use, work-from-home technologies, increased activity on public-facing networks, greater use of online services, and cloud migrations.

Per social distancing guidelines, agencies nationwide continue to encourage telework wherever possible, meaning tens of thousands of civil servants access confidential network data daily. Many federal employees are teleworking without official provisions or policies. They don't have agency-issued equipment or training on connecting to, signing on to, or accessing federal networks, applications, and resources. Employees also use their own devices such as smartphones, tablets, and older laptops with both out-of-date operating systems and virus protection.

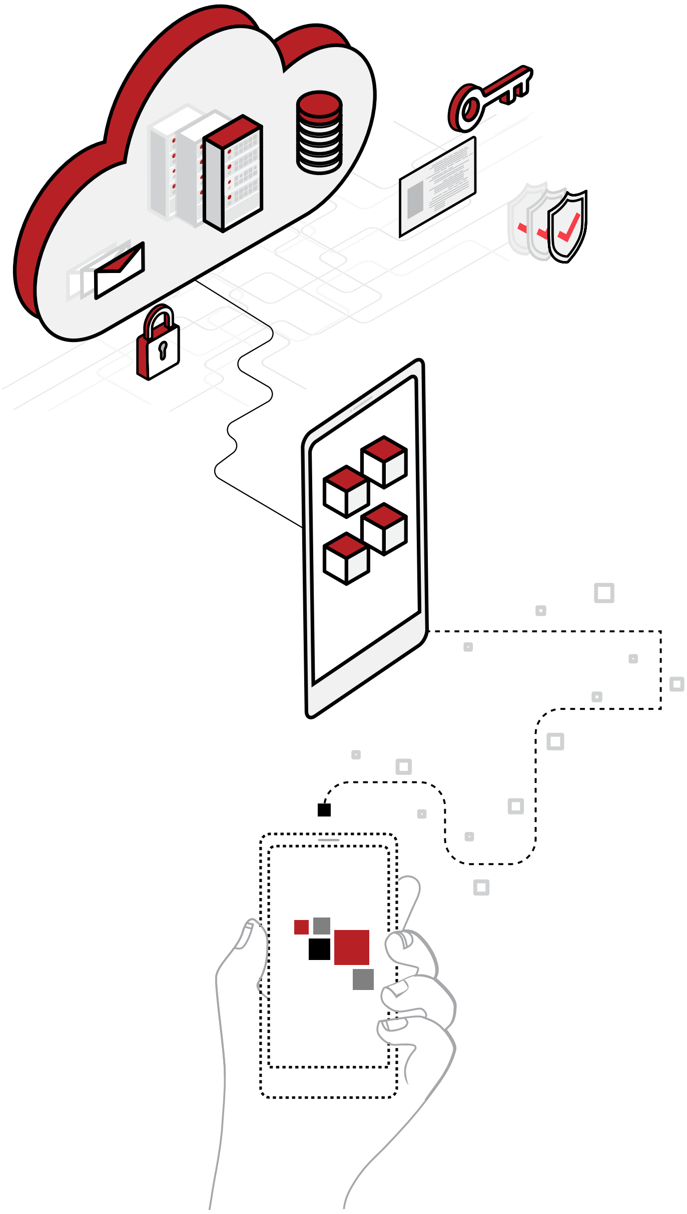
In addition to teleworkers, remote contractors and active service members continue to use mobile devices to perform work functions. Every remote point-of-access creates a security risk for federal agency networks and systems. This risk escalates when data access occurs via unsecured mobile devices such as personal smartphones and tablets. Given the exponential increase in user connections, some access and security policies have been relaxed or circumvented. Even virtual private networks (VPNs), otherwise considered secure, can't handle the traffic volume or deliver appropriate security controls for mobile device use and Bring Your Own Device (BYOD).

The overall cloud services market is expected to grow to **$266.4 billion in 2020**, and federal agencies already feel the change. With this growth comes a new set of concerns for federal agency IT departments and security experts. When working to secure cloud environments, problems include difficulty meeting regulatory requirements, lack of inherent and satisfactory security, and an increased attack surface. In one study, over 40% of federal agency cybersecurity leaders said their cyber strategies lag behind cloud computing evolution.

Cybersecurity was an issue before COVID-19, but all of these factors point to increased challenges. Federal agencies face a new normal, including shifts in how and where people work and what technology types keep them productive.

The Solution

Hypori Virtual Mobility addresses the cybersecurity challenges associated with increased mobile device use, increased teleworking, and other COVID-19-related changes. It delivers military-grade security enabling federal agencies to connect to multiple network classifications from a single device.



Hypori's solution securely contains all federal agency data, from social services to highly classified military information, in an agency-owned data center with 100% separation from end-user details and activities. Since all agency data resides safely on the agency-owned virtual device, there is no need to secure service members', civil servants', and government officials' personal devices.

With Hypori, agencies shift cybersecurity management from vulnerable personal devices to virtual devices that sit securely in a data center. Federal agencies have no access to personal data on end-user devices, and no exposure should they be compromised. All public sector mobile device users have secure virtual access to the information needed for successful telework without threatening national security.

Hypori's military-grade Virtual Mobility solution is also CSfC*, HIPPA, PCI DSS, FISMA, NIAP compliant, and Common Criteria certified and is currently used by the United States DoD.

To learn more about Hypori Virtual Mobility, contact us for a demonstration today.

Contact us

info@hypori.com

*The National Security Agency Commercial Solutions for Classified (CSfC) provides DoD entities the ability to conduct secure classified communications using Commercial-off-the-Shelf (COTS) products. Under this program the Mobile Access Capability Package v2.0 provides a framework for how to secure these communications from mobile end user devices into government enterprise resources. Under the MACP v 2.0, communications must be established using an inner and outer tunnel to provide the secure communications path. Intelligent Waves, LLC's Hypori Client v4.1 for iOS and Android is eligible to be used as a TLS Software Application Product component in a CSfC solution. This means that in combination with a CSfC eligible TLS Protected Server, Hypori is eligible to provide the inner tunnel for secure communications.

hypori.com