Ovum
TMT intelligence | informa

Government Agencies Should Expect More than Just MTIPS

Secure internet service is just the beginning of network security and advanced services with the new EIS contract

Publication Date: July 2018

By Mike Sapian

Summary

In brief

Cyberthreats have expanded and accelerated exponentially with the rise of mobility, BYOD, lack of corporate perimeter, and growing use of the Internet of Things. In the new General Services Administration Enterprise Infrastructure Solutions (EIS) contract, government agencies have a wider variety of security services – from selected providers – for better security options. The Managed Trusted Internet Protocol Services (MTIPS) program provides Trusted Internet Connection (TIC)-compliant managed security services through EIS, but that is not necessarily enough.

Ovum view

With the new EIS contract in place and with the larger variety of provider awardees, government agencies can now get a broader selection of services, solutions, and options. Along with the new providers comes more managed services that offer innovative versions of MTIPS-based internet services. EIS brings into the mix not only additional providers, but also some new offers around WAN, security, and other communications services. Many of these providers come with a new and fresh way to deliver services, support a larger variety of purchasing options, and offer several cloud-based programs. All these combined should give government agencies better opportunities for adoption of new, improved services that will help them transform the way they operate.

The introduction of providers will also allow for more creative options to help transition from legacy service agreements to newer, more flexible options; new consumption models; and innovative offers, including short pilots for new technologies and services such as SD-WAN**.** For the most innovation, agencies need to look beyond the traditional providers to the new providers, powered by their strategic vendors and partnerships. Agencies will see more nimble, responsive alternatives with new players that are not encumbered by legacy processes or networks. Many large agencies can also aggregate their provided services as an offer to smaller agencies to leverage many of these innovative and more cost-effective arrangements. Ovum expects many new alternatives that will be attractive to the agencies looking for innovative offers, legacy service replacements, and unique purchasing models.

Key messages

- MTIPS is focused on securing dedicated internet access. Most agencies will need complete WAN and hybrid network service protection.
- Internet, VPN, and security technologies have improved many MTIPS/TIC platforms but also allowed for integration of hybrid WAN services.
- Customers now require network security for all WAN services (hybrid WAN, SD-WAN) but want it to be available as a single integrated offer, aligned with an overall security strategy.
- EIS providers, empowered by strategic partnerships, are offering many advanced services with the new EIS contract, including holistic and transformational security solutions.
- MetTel has recently been added to the EIS contract and is one of the new, innovative providers, along with the traditional providers of these services such as AT&T, CenturyLink, and Verizon.

MTIPS is the beginning of security but not enough

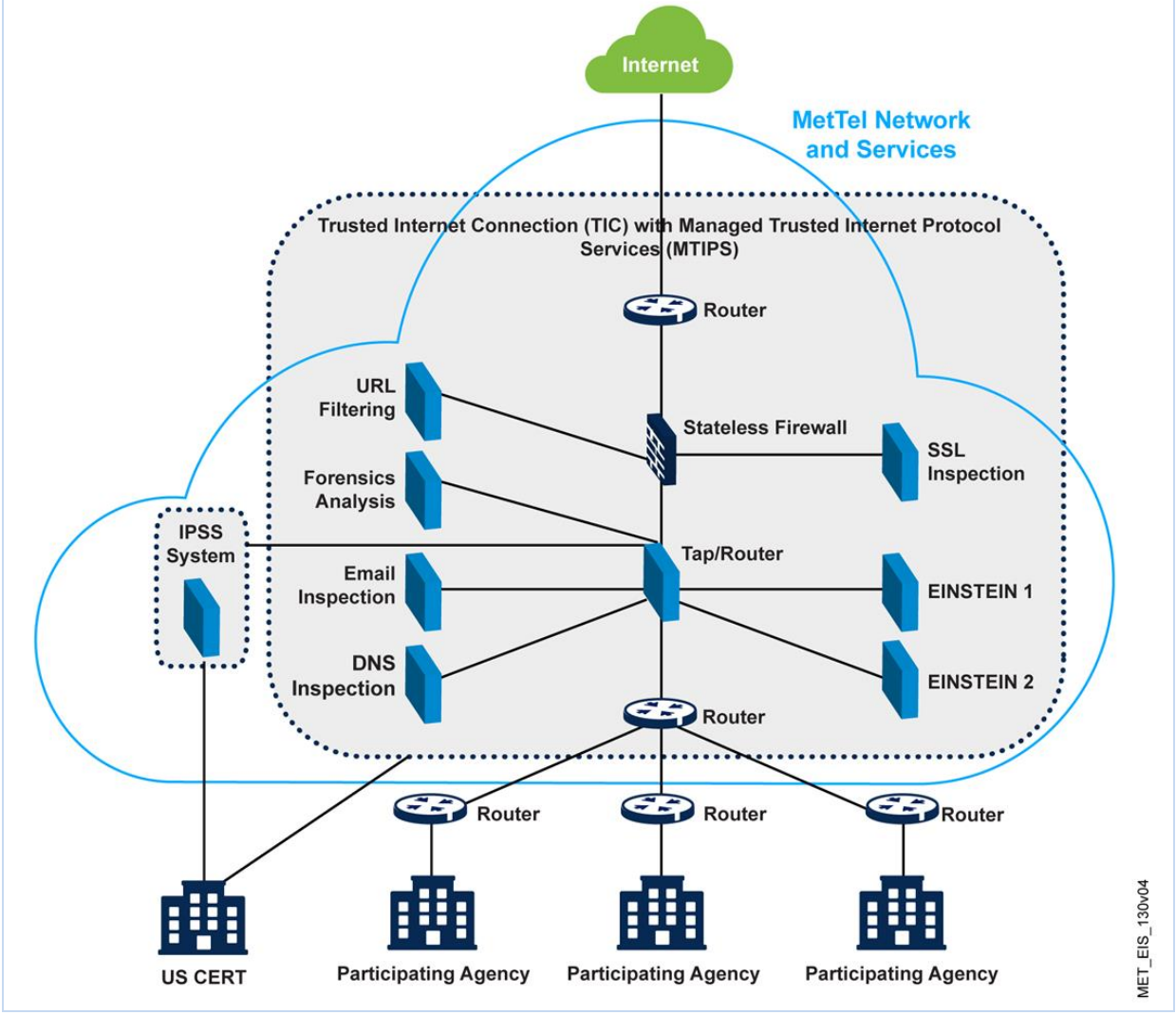
MTIPS has historically been one of the major components of security for federal internet services. The program began with the federal government's concern for use of the public internet. As MTIPS migrates to the new EIS contract, agencies can improve their overall security posture. What was once thought of as only "internet security" is now seen as a mission-critical element to safeguard all agency communications systems from threats inside and out. To better secure any organization and adapt to more intelligent threats, both reactively and proactively, a comprehensive security strategy with MTIPS at its core but surrounded by a range of additional managed security services is recommended. Only a short list of companies with expertise in providing these complex security solutions and services has been approved as part of the EIS contract. As you look at the menu for MTIPS and managed security services in EIS, you will see a few legacy players along with one new entrant – MetTel.

New and improved MTIPS platforms now available

Due to the speed with which digital technology advances, security around internet services and MTIPS platforms continues to progress at a rapid pace. Most legacy providers have updated their existing MTIPS platforms to provide more advanced features and capabilities in addition to basic internet access security. MetTel, for example, is providing more technical support, program management, and a wealth of new technology solutions from its partnership with Forcepoint to power its enhanced MTIPS service platform and broader managed security services. Forcepoint is majority owned by Raytheon and was acquired based on its reputation for providing security solutions in some of the most complex and rugged military environments. Raytheon has a long history of serving government agencies, including military installations.

MetTel's MTIPS service goes beyond internet service to support MPLS and the growing secure SD-WAN network implementations. Ovum's research has shown that more than two-thirds of customers (70%) are demanding increased use of internet as part of their SD-WAN service packages. MTIPS demand will increase based on this demand as agencies look for more secure ways to implement internet services in the hybrid network mix. Only solutions certified by the Department of Homeland Security (DHS) can be considered for use with government customers, which makes this MTIPS platform so critically important.

Figure 1: MetTel's MTIPS platform with highlighted unique features



Source: MetTel/Ovum

New EIS providers offer many advanced security alternatives with unmatched expertise

The EIS contract includes the traditional large US carriers (AT&T, Verizon, and Level3/CenturyLink) but also now includes some new service providers. Given the large investment required for the completion and compliance efforts related to competing for EIS services, this was somewhat of a surprise to most players in the US telecoms industry. One of the eight in the contract is MetTel, which is a large domestic communications solutions provider that has focused mainly on the enterprise market in the US and has developed a broad service portfolio of network and value-added services. Now government customers can leverage MetTel's expertise and innovative solutions to help them digitally transform their services, just as other enterprise customers can.

Keeping up with the rapidly changing cybersecurity landscape

A major challenge for federal agencies is that cybersecurity is evolving at an ever accelerating rate as threat actors grow in size and abilities. It has been increasingly difficult for agencies to pay for and keep the talent they need to ensure their own security. In the past, MTIPS often provided the only way for agencies to acquire security solutions, but today they can get the most advanced, adaptable solutions without having to rely on acquiring the skills in-house or making large capital expenditures.

MetTel can offer flexible, open WAN options with proven security packages through its Raytheon partnership. Beyond MTIPS, MetTel is approved for

- managed security services
- managed prevention services
- vulnerability scanning services
- incident response services

With agile companies offering adaptive solutions, predictive threat detection and anticipation is a real possibility for federal agencies.

MetTel with Raytheon: A new combination for network and security

MetTel is a comparatively small but extremely agile communications technology leader. While approved vendor status for federal contracts has long been the domain of major carriers such as AT&T, Verizon, and CenturyLink, MetTel has broken the mold as the first nontraditional provider to win a position in a contract such as EIS.

Raytheon is a well-established vendor in government circles. Raytheon's experience supporting federal and intelligence community customers in network, server, and web app security gives its cybersecurity customers a unique perspective on how best to handle the false positives and false negatives encountered during threat hunting and vulnerability scanning. Further, Raytheon has extensive subject-matter expertise in the reverse engineering and analysis of malware through its Cyber Security Innovations group.

Forensics and evidence collection capabilities

MetTel and Raytheon together offer "digital forensics and incident response" kits that consist of preconfigured laptops with best-of-breed software to perform forensics and handle evidence collection, among other functions, during incident response.

Specific MetTel-Raytheon programs include the following:

- The Managed Trusted Internet Protocol Service is newly built and leverages the latest technologies, including Forcepoint. It is powered by the MetTel-Raytheon partnership, which scales quickly and takes advantage of the newest advanced network technology for access.
- MetTel can also integrate Raytheon's Automated Threat Intelligence Platform and other advanced managed security services, including managed prevention services, intrusion-prevention security services, and security operations center capabilities.

- MetTel has invested in a new federal portal, which is integrated into and powered by its successful Bruin communications management solution. Over time, Bruin will provide detailed reporting and analysis for threat management.
- Agencies will have access to the Raytheon-managed DHS DOMino program, which provides support for large federal agencies such as the US Postal Service and the Department of Health and Human Services. DOMino leverages Einstein, which is the security analytics platform that detects cyberattacks targeting federal civilian government networks and actively prevents potential compromises.
- As part of the EIS contract, MetTel can offer a full MSSP portfolio of services, such as cybersecurity consulting and assessments, on a contract basis to federal agencies for custom consultations, including detailed review of security practices and recommendations for improving the security posture of the agencies and prioritization of security investments.

Further strengthening the MetTel security portfolio is Forcepoint, a division of Raytheon that has been serving the US government for years with military-grade security. Forcepoint is the premier firewall provider for all government agencies. Forcepoint's Next Generation Firewall (NGFW) combines fast, flexible networking (SD-WAN and LAN) with industry-leading security to connect and protect people and the data they use throughout diverse, evolving enterprise networks. It was designed from the ground up for high availability and scalability, as well as centralized management with full 360-degree visibility. Forcepoint NGFW uniquely combines enterprise SD-WAN with the industry's top-rated security, manageability, and availability to more efficiently protect today's highly distributed agencies.

Ovum believes that with innovative and proven providers such as MetTel, Raytheon, and Forcepoint partnering to deliver adaptable security to address the ever-changing security threats, the US government will greatly enhance the ability to safeguard its IT and communications networks. This portfolio of MTIPS plus managed services would also present a very compelling offering to commercial industry clients, as the partners expand it to the private sector.

Appendix

Author

Mike Sapien, VP & Chief Analyst, Enterprise Services

mike.sapien@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo