# How to Build a Foundation for the TIC 3.0 Era

## MARKET TRENDS REPORT

govloop FORTINET

# Introduction

Agencies continue to face a vast array of cyber threats, and network security is having a hard time keeping up. At the same time, more agencies than ever are moving data, applications and infrastructure to the cloud. In doing so, they are saving money while increasing efficiency, reliability, flexibility and the ability to collaborate. All of this has increased concerns about malware and unauthorized access, which can lead to the theft of sensitive data.

To address these issues, the federal government has worked hard to bolster agencies' network defenses through guidelines like the Trusted Internet Connections (TIC) program, which aims to strengthen the security of data, networks and boundaries. TIC 3.0 is a major step forward from TIC 2.2, adding use cases and bringing government IT closer to the capabilities available to the private sector by helping improve network security, digital efficiency, resilience and risk management posture in an environment-agnostic way.

But adopting TIC 3.0 guidance is only part of the solution. True network security requires more. It requires moving to modern technologies like SD-WAN; incorporating more automation, artificial intelligence and machine learning; implementing zero trust networking; and adopting a unified technology platform to tie it all together. Technologies like these make cybersecurity protection and defense more effective while consolidating network and security management.

To learn more about how agencies can achieve better network security, GovLoop teamed with Fortinet, which provides solutions that address critical security challenges. This report will discuss the current network security challenges agencies are facing and how to best address them.

# By the Numbers

1

**Within one year of OMB's September 2019 memo on TIC 3.0, agencies are required to update their network and system boundary policies and identify which TIC use case will be allowed for the agency.**

*Source: The White House*

---

# $3.86m

**The average cost of a data breach in 2020**

*Source: IBM*

---

***"The world marches forward, and cloud computing, strong encryption and mobile devices are now the norm. It's time again to increment the TIC model."***

*Source: CISA*

# 419%

**Top-tier IT infrastructure leaders are 419 percent more likely to have an end-to-end integrated security architecture than bottom-tier leaders.**

*Source: Fortinet*

---

# 62%

**of C-level executives said the growing threat of destructive cyberattacks is one of the top cyber concerns at their organization**

*Source: Deloitte*

---

1

**The most difficult to hire position of all is that of cloud security architect.**

*Source: Fortinet*

---

# 78%

**of security teams are planning to deploy zero-trust network access**

*Source: Cybersecurity Insiders*

# 72%

**of organizations consider security their top WAN concern**

*Source: Gartner*

# 57%

**of organizations are applying automation to help prevent security exposures to the network**

*Source: SANS*

# The Challenge: Complexity Creates Security Risks

Most agencies today use multiple clouds in addition to on-premises environments to house data and services. That makes it difficult to ensure security, especially when each environment has its own set of services and security policies. When that happens, it can easily cause security gaps and increase an agency's attack surface. Multi-cloud environments can make other security challenges more likely, due to poor network visibility and complex security management.

The current and abrupt shift to remote work also has challenged security. While agencies did whatever they needed to do to get employees up and running remotely, some had to cut corners on security policies, for example, to make things happen. Over time, agencies run the risk of those ad hoc changes becoming the "new normal."

"Out of necessity, some agencies accepted risk in the process of getting people to work remotely," said Jim Richberg, CISO for the public sector at Fortinet and a former federal executive for the federal intelligence community. "Now it's time to take a second look and make sure that everything is fully secure."

And as agencies work to combat cyber threats from all angles, many have adopted a variety of tools. Multiple studies find that most organizations have between 20 and 75 security solutions, each solving a separate problem. While these tools can help fight specific cybersecurity threats, they often don't integrate well with one another, creating visibility problems and increasing the workload on overextended cybersecurity staff. Tool and complexity overload can significantly reduce cybersecurity effectiveness.

# The Solution: Cut Complexity With TIC 3.0

One of the best ways to start addressing these challenges is by turning to the Cybersecurity & Infrastructure Security Agency (CISA)'s TIC 3.0 use cases. Working from use cases that support mobile computing, cloud, branch and remote users, agencies can move forward to accomplish their IT and security goals, while meeting changing mission needs and embracing new technologies.

TIC 3.0's direct-to-cloud use case, for example, lays out all of the functional elements necessary to create usable, secure, reliable cloud platforms. It provides agencies with the guidance they need to take better advantage of cloud technology, including closing visibility and security gaps that often result from inconsistent policy application to multiple cloud environments. It helps agencies understand which security policies and best practices are most important, shapes their IT cloud modernization with models such as zero-trust network access and builds capabilities for situational awareness, risk management and resilience.

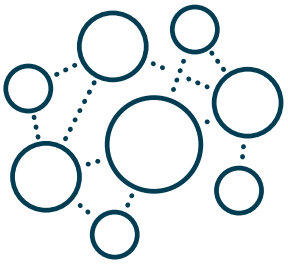
TIC guidance for branch offices facilitates agencies' use of Software-Defined Wide Area Networking (SD-WAN) technology to directly connect approved traffic to the internet instead of relying on expensive, low-bandwidth connections such as T1 lines. Implementation of SD-WAN technology has been growing exponentially in the private sector due to its compelling combination of cost savings, better user service and operational flexibility. Without SD-WAN, if an outage occurs, the traditional hub-and-spoke networking method requires IT staff at branch locations to manually fix problems and update capabilities.

With SD-WAN, the network software can automatically route around a problem, and can split traffic across multiple low bandwidth pathways to enable a composite higher bandwidth connection that can handle demanding applications like video conferencing. SD-WAN also allows agencies to manage both network and security operations for branch locations off-site and from a common control panel, which improves shared visibility and control.

The final TIC 3.0 use case revolves around remote users — something that is top of mind for agencies today as they grapple with defining their "new normal" operating posture post-COVID. Agencies want to ensure that remote workers' computing platform, data access and transmissions are fully secure, and that agency networks can handle the load with acceptable capacity, performance and security.

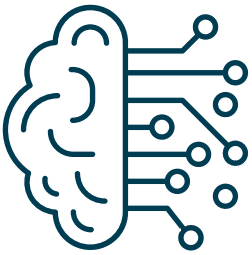
With this guidance, agencies can directly connect remote users to the internet instead of having to "backhaul" to an agency's network to pass through a trusted internet connection (TIC) or managed trusted internet protocol services (MTIPS). The best way to accomplish this is by using tools, including a virtual private network (VPN).

# Best Practices for Securing the Modern Enterprise



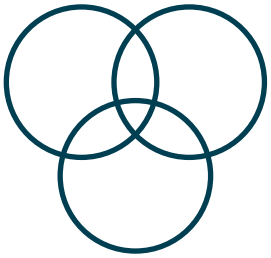
## Leverage the capabilities of secure SD-WAN.

Agencies are taking advantage of SD-WANs because of their compelling cost and performance advantages, but many of these solutions either ignore security or address it by ad hoc measures like "daisy chaining" of networking and on-site or cloud-based security that re-introduce complexity and potential performance problems. To avoid these problems, choose a modern SD-WAN solution that integrates networking, traffic management and security functions into a single appliance.



## Incorporate artificial intelligence and machine learning into your cyber strategy.

Protecting an agency against malicious activity requires both real-time situational awareness of activity across the IT environment and automated response. The deluge of security data agencies collect every day makes this virtually impossible without AI/ML technologies. Look for a solution with a mature AI/ML capability that has been trained and reinforced over time. This will provide the best results in terms of spotting malicious activity and differentiating true threats from false positives. By spotting and automating orchestrated responses to simple threats, security teams also will have more time to investigate and remediate efforts on more sophisticated and complex attacks. For agencies with sensitive information, consider a containerized solution that can be deployed on-premise, which provides the benefits of AI/ML without exporting data or telemetry from an agency's network.



## Shift from cyber solutions to a cyber platform.

While SD-WAN along with additional bolt-on security products can protect a network, you'll get the most value out of your cybersecurity investment by consolidating around a single technology suite or ecosystem. Independent research from NSS Labs demonstrated this point, and found that platform approaches to cybersecurity outperformed non-integrated best-of-breed solutions. "With a platform approach, you have the combined power of integrated cybersecurity solutions and more threat data," Richberg said. "That type of globalization of cyberthreat intelligence and the ability to quickly take action against anything the platform deems abnormal makes your solution more effective." While the platform approach is best, not all platforms are equally effective. Do your research to make sure the platform you choose is comprehensive, mature and an open-ended ecosystem of interoperable products and services from multiple vendors.

# Case Study: Overcoming Branch Office Security Challenges

By 2018, IT leaders at an independent federal agency that provides services to citizens and businesses had had enough.

With thousands of users at dozens of locations across the country, the process of transporting network traffic back and forth between branch locations and headquarters had become laborious and expensive. At the time, for example, network traffic from the West Coast offices would traverse the country via VPNs for final security inspection via a traditional custom TIC solution located at the East Coast headquarters. The inspected traffic would then leave headquarters, transit out across the open Internet (i.e., to a CSP, another federal agency or business partner), then return to the HQ TIC for reinspection and transmission across the agency WAN back to the West Coast field office. This less-than-desirable situation is often referred to as the "trombone effect."

The IT team first tried to address the issues by implementing large physical security devices to perform inspections, but found that it took too long, caused performance bottlenecks and was too expensive.

The next step was doing a proof-of-concept to determine whether the TIC 3.0 approach would solve their problems. Virtual instances of FortiGate software, along with other virtual Fortinet fabric products, were deployed via a public cloud service provider to connect branch offices to the closest regional zone for security inspection. Branch sites were secured via encrypted VPNs to the CSP.

The proof-of-concept was a resounding success, resulting in much better network performance due to a shortened path to the security inspection point, and lower costs. The agency also was able to use a variety of free tools available in the public cloud for management items associated with logging and reporting.

The agency then chose to formalize the solution. One year after full deployment, the agency saw a 50% cost savings in infrastructure due to the move from physical devices at headquarters to virtual equivalents in the cloud. The agency re-invested those savings, adding broadband connections to branch office sites that had SD-WAN technology, further improving network performance and increasing network resiliency.

## HOW FORTINET HELPS

Fortinet provides federal agencies with integrated and highly automated solutions to help modernize security infrastructures, enable SD-WAN architectures, move legacy infrastructure to the cloud and implement zero-trust networking principles.

With an ever-growing attack surface and increased digital complexity, agencies today need to be able to intelligently examine network traffic in real time. Fortinet's security-driven network solutions provide the ability to not only examine network traffic in real time, but track it over time to see what's normal and what's abnormal. "With AI and ML integration, the platform also can determine whether the abnormal behavior simply bears watching or whether it matches the characteristics of malicious activity and should be blocked immediately," Richberg said.

Fortinet solutions are compliant with both FIPS 140-2 and Common Criteria. They also are certified by the NSA's Commercial Solutions for Classified program.

***To learn more visit: www.FortinetFederal.com.***

# Conclusion

TIC 3.0, the latest and most advanced federal guidance on improving network security, is a good place to start for agencies with growing resources in the cloud.

With specific cloud-related use cases, TIC 3.0 addresses head-on challenges around traffic visibility, security gaps and the ability to maintain control over that traffic. Its use cases specifically for branch offices and remote users are particularly relevant in today's remote work environment. By relying on TIC 3.0 and adopting enabling technologies like SD-WANs, agencies can make great headway in ensuring network security across the board.

Along the way, agencies should carefully evaluate their technology options, focusing on intelligent features like artificial intelligence and machine learning, as well as considering an integrated cybersecurity platform.

## ABOUT FORTINET

Fortinet (NASDAQ: FTNT) provides federal government customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and in the future.

The federal government owns some of the world's most sensitive—and coveted—data. Compromised systems can lead to disastrous consequences—for national security, the economy, and technological innovation. By providing integration, automation, compliance, and performance at scale, Fortinet offers federal agencies world-class solutions for on-premises perimeter security, secure remote access, multi-domain networks, advanced threat protection, zero-trust network access, operational and security awareness, third-party and insider threat protection, and many other needs.

## ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.


1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop