RESEARCH BRIEF

ZERO TRUST

THE NETWORK SECURITY INFRASTRUCTURE OF TOMORROW

vmware®

carahsoft®

INTRODUCTION

In our interconnected and highly-globalized world, agencies must deploy emerging technology to improve service delivery and connect employees to data anywhere, anytime. But as trends like cloud, virtualization, telework and mobile continue to gain traction in government, cybersecurity cannot be an afterthought: it's mission critical. And now, more than ever before, mitigating the impacts of a cyberattack is of the highest national importance.

Today, cyber hackers can be anyone from disgruntled employees, nations or terrorist organizations. Therefore, how we protect government networks requires a shift in mindset. The network security phrase "trust yet verify" is now an archaic way of addressing the challenges of network security.

No longer can agencies trust that they have an impenetrable boundary as their first line of defense to protect their data. Cyber professionals now realize that no information is safe. There is no longer an easily defined security perimeter. No person can be trusted. And, inevitably, an organization will be attacked.

That's why now is the time for government to embrace a new approach to cybersecurity. This change in mindset is what Forrester Research describes as the "Zero Trust" model.

Throughout this research brief, GovLoop and VMware will illustrate the benefits of a Zero Trust approach to cybersecurity, and how it can help organizations remain safe and secure in the radically changing world of network security.

Specifically, this report will:

- Examine findings from a recent GovLoop and VMware survey of 80 respondents, mainly state and local government employees (See Figure 1, page 4.)
- Discuss micro-segmentation and how it relates to a Zero Trust approach.
- Highlight findings about Zero Trust from Forrester Research.
- Include comments explaining the Zero Trust model from two industry experts at VMware: Ahmed Ali, Networking and Security Account Manager; and Geoffrey Huang, Director of Product Marketing, Networking and Security.

With the Zero Trust model, state, local and federal agencies can protect all resources regardless of location; deploy a least privilege strategy with strict access control; and inspect all log traffic on a network. With this model, government, at all levels, can be confident that their networks are secure, and prepare to mitigate the impacts of an attack when one occurs.

In this report, we go in-depth into the meaning of the Zero Trust approach, and discuss how state, local and federal agencies can benefit from this new network security model. As our research shows, today there is an opportunity for government to learn about the power of the Zero Trust model. Our report is your first step to learning about the advantages of the approach and how it can improve the public sector's overall security posture.

THE STATE OF CYBERSECURITY

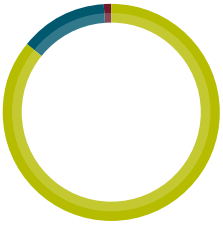
We surveyed the GovLoop audience to gain a better understanding of their knowledge about the Zero Trust model, cyberthreats they face and their level of confidence in their ability to thwart cyberattacks. Our survey consists predominantly of state and local government employees.

So what does cybersecurity look like, according to the GovLoop community? Some of our findings are revealed below.

WHAT LEVEL OF GOVERNMENT DO YOU WORK FOR?

53%	State
23%	County
17%	City
4%	Other
3%	Federal

HOW IMPORTANT IS NETWORK SECURITY TO YOUR ORGANIZATION?



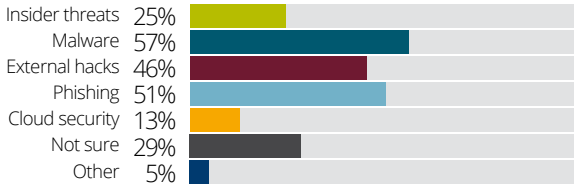
86%	Very Important
13%	Somewhat Important
1%	Not Important

HOW WOULD YOU RATE YOUR AGENCY'S STATE OF CYBERSECURITY?

3%	Not at all safe
20%	Somewhat Safe
32%	Adequately safe
37%	Very safe
8%	Extremely Safe

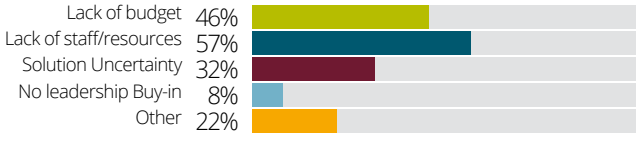
WHAT IS THE BIGGEST CYBERSECURITY THREAT FACING YOUR AGENCY?

(SELECT ALL THAT APPLY)



WHAT ARE THE BIGGEST BARRIERS PREVENTING YOUR ORGANIZATION FROM BEING SAFE?

(SELECT ALL THAT APPLY)



WHAT IS ZERO TRUST?

This survey indicates that there is an opportunity to teach individuals about the benefits of Zero Trust, especially at the state and local level of government.

"Most IT admins (public and private sector) adopt an 'outside-inside' strategy: build a moat around your data center to keep bad actors out, and assume that everything inside the data center is consequently secure. Zero Trust inverts this approach: of course, you need to protect the perimeter of your data center with firewalls, but more than that, you need to have security everywhere inside the data center, down to the finest granularity possible, " said Geoffrey Huang, Director of Product Marketing, Networking and Security at VMware.

When survey respondents were asked about their knowledge of the Zero Trust approach, 62 percent responded they had not heard of Zero Trust, while 22 percent vaguely understood the model. Only 6 percent of individuals were familiar with the Zero Trust architecture, and 80 percent of individuals who understood Zero Trust had no plans to implement the security model.

"With Zero Trust, IT administrators start with the assumption that threats could be anywhere inside the data center, then act accordingly. The result is a network where security is pervasive throughout the data center, rather than a network that attempts to secure only the boundary of the data center," said Huang.

This new model comes at a time when agencies are facing more high-profile data breaches, even though organizations are spending more and more on securing networks. For many organizations, the reality is that they are spending more on infrastructure, without becoming any more secure.

Part of the reason why is that security today is often based on two flawed assumptions, which Zero Trust seeks to solve. The first is that there are people that you can trust. The second is that you will be successful 100 percent of the time in thwarting attacks.

"What we have learned over the course of a couple decades assessing cyber strategies is that those two assumptions are completely false and invalid," said Ahmed Ali, Networking and Security Account Manager at VMware. "If you build a security program based on them, bad things will happen."

What the Zero Trust approach does is create a security policy and architecture that trusts no one, and makes the assumption that security defenses will ultimately be breached. "An agency is not going to be perfect 100 percent of the time. The policy should ultimately seek to limit the damage of a breach," said Ali.

"A Zero Trust approach allows public sector entities to make their cybersecurity posture far more resilient, limit the damage of any breaches, while giving better success rates for protecting the citizen data they are entrusted with," said Ali.

With the Zero Trust approach, organizations will not only be safer today, but will also retain an architecture that will protect them from future threats. Although the term is still fairly new in the government space, there are some institutions that are beginning to adopt the model.

"The earliest examples are in national security, state governments and higher education," explained Ali. "These organizations have seen the most pressure from recent insider threats. There is a common understanding that the architectural model they have been using to secure their data is not aligned with the modern threat environment."

As we've described, the Zero Trust architecture creates tight security within a data center. But, in order to achieve this, there is another important component to the Zero Trust architecture: micro-segmentation.

"Micro-segmentation is an example of Zero Trust in action," said Huang. "It is one way — possibly the only realistic way — to achieve Zero Trust. It applies a software-defined data center approach to networking: namely, giving IT admins the ability to create, move, snapshot, restore and delete entire networks fully in software — just as IT admins do with virtual machines today. This network virtualization capability makes it possible to have tight, finely granular security everywhere in the data center."

Many organizations have already started to explore network virtualization. Our survey found that, currently, 57 percent of government is considering a software-defined data center or network virtualization platform. With network virtualization, the survey finds that reduced costs, increased security and simplified infrastructure management are the top three benefits organizations are seeking to gain.

Individuals not pursuing a virtualization platform articulated this was because they were not sure about what it is, lack the budget for it and are uncertain about its benefits (Figure 2).

Given all the benefits of Zero Trust, what is preventing organizations from deploying the model? Our survey finds that a lack of knowledge about implementation was the leading factor, at 50 percent; additionally, 24 percent of organizations lack skilled employees to deploy the service (See Figure 1-C.)

Figure 1-A.

ARE YOU AWARE OF WHAT THE STRATEGY OF ZERO TRUST OR MICRO-SEGMENTATION IS?

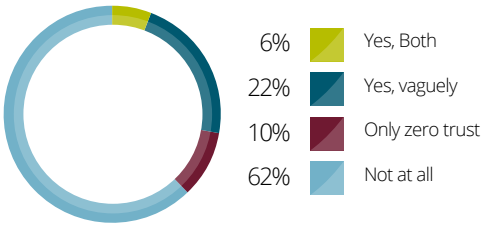


Figure 1-B.

IF YES, DOES YOUR ORGANIZATION EMPLOY A ZERO TRUST OR MICRO-SEGMENTATION STRATEGY?

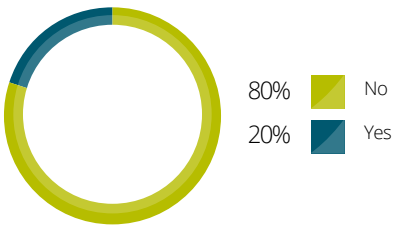
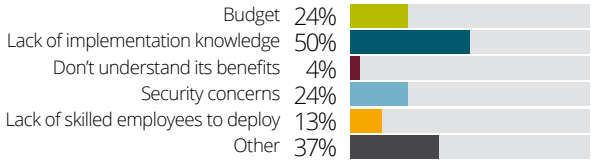


Figure 1-C.

IF NO, WHAT IS PREVENTING YOU FROM EMPLOYING A ZERO TRUST OR MICRO-SEGMENTATION STRATEGY?
(SELECT ALL THAT APPLY)



THE ZERO TRUST FRAMEWORK

Today, in order to protect a network, security teams rely on several different security instruments to keep data secure. These could range from web application firewalls (WAFs), content-filtering gateways or network access control solutions. For the Zero Trust network, however, Forrester believes a new kind of product category will emerge: the segmentation gateway.

"[The segmentation gateway] takes all of the features and functionality of individual, standalone security products and embeds them into the very fabric of the [segmentation gateway]. By embedding a packet-forwarding engine, we have a device that can sit at the very center of the network. The software gateway's larger value lies in its ability to properly segment networks in a secure manner and build security into the very DNA of the network. Presaged by the rise of unified threat management (UTM) and next-generation firewall (NGFW) appliances, the Zero Trust segmentation gateway vision is well on its way to reality," reads a Forrester report.

Organizations must focus on learning how to build a Zero Trust infrastructure. But Forrester warns that all the technology components are not yet available for purchase. "While you cannot go out and simply buy a Zero Trust network, cybersecurity professionals can use the architectural design components of Zero Trust to help get past today's biases about how we should build networks and begin looking at network design from a new point of view," said the report

The key components to creating the Zero Trust architecture are:

» **Manage data for security & compliance**

With Zero Trust, organizations can build compliance into the architecture. For example, if one security requirement entails the placement of a firewall between a wired and wireless network, the Zero Trust network can implement the firewall automatically, rather than making this task a manual process for security teams.

» **Centrally manage from a single console**

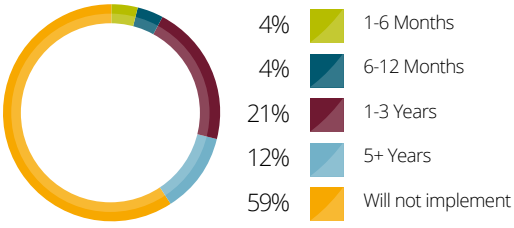
With Zero Trust, security teams can manage from a single location and gain improved network awareness about the state of their systems. Zero Trust reduces complexity and consolidates management consoles, making it easier for managers to understand the state of their networks and what vulnerabilities might exist.

» **Collect, analyze & manage all data**

Critical to the success of a Zero Trust network is the ability to identify and track all log traffic across the network. Forrester refers to this as a "data acquisition network," in which all data is collected in a single place and can be analyzed in near real time.

Figure 1-D.

IF YOU ARE GOING TO IMPLEMENT A ZERO TRUST OR MICRO-SEGMENTATION STRATEGY, IN WHAT TIMEFRAME DO YOU PLAN ON DOING THAT?



10 Benefits of the Zero Trust Model

Zero Trust provides many benefits for the public sector, and below we highlight ten. With Zero Trust you can:

1. Obtain a holistic view of your network for improved network visibility to spot trends, patterns and abnormalities.
2. Consolidate many disparate systems to gain more value from your existing IT.
3. Become more proactive against cyberthreats, because identities are established before accessing network.
4. Develop robust security policies and then automate them to save employee time and reduce human error.
5. Reduce cost of ownership through consolidated solutions and improved management.
6. Secure and enable IT trends like mobility, telework, cloud computing and virtualization.
7. Maintain government compliance by segmenting off highly-sensitive data and information.
8. Reduce your attack surface by deploying a least privilege policy and access control
9. Prepare your network to be secure for future trends, such as the "Internet of Things."
10. Fortify your security posture by taking an "inside-out" approach to security, which secures data within your network and trusts no one to access your network without proper credentials.

HOW VMWARE CAN HELP

VMware offers a full suite of services to help deploy the Zero Trust approach. With cybersecurity being of critical importance for government agencies, it's time for agencies to embrace the new model, and craft the necessary architecture. This means exploring the software-defined data center (SDDC), which will give agencies the benefits of increased efficiency and agility.

Additionally, agencies will gain the advantages of computing, networking and storage and greatly improve their ability to meet mission need.

But, above all, the VMware SDDC model provides "baked-in" security advantages, due to VMware's NSX platform. With this platform, agencies are able to move toward the Zero Trust model, and reduce incidents of cyberattacks. With these baked-in strategies, VMware is helping organizations make micro-segmentation a reality in the data center for the first time.

In addition, VMware NSX consists of three kinds of security for data centers:

1. Fully isolated virtual networks
2. Segmented virtual networks
3. Segmentation with advanced security services

Now, security solutions like micro-segmentation are a feasible, cost-effective way to help improve network security — making a secure data center a reality.

"Zero Trust alludes to one of the key changes as to how an agency must approach cybersecurity: they cannot seek a magic product that is going to be their savior from a cybersecurity perspective. Zero Trust is a different approach: it is not a product, it is not a solution — it's an approach to doing cybersecurity," said Ali.

If you are looking for more information on the Zero Trust approach, be sure to view these additional resources:

» Developing a Framework to Improve Critical Infrastructure Cybersecurity

» Data Center Micro-Segmentation: A Software Defined Data Center Approach for a "Zero Trust" Security Strategy

Figure 2.

ARE YOU AWARE THAT NETWORK VIRTUALIZATION CAN LEAD TO A BETTER SECURITY MODEL?

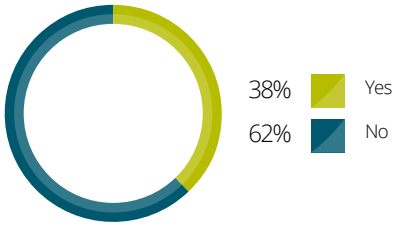


Figure 3-A.

DOES YOUR ORGANIZATION CURRENTLY HAVE OR ARE IS CONSIDERING A SOFTWARE DEFINED DATA CENTER OR NETWORK VIRTUALIZATION PLATFORM?

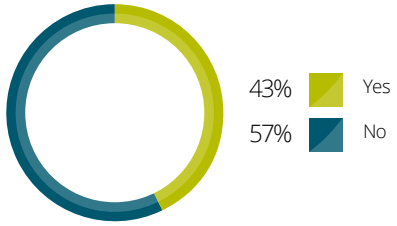


Figure 3-B.

IF SO, WHAT BENEFITS ARE YOU HOPING TO DERIVE FROM THIS NETWORK VIRTUALIZATION PLATFORM?
(SELECT ALL THAT APPLY)

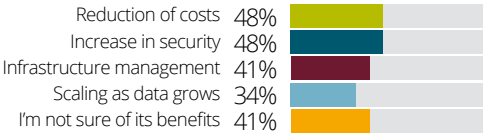
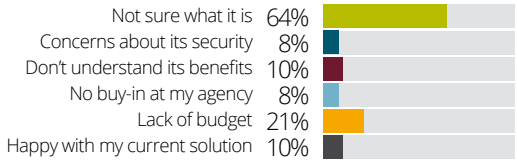


Figure 3-C.

IF NO, WHAT ARE YOU NOT CONSIDERING A NETWORK VIRTUALIZATION PLATFORM?
(SELECT ALL THAT APPLY)



ABOUT VMWARE

VMware is the industry-leading virtualization software company. VMware's technologies simplify IT complexity and streamline operations, helping businesses become more agile, efficient and profitable. By virtualizing infrastructure—from the data center to the cloud to mobile devices—VMware enable IT to deliver services from any device, anytime, anywhere.

vmware®

carahsoft.

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 150,000 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
Catherine Andrews, Director of Content at
catherine@govloop.com.

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop

GovLoop
1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
@GovLoop