CONSIDERING THE CLOUD? FIVE QUESTIONS FEDERAL AGENCIES SHOULD ASK

By Aamir Lakhani, lead researcher and cybersecurity expert, Fortinet

The cloud is an increasingly attractive prospect for federal agencies, but many still have unanswered questions about how public cloud security stacks up. Now that the president has mandated a move to the cloud in a recent cybersecurity executive order, agencies will have to move quickly to comply. Below are five key questions that federal technology leaders should ask their public cloud prospects to see if they have what it takes to store and manage federal data securely.

1. Do you allow auditing or pen testing in your environment?

Many customers are not aware that there are major cloud providers that do not allow pen testing. Though this makes sense, as it could damage the cloud that other customers rely on, it also makes for a challenging situation. Most customers do not realize how to audit applications and aren't sure what they are allowed to audit. The only course available with these vendors is to run the denial-of-service attack and see if the application will survive the load. To avoid this scenario, then, choose a solution that allows auditing and testing.

2. Are my apps ready for the cloud? How do I support my apps in the cloud, and how do I get my data back?

These questions should be answered when applications, especially custom applications, are being designed, not further down the road. Agencies need to build into APIs application controls that allow them to audit those applications. Nowadays, when an agency is thinking about applications, it needs to make sure the apps are cloud-ready. This means not only asking if the app can run on Amazon or Microsoft, but making sure it can be inspected deeply through APIs versus through just a gateway. A gateway is not going to do any good when everything is encrypted in between.

Agencies must also consider which applications actually need to move to the cloud, and in what time frame. Migrating to the cloud is more complex than "lift and shift"; customers need to ensure that those apps will have the support they need and that they will be able to retrieve all the apps' data.

3. Is your security scalable?

Security needs to be elastic to scale with the cloud infrastructure itself and to provide transparent protection without slowing down the business. Cloud environments need super-fast physical firewalls that provide highly scalable north-south data center and network security protection at the edge of the private cloud. They also need virtual firewalls that provide north-south protection for public clouds. In addition, they need virtual firewalls that provide "east-west" protection for data and transactions moving between devices in the cloud. High-performance firewalls and network security appliances need to scale vertically to meet performance and volume demands, and horizontally to seamlessly track and secure data from IoT and endpoints, across the distributed network and data center and into the cloud.

4. Is your security aware?

A cloud provider's underlying security infrastructure should offer automatic awareness of dynamic changes in the cloud environment to ensure holistic data safety. It's no longer sufficient to detect bad traffic or block malware using discrete security devices. Security should be integrated into a SIEM and other analytic tools (such as Big Data Security Analytics) in private and public clouds, with the ability to gather and correlate data. This will enable automatic orchestration of changes to security policy and posture in response to detected incidents and events. The individual elements need to work together as an integrated and synchronized security system with true visibility and control.

5. Do you offer segmentation?

Because pooling resources through technologies such as virtualization and software-defined networking (SDN) creates significant IT efficiencies, cloud environments have become increasingly aggregated – to the point where entire data centers can be consolidated. If a cybercriminal or advanced threat breaches the cloud perimeter via a single vulnerable application, there's usually little to protect critical assets within the flat and open internal network. To mitigate the serious potential for damage and loss, organizations need to separate business units and applications. Networks need to be intelligently segmented into functional security zones to control east-west traffic.

End-to-end segmentation offers deep visibility into east-west traffic moving across the distributed network, limits the spread of malware and enables the identification and quarantining of infected devices. A strong end-to-end segmentation strategy includes internal segmentation firewalling across data centers, campuses and local offices, and secure micro-segmentation for SDN and cloud environments.

MAKING A SAFE SHIFT

With a mandate from the White House to migrate to the cloud, federal agencies are feeling the pressure to make the shift quickly yet securely. Agencies must vet their options thoroughly to ensure the choices they make keep government and citizen data safe. Asking the five questions above will help rule out unsatisfactory solutions and provide a firm foundation for the government to enjoy greater security, efficiencies and cost savings.

ABOUT THE AUTHOR:

Aamir Lakhani is a leading global cybersecurity strategist and researcher with experience in zero-day research, exploit development, network and infrastructure implementation, malware research, digital forensics and cyber underground research. He has worked with multiple vendors and technologies on large-scale deployments, leads research on major global malware outbreaks with multiple competitive security corporations, has appeared on major media outlets discussing cyber security, and is the author of several cybersecurity books.

ABOUT FORTINET FEDERAL

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. We empower our customers with intelligent, seamless protection across the expanding attack surface, and with the ability to take on ever-increasing performance requirements of the borderless network - today and into the future. Our federal solutions protect the classified and unclassified systems used by 12 of 15 cabinet-level agencies, and those of numerous independent agencies, utilizing Fortinet's specially configured USG product line. These platforms comply with federal certification requirements including NIST FIPS 140-2, NIAP Common Criteria certification, and are on the Commercial Solutions for Classified Programs (CSfC) approved Components List. Learn more at www.FortinetFederal.com.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

Fortinet Federal, Inc.
12005 Sunrise Valley Drive
Suite 204
Reston, VA 20191
Tel: 703-815-7197
federalsales@fortinet.com
www.fortinetfederal.com