STRATEGIC SECURITY ARCHITECTURES
FOR CLOUD DATACENTERS

Prepared for
<VA> vARMOUR

By
Peter Christy, Research Director
ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

© 2015 451 Research, LLC and/or its Affiliates. All Rights Reserved. Reproduction and distribution of this publication, in whole or in part, in any form without prior written permission is forbidden. The terms of use regarding distribution, both internally and externally, shall be governed by the terms laid out in your Service Agreement with 451 Research and/or its Affiliates. The information contained herein has been obtained from sources believed to be reliable. 451 Research disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although 451 Research may discuss legal issues related to the information technology business, 451 Research does not provide legal advice or services and their research should not be construed or used as such. 451 Research shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.
# TABLE OF CONTENTS

## STRATEGIC CONTEXT

**THE SECURITY CHALLENGES**  
1  
*Digitalization Breaks Infrastructure* 1  
*Digitalization also enables new and powerful infrastructure* 2

## CLOUD COMPUTING

3  
*New application deployment architecture.* 3

## CLOUD SECURITY

4

## ABSTRACTION

4

## THE POWER OF VIRTUALIZATION SOFTWARE

4  
*New infrastructure architecture enables new solutions* 5

## VIRTUALIZED SECURITY INFRASTRUCTURE

6

## THE CHALLENGES IN IMPLEMENTING VIRTUALIZED SECURITY

7

## SUMMARY

8
STRATEGIC CONTEXT

Enterprise IT is undergoing rapid evolution driven by the collective opportunities provided by mobile devices, the Internet of Things, big data and cloud computing. Together these technologies are transforming businesses by providing greater insight into the business opportunities and challenges, and enabling rapid response and adaptation. We talk about the end result as the ‘digital enterprise’ and of the ‘digitization’ of businesses. Industry leaders like Cisco’s John Chambers speak of digitization as an existential issue, warning that companies that don’t transform won’t survive.

IT for a digital enterprise requires new technology and architectures, and much of what is new is in ‘infrastructure’ – all the software and hardware that sits under the executing application. Our focus here will be on the security aspects of infrastructure, where it is clear that the old models and mechanisms no longer work, but also that new cloud-scale software architectures offer new and powerful mechanisms for modern IT security.

THE SECURITY CHALLENGES

Historically we have defended IT against attack in a manner similar to defending a castle. We trust things inside the castle walls and distrust things outside the walls, with the objective of keeping them out. In IT the ‘wall’ is usually a network perimeter – we trust users inside the network and distrust those outside, with the goal of stopping attacks at the perimeter, thereby preventing compromise of the internal resources.

DIGITALIZATION BREAKS INFRASTRUCTURE

![Diagram showing the transition from trusted assets and trusted individuals to untrusted individuals with the network perimeter]

Assets & Trusted Individuals

Untrusted Individuals

Network Perimeter
The 'castle' defense just doesn’t work anymore, for many reasons. First, fewer application users are inside the castle, in part because an increasing percentage of users aren’t employees (e.g., business partners, customers, prospects), and also because even the employees are increasingly using applications outside the castle via external Wi-Fi or cellular access through the Internet. Second, it’s no longer enough just trying to prevent breach and compromise. Modern attacks are described as ‘slow and persistent,’ where a seemingly minor initial compromise is just the first step toward the ultimate goal. There is abundant evidence that most businesses suffer this kind of compromise, and that the more important focus is on how fast you can detect the breach and mitigate the damage.

**DIGITALIZATION ALSO ENABLES NEW AND POWERFUL INFRASTRUCTURE**

The bottom line is that you can’t implement security at the perimeter and hope to succeed. Whether an individual is inside or out tells you little about their trustworthiness. With slow and persistent attacks, even ‘trusted’ people must be watched carefully because their system or identity may have been compromised. Simple categorical (black-and-white) security can’t work any more. Security decisions – whether to permit or deny some action – have to be made in a very granular way: what should a person be able to do at some moment with respect to a specific service or data item?
CLOUD COMPUTING

Meanwhile, it has never been easier to use an application. Modern cloud computing enables on-demand services where computation and storage resources are available within minutes at essentially any scale, and you only pay for what you use. It is no longer necessary to buy, install, provision or run a server in order to get the benefit of an application.

From an infrastructure perspective, cloud computing is very different. We are used to provisioning each application separately – literally as its own set of dedicated hardware and software – then connecting it to a network for access to resources (data), for links between applications, and to provide external access. With cloud computing, however, we ‘virtualize’ the hardware resources with a new layer of software. For example, we virtualize a server by use of a hypervisor that enables that server to be shared between multiple incompatible software stacks; and we virtualize the network with a layer of software that creates logically separate application networks that all share common hardware resources.

NEW APPLICATION DEPLOYMENT ARCHITECTURE

Cloud computing is a new challenge for IT organizations that are used to managing the performance of isolated, discrete applications. With a cloud fabric, all applications share the same resources, so diagnosing and remediating problems is an entirely new challenge, as is managing resources that are critical to the availability of many applications.
CLOUD SECURITY

With a cloud datacenter, security also takes an entirely new form. When the applications are each in a separate silo, security is implemented in the network by rules that control connectivity (what can connect to what), and by specialized network ‘appliances’ that implement security functions such as firewalls, load balancers, application firewalls, data loss prevention, and intrusion detection and prevention.

This approach breaks with the introduction of a cloud fabric. To begin with, it is no longer obvious what is running on which server because virtual workloads can be positioned and relocated flexibly and dynamically as resource usage and performance dictates. Second, the virtualization software we have added gets in the way. For example, when the network is virtualized, the physical network no longer really understands the specifics of the traffic because each physical link multiplexes traffic from the many virtual endpoints, making a legacy-architecture physical network literally blind to many important details.

On the bright side, though, the distributed cloud platform that provides virtual resources for the applications is a powerful means of implementing innovative new security approaches if the security elements are also transformed into virtualized software designed to run at cloud scale (hundreds, or virtual thousands, of servers).

ABSTRACTION

The Power of Virtualization Software

An essential part of a cloud fabric is the virtualization software layers that we insert between the application workloads and the hardware on which they ultimately run. These layers serve to share the hardware resources between the workloads, to present the details of the ‘hardware’ in the way the workloads expect it, and to provide the logical isolation between the workloads as if they each had a private system.

What is more important (although probably less obvious) is that we can use the virtualization layer to provide virtual resources that are different from, and better than, the physical resources underneath. For example, a virtual server can be quickly created on demand, moved around the datacenter, cloned, and then discarded – none of which is possible with a physical server.
Similarly, a virtual network isn’t limited by the nasty details of networking – virtual network segments can span a complex network or even multiple networks. There can be as many different logical networks as we want – not just the 4,096 VLANs that modern physical network architecture supports. When it comes to security, virtualization software is ripe with opportunity. For example, we can keep all workload programs and data encrypted until it executes; we can transparently encrypt communication links to be compliant with regulations; and we can add instrumentation and analysis that didn’t exist in the physical resources.
VIRTUALIZED SECURITY INFRASTRUCTURE

Cloud infrastructure enables us to take advantage of the virtualization software layers to create virtual networks and add distributed security elements – traffic instrumentation and traffic control that have the potential to greatly improve security compared with what was possible in the physical world.

Let’s begin with instrumentation. In the modern world of slow and persistent attacks that begin with a ‘minor’ breach and then build on that initial compromise until valuable assets are reached, it is essential that we be able to ‘see’ the signs of the attack as they occur (e.g., communications with a remote control system; attempts to penetrate new systems from a compromised system). In the physical world, this observation was done most easily with traffic analysis at the gateway to the external network by looking, for example, for anomalous traffic (communication from an unexpected application or port to an unexpected or unknown external system). In a virtualized world, we can place our distributed instrumentation sensors (software) anywhere we want and dynamically observe traffic at any point, with whatever level of detail we need.

Network virtualization with the ability to create new networking abstractions enables us to define traffic-control rules and policies that are simpler and more precise, based on the explicit application needs (permitted communications) and known security risks (denied communications). It also enables us to articulate how these rules change in the case of the inevitable compromise of a workload or host, balancing the need to contain the workload with the need for continued business operations. In a virtualized datacenter, control policies can include new options such as moving a workload into a quarantine zone; constraining permitted communications to white-listed application behaviors; or introducing new detection and instrumentation sensors to further map the extent of the compromise.

An additional – and crucial – property of a distributed systems approach is the opportunity to instantiate and extend security-processing capabilities as required, and to insert them judiciously in response to the prevailing security threat context. For example, it affords the capability to introduce advanced enforcement capabilities to a micro-segmentation deployment (such as processing operations occurring at the application layer to improve visibility and efficacy), to conduct full deep-packet-inspection processing against a suspected subset of traffic, or to transparently insert deception-based controls.

The deployment flexibility of distributed software sensors and control agents is complemented by recent advances in big data that let us cost-effectively analyze the large volumes of instrumentation data that we can generate, together forming a remarkable tool for detecting the signs of an ongoing attack early on, when it can be stopped and mitigated. Collectively we now have tools (granular instrumentation, analysis, granular control) that are far better than ever before.
Cloud infrastructure and virtual networks also give us a powerful new security tool – the virtual network itself. With a virtual network (implemented in the virtualization layer, using the physical network as an underlay for data transport), we can control very precisely which application elements can communicate with each other by putting them on a logical private network and using the basic capabilities in the vSwitch to permit or deny specific communications.

THE CHALLENGES IN IMPLEMENTING VIRTUALIZED SECURITY

Virtual networking and virtual security can’t be effectively implemented by simply creating virtual software versions of the existing devices because the scale of cloud computing (hundreds of servers, thousands of virtual machines) is much greater than the design points of the existing products. In a virtualized cloud fabric, we want to deploy and manage thousands of distributed firewalls (one ‘in front’ of each workload), and it is unlikely that an existing design will scale to that.

Fortunately, the early pioneers of large-scale computing have already developed new system architectures that can be adapted. The goal is to keep the distributed functions as simple as possible, while being able to manage each individually and in groups, and to be able to collect and centralize the data generated, especially for instrumentation. There are good approaches that can be adapted, but they are quite different from older appliance designs where the appliances were deployed in much smaller volume. The architecture is the critical factor here. It can be adapted from an existing cloud-scale software architecture, or created by software architects familiar with such designs.
SUMMARY

- Modern IT demands new security architectures. Perimeter defenses simply don’t work.

- Cloud computing is very different technically, as separate application silos that are loosely interconnected are replaced by distributed, virtualized cloud fabric software.

- The abstractions that can be created with this virtualization layer can provide powerful tools for security. For example, a virtual network is not limited by the constraints of physical network configuration; with distributed fabric software, we can put security controls (e.g., block all but good traffic) exactly where we want them (e.g., in front of each workload.)

- We can add unprecedented dynamic traffic instrumentation, which is essential if we are to detect and mitigate slow and persistent attacks early on, before the damage is done.

- Modern big-data capabilities give us unprecedented analytic capability in terms of data-set size and analytic power – just what we need when we’re looking for the attack signal in the sea of datacenter instrumentation data that we can now gather.

- It is highly unlikely that existing device and appliance software can be adapted to run at this scale, and it’s more likely that effective solutions will require re-engineering the desired capabilities using ‘cloud-scale’ software architectures.