CLOUD-BASED SECURITY THREATS WITH PRESENT CHALLENGES AND OPPORTUNITIES FOR MANAGED SERVICE PROVIDERS (MSPs)

Bhaskar Kamal Baishya[1]

[1]*M.Tech CSE Student, Computer Science and Engineering, NERIST, Arunachal Pradesh, India*

Abstract

The increase in global Internet security threats means businesses now have to allocate a significant portion of their budget to protecting their users, monetary. assets, data, and intellectual property. Unfortunately, implementing traditional client/server endpoint security solutions often entails suffering unplanned downtime and performance issues. As a result, many Managed Service Providers (MSPs) have added endpoint management to their portfolio of services. This in turn delivers powerful security solutions that protect against even the most sophisticated online threats, without sacrificing system performance because they can be deployed with ease and are simple to manage. Backed by a unique, real-time threat detection architecture they provide scalable security that addresses historical challenges MSPs have faced quickly and efficiently, while helping generate new revenue streams and maintain margins full stop.

Keywords: *Managed Service Providers (MSPs), BYOD (Bring Your Own Device), Total Cost Of Ownership (TCO).*

----------***----------

1. INTRODUCTION

Cloud computing has fundamentally changed the way businesses and consumers use computers and technology and the way Information Technology (IT) professionals manage those resources. While the cloud has delivered a multitude of benefits to technical and non-technical people alike, there have also been significant downsides to reliance on cloud technology, including unplanned outages and even outright cyber-attacks and data theft. Though the cloud has become ubiquitous, there still remains considerable confusion as to how cloud computing can be used by managed service providers (MSPs) to enhance the security, privacy, and productivity of their customers. Below are several common scenarios in which cloud computing is helping MSPs to more efficiently and cost-effectively ensure greater endpoint (PC, laptop, smart phone, tablet, etc.) security for clients all over the world.

2. ADVANCES IN MSP SECURITY OPERATIONS & TOOLS

Companies across the industrial spectrum face significant new challenges. Years ago it was commonplace for MSPs to host their service delivery applications and technology in their own facilities or in co-location facilities. The software and tools, just then becoming cost effective, needed to be closely managed by the MSP in order to be effective. Thus MSPs frequently had to allocate employees specifically to monitor and manage the MSP-enabling technologies they utilized to deliver managed services to their customers—a costly and inefficient process. Today, we should thank to advances in cloud computing, software is not only lower in cost but also easier to manage and deploy using cloud based-architectures.

Many technology vendors are utilizing cloud-based Software as a Service (SaaS) platforms to provide greater availability, redundancy, and security than their MSP partners could ever have imagined. These advances are immediately translated into benefits not only for customers, but also the MSPs who must manage those customer endpoints. For example, before the advent of cloud-based security monitoring and management, MSPs historically had to acquire and implement a broad variety of tools to deliver comprehensive security monitoring and management to their clients. This hodgepodge of solutions, frequently sourced from different vendors, presented varying degrees of difficulty when it came to their functionality, manageability, and cost. What's more, MSPs found it particularly time consuming and expensive to administer this diverse collection of tools in order to provide clients with effective endpoint security. Fortunately, recent years have seen great advances in the types of technologies being offered by many companies.

Many companies had created security technologies that give MSPs powerful, flexible, and extremely efficient monitoring and management capabilities from a single source, rather than having to procure many different tools from different vendors. This ability to purchase integrated tools from a single vendor, all specifically built to be compatible and complementary, greatly simplifies an MSP's deployment and internal management of its monitoring systems—and gives MSPs an opportunity to significantly reduce their costs and boost their profitability. With these important advancements in MSP security tools and operations in mind,

it's instructive to consider some of the more common contemporary security threats that face MSPs and their customers and how these challenges can be more effectively addressed.

3. BYOD (BRING YOUR OWN DEVICE)

Perhaps no single phenomenon has been more disruptive (and potentially lucrative) to MSPs than the trend of customers bringing their own devices into corporate environments (otherwise known as Bring Your Own Device, or BYOD). BYOD started to become prevalent after Apple introduced its iOS mobile operating system. Soon corporate executives began to arrive at work with iPhones (and later, iPads), demanding that their IT department to "make it work" despite the fact that these devices were not officially sanctioned or managed by the IT department.

It wasn't long before mobile devices (and subsequently cloud environments, including applications) began to become more pervasive in the corporate network. While supporting the CEO's iPhone may have been feasible, it soon became clear that when all of the other employees began to expect similar accommodations for their mobile endpoint devices, IT professionals around the world needed to figure out an effective solution—and quickly. Of course, savvy MSPs also saw this as an excellent opportunity to offer additional revenue producing services to their clients. BYOD is now a common place end point security challenge to every company, with a variety of solutions being employed by IT departments and MSP organizations across the globe. The specific responses to this challenge vary depending on the sophistication and resources of the MSP, but there are some common threats and issues that every MSP should consider when evaluating BYOD solutions for its customers.

First and foremost, MSPs should discuss with their clients the need for a BYOD policy that is secure and reasonable for both parties. BYOD can offer companies significant benefits in the form of greater user productivity and satisfaction, but it also poses considerable threats for a corporate network environment if not properly addressed by the MSP. Some of the more common risks associated with ungoverned BYOD usage includes:

1) Data loss/theft.
2) Violation of corporate IT policies and procedures.
3) Introduction of foreign/unapproved cloud environments.
4) Mixing personal and corporate data on same device.
5) Creating policies that bypass device monitoring, management by MSP.

These risks are significant, particularly because seemingly innocent actions and decisions by end users can profoundly compromise corporate data security. To mitigate these risks, MSPs must introduce BYOD policies and solutions that are non-intrusive for end users while still providing robust protection from outside threats. Ideally, any BYOD protection solution that an MSP selects should utilize the same platform as the MSP's main endpoint security solution; this integrated approach ensures quicker, more familiar deployment and management tasks for MSP technicians, thus freeing their billable time for more lucrative duties. By combining reasonable BYOD policies and integrated BYOD solutions for their clients, MSPs can help ensure the security and productivity of their customers' IT environment—while adding another revenue producing client service that easily blends into their established endpoint security management workflow.

4. DATA PRIVACY AND SECURITY

Spurred by trends like BYOD, the importance of protecting data privacy and security has never been greater than it is today. Data security is no longer just an arcane IT concept reserved for large enterprises; it's now an issue that touches organizations of all sizes, as well as end users, around the world. Most worryingly, the risk of losing data privacy and security has grown as the value of that data has increased for cybercriminals. These perpetrators dedicate tremendous resources to creating viruses, malware, and other mechanisms for compromising networks, systems, and end user devices in order to gain access to sensitive (and profitable) data.

Characterized by an unprecedented volume, velocity, and variance of threats, today's global security environment demands that MSPs take decisive steps to protect customers from a new generation of aggressive cybercriminals intent on compromising data integrity and security. By leveraging cloud-based security tools, MSPs are in a far better position to protect customers from cyber threats than any company's internal IT department utilizing conventional security solutions. A multitude of client endpoints around the world can be protected by cloud-based security solutions, which are deployed, monitored and managed from one central web portal. This enables MSPs to deliver robust data security solutions to clients anywhere in the world, faster and at a lower net cost to the MSP than traditional server-based security solutions.

5. ENDPOINT MANAGEMENT

One of the most important models for protecting data and security involves securing client endpoints (such as desktop computers, laptops, smart phones and tablets), because such devices are frequently targeted by cybercriminals. Cloud-based endpoint management and protection provides MSPs with a highly efficient, cost-effective way to protect their customers from a variety of cyber-attacks.

The advantages of using a cloud-based endpoint security platform become readily apparent when users no longer have to suffer through time-consuming signature (also known as virus definition file) downloads and scans. These processes can place enormous CPU loads on the protected device, causing significant reductions in end-user productivity—and consequent increases in client frustration. The easier a security solution is for clients to use, the higher its adoption rate and user satisfaction will be.

Another critical advantage that cloud-based endpoint solutions offer is the MSPs ability to manage a multitude of customers with far fewer employees. Because the technology is hosted in the cloud, an MSP can devote less technician time to managing its endpoint security solution, and that is the single most important factor when determining a solution's total cost of ownership (TCO). Initial purchase price of such solutions is generally very similar, but the actual TCO of a web-based solution is often dramatically lower than that of traditional server-based solutions that demand far more (costly) attention from an MSP's technicians.

6. CYBER THREATS

The world of the Internet has become increasingly dangerous; not only are there more threats than ever, but they are also more difficult to identify and protect against, especially with more users surfing the web. As such, organizations (and the MSPs that serve them) need better methods for protecting and safeguarding corporate data than ever before.

MSPs who take advantage of modern cloud-based security (such as Web root Secure Anywhere® solutions) are far better able to protect their clients from this constantly-evolving environment of Internet-based threats and malware. Some of the most significant security benefits of this cloud-based technology include:

1) Prevents spyware & viruses commonly spread through Internet.
2) URL filtering to help end users ensure they reach correct destination (prevents routing users to sites designed to steal data or infect devices).
3) Prevents phishing & bad content that could compromise networks and sensitive data.
4) Prevents URL circumvention (stops user attempts to either access blocked pages or circumvent monitoring).

Cloud-based protection of cyber threats is an essential feature for MSPs to offer their clients, as the likelihood of data loss or malware infection continues to grow. Preventing infections not only benefits clients by ensuring uninterrupted operations and continued productivity, it also helps to solidify a client's confidence in their MSP, an important factor when an MSP seeks to maintain long-term, stable, and profitable relationships with its customers.

Managed service providers and IT administrators can use or an existing modern cloud-based security solution to create custom access policies for departments, groups and individuals, and to demonstrate compliance with acceptable-use policies. The built-in quota policy limits bandwidth consumption, time spent online and number of sites accessed.

7. MOBILE DEVICE MANAGEMENT

Mobile devices are a particular target of cyber criminals these days because many of these devices (smart phones and tablets, in particular) were initially aimed at the consumer market and thus don't have the same types of embedded security features as PCs and laptops, which are often designed to meet more stringent business computing requirements. The rise of BYOD makes this lack of security features even more troubling. Mobile device management, or MDM, is thus important not only to ensure unbroken end-user productivity, but also to protect the corporate data and networks those mobile devices access every day.

To help MSPs achieve these goals for their clients, cloud-based mobile security includes a comprehensive suite of management tools specifically designed for MDM. MSPs can leverage these technologies to remotely manage a wide variety of mobile devices, regardless of their design or operating system, and ensure that those devices comply with the requirements of their client's organization. Customers can rest assured that their users are being productive while still being secure in their usage of mobile devices, and MSPs boost efficiency and cut costs by employing a mobile solution that seamlessly integrates with their existing endpoint solution.

8. CONCLUSIONS

It is an unfortunate fact that with each passing day the Internet is becoming a more perilous place; threats are multiplying in both their complexity and ferocity, and MSPs must adapt in order to protect customers from these rapidly-escalating risks. By partnering with modern cloud-based security, MSPs can take advantage of innovative, cloud-based technologies that make it easy to deploy and manage a comprehensive suite of security solutions purpose-built to protect organizations and users from a variety of threats. Combining unrivalled power and unprecedented efficiency, modern cloud-based security solutions give MSPs the modern tools they need to ensure client security, build customer loyalty and dramatically reduce security solution management costs.

REFERENCES

[1]. Andreas Berl1, Erol Gelenbe, Marco di Girolamo, Giovanni Giuliani, Hermann de Meer1, Minh Quan Dang and Kostas Pentikousis,"Energy-Efficient Cloud Computing, "The Computer Journal, Vol. 53 No. 7, 2010.
[2]. Chipurupalli Sekhar, U. Nanaji, "Secure Cloud By It Auditing," International Journal Of Modern Engineering Research (IJMER) www.ijmer.com vol.1, Issue.2, pp-332-337 issn: 2249-6645.
[3]. Anthony Bisong & Sayed.M.Rahman, "An Overview Of The Security Concerns In Enterprise Cloud Computing," IJNSA, Vol.3,No.1, Jan 2011.
[4]. Amazon EC2 and S3, online at http://aws.amazon.com/
[5]. Google App Engine at http://code.google.com/appengine/

[6]. Website references, www.wikipedia.com, www.saleforce.com, www.ibm.com,www.sun.com.

BIOGRAPHIES

Bhaskar Kamal Baishya received his B.Tech Degree in Computer Science and Engineering from, Assam Don Bosco University, Assam. Now he is an M.Tech final year student in the Department of Computer Science and Engineering, North Eastern Regional Institute of science and Technology, Nirjuli, Arunachal Pradesh. His research interest includes Embedded Systems and Cloud Computing.