Cyber Security Crisis Reality -vs- Myth

By Dr Venkat Rayapati

Introduction

Anchored by 25 years of cyber security expertise, Dr. Rayapati addresses the critical value and scale from the adoption of a cloud security solution which is contrasted by the glaring deficiencies of current security offerings in the marketplace. He shares visibility to the future requirements of security including the ever expanding need to address an increasingly complicated threat matrix. This paper discusses how a CISS (Cyber Intelligent Secure Software) solution will provide all the benefits of scalable cloud security resulting in a highly protected network

Overview

Imagine you are the IT manager for a bank, city government, or other critical services business. The CSO frantically contacts you telling you that the network is down and as head of IT he wants to know when it will be fully operational and WHY THIS HAPPENED! Your top priority will be to get the network fully operational as soon as possible, but then equally important is finding out why it went down. You need to prevent that from happening again and receiving another call from the CSO.

- Today we are going through a significant transformation, no industry is safe or secure from being attacked. Traditionally, finance institutions were the main target for hackers. Today, the big four banks in the US are spending in excess of $1.5 billion on cyber security.
- Sony Entertainment in October 2015 was attacked for ransom for their movie the “Interview”. Sony Entertainment paid $8 million to the attackers for ransom.
- In addition to the above, in 2015, the “Year of The Healthcare Attacks”, a total of 105 thousand records were compromised and held for ransom. In 2016, in healthcare alone a total of $6.2 billion was lost due to ransom and lawsuits.
- The $81 million bank heist of the Central Bank of Bangladesh is one of the most successful cyber bank thefts in history. The bank was attacked via SWIFT, a well-known and utilized international bank messaging system. In January 2016 Europe’s largest financial lender HSBC suffered a DDoS attack, keeping several banking customers unable to access their accounts. A new threat called GozNym malware has been identified targeting banks in the North America, Asia, and Europe.
  Threat and security are symbiotic; one would not survive without the other. As threats become more widespread, increasingly sophisticated, and overly complex, the corporate security strategy becomes more challenged trying to keep up.

“Companies spend millions of dollars on firewalls, encryption and secure access devices, and it’s money wasted; none of these measures address the weakest link in the security chain.”

Kevin Mitnick Famous Hacker

Challenges – Multiple Vendors

While it's clear that stacking appliances on top of each other may not be effective in addressing security challenges, blended threats cannot be tackled by just one security solution. According to IDC, perpetrators of malware and ransomware have become more focused- gunning for quick and huge financial gains. They have become more adept at tapping into an arsenal of attack measures to get into your network. By deploying what you are led to believe are overall solutions, you are in effect opening up the door for smart hackers to sidestep the rules you set in place, having thought that another appliance has it covered.

The Myth of Stacking Appliances

The work that needs to be undertaken to cover the above threats means that stacking five to ten appliances on top of each other delivers operational challenges and could be a potential bottleneck as well as unwittingly leaving holes in your defense.

Multiple solutions are typically developed and managed by different vendors, which can pose a challenge when it comes to interoperability. For these single end-point solutions to be effective, every solution needs to be fine-tuned by an expert and monitored within multiple threat vectors. Often, these threat vectors are duplicated for different solutions, leading to redundancies, confusion, and ultimately holes in the security infrastructure. Additionally, these solutions are designed and intended as a point solutions, and not to integrate or work with other security products.

Cloud Evolution

The evolution of cloud computing has many benefits from a scalability, flexibility and cost perspective. The business owner sees the productivity gains but has only one eye on security over profit. Threats today emerge quickly as we are at a point where significant change is happening in the way we compute, collaborate, store and retrieve data. What was once within the “safeguard” of network, is now moving rapidly outside the perimeter to the Cloud.

In addition, emerging cloud based hosting requirements means firewalls have to adapt the current security policies to both application and users in a more granular way, which is not considered before. With the advent of the cloud, corporations are challenged with understanding how to migrate their data to be more accessible, flexible, and manageable, yet still protect their most critical assets: employees, data, revenue, and reputation.

Cloud Scale

As internal and external threats continue to evolve in the organizations, it's even more important to know who is accessing files and receiving malicious spam and ultimately who is posing a threat to your network security and corporate data within the cloud.

Traditional ways of looking at firewalls limit an organization's ability to meet the fight for security brought on by the movement of applications to the cloud. Cloud computing adds to this complexity in application access and control.

By blurring the hitherto clear distinction between internal applications hosted within organizations' data centers and external applications available over the Internet, the challenge of managing application access and control becomes far more complex and risky as hardware centric UTM’s struggle to address security for cloud computing resources

Cloud Security Challenges

At the beginning of this paper I stated that “Threat and security co-exist one would not survive without the other”. No area highlights this more perfectly than cloud and non-corporate device usage to gain access to applications in the cloud. Often, the needs of the business come first as gains made by using the virtual environments outweigh security considerations. The challenges posed by cloud and virtualization have created problems for organizations to balance, productivity with security.

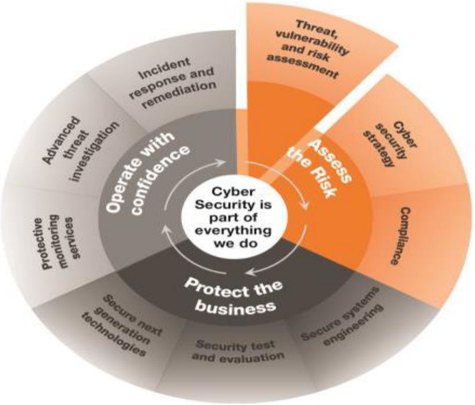
- Emerging cloud based hosting requirements mean that firewalls have to adapt to apply QoS by both application and users in a granular way that is beyond the current usage policies.
- Enter cloud computing - today we stand at a point where significant change is happening in the way we compute, collaborate, transfer, store and retrieve data. What was once within the network, is now moving rapidly outside the perimeter or our control.
- Cloud services has gained increasing mainstream acceptance. Cloud increases this outward application mobility multi-fold with most or all internal applications set to move outside the perimeter. This phenomenon critically impacts bandwidth consumption and cyber risk of any organization.

Organizations will struggle to manage and protect the need for the three categories of applications:

- Mission Critical Applications
- Business Critical Applications
- Social Media Applications

Introducing Cyber Forza-CISS

CISS (Cyber Intelligent Security Software) was designed to address, in a comprehensive way, the multi-faceted needs of security for an organization. For any organization security falls into five categories:


Threat, vulnerability and risk assessment
Cyber security strategy
Compliance
Secure systems engineering
Security test and evaluation
Secure next generation technologies
Protective monitoring services
Advanced threat investigation
Incident response and remediation
Assess the Risk
Protect the business
Operate with confidence
Cyber Security is part of everything we do

- Privilege Security
- Application Security
- User and Device Security
- Network Security
- Physical Security

As with any inflection point a new perspective is needed to address the migration of On Premise or Cloud access and connectivity using a myriad of devices. At the forefront of this must be network, application, user and device security. The approach taken not only needs to address today challenges of multiple simultaneous attacks vectors but must also have artificial intelligence to address the needs for tomorrow and beyond.

By integrating Artificial Intelligence and behavioral analytics, CISS provides an advanced threat protection solution comprising of multiple intelligent threat vectors that operates seamlessly to address the security needs for On Premise, Virtual and Cloud environments:

"It is up to senior business leaders to take the lead in protecting their organizations."

-Stuart Madnick, Director, MIT's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity

Cyber Forza-CISS Protects What You Can't

Current hardware only solutions available from single point UTM solutions, do not scale or sufficiently protect against cloud initiated cyber threats.

Protection	Features
✓ Ransomware	✓ Robust Forza OS
✓ DDoS attacks	✓ Response & Action
✓ Malware	✓ Numerous Reporting
✓ Spam	✓ Tasks and Workflow
✓ Networks attacks	✓ Customized Rules
✓ VPN Attacks	✓ Active Directory
✓ Email	✓ Detection & Prevention
✓ Gateway	✓ Groups/Departments/ Users
✓ URL & Web filtering	✓ Artificial Intelligence
✓ IDS/IPS	✓ API's
✓ Firewall	✓ Permission & Rights
✓ SSL	
✓ All Types of Viruses	

Cyber Forza- Cyber Intelligent Security Software (CISS) is a software solution with a robust Forza OS integrated with AI, which is highly scalable, flexible, and cost effective to protect cyber attacks.

CISS can be deployed On Premise, virtualized, and cloud environments.

"Lockheed Martin uses Cyber Forza to protect its core infrastructure."
Head of Security ISDG, Angie Heise

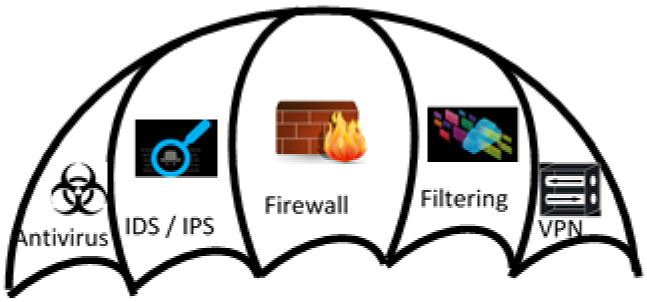
To secure data in multi tenanted public cloud environments where often chaos reigns when threats surface. Organization need to think from a holistic approach to manage cyber security with workflow management, and integration with other departments. Hackers today are using multiple threat vectors and techniques to gain access to any public or private cloud network to ransom. A new holistic approach that has an integrated intelligent multifaceted defense mechanism addressing the security need beyond perimeter network protection is required. This new approach must be able to address the current challenges. Artificial Intelligence (AI) integrated with Cyber Security solutions to protect against behavioral attacks, such as advanced malware and ransomware.

Conclusion

In today's **threat landscape,** cyber attacks are a given. Hackers are targeting your corporations**,** their attacks are more sophisticated, and how you respond to a growing deluge of incidents has never been more critical. Avoiding key strategic and technical mistakes can mean the difference between successfully fending of attacks or becoming the next Headline.

It is not a question of if your organization will be attacked but when?

For cyber attacks, organizations need an effective process of identifying, detecting, and preventing before they cause major damage, to respond in a timely and accurate manner.



Cyber Forza-CISS streamlines the efficiencies on how you protect your entire IT infrastructure and breaks away from the traditional multi-silo solutions.

Cyber Forza-CISS gives you an entire solution under one umbrella with the flexibility to incorporate it in your existing security policies and protect your entire organization with just one application.

Cyber Forza can help your organizations to identify, detect, prevent cyber internal and external threats by providing solutions for Healthcare, Financial, Public safety, Educational, and Retail markets.