How Do You Secure an Environment Without a Perimeter? Using Emerging Technology Processes to Support Information Security Efforts in an Agile Data Center

Charla Griffy-Brown
Pepperdine University

Demetrios Lazarikos
Blue Lava Consulting

Mark Chun
Pepperdine University

Cloud computing has transformed businesses, enabling agile and cost-effective IT infrastructure. The critical problem is that these new opportunities resulted in a co-mingled architecture which is difficult to secure. Based on interviews with boards of directors and executive leadership teams facing these new environments, our research question was: How do we secure increasingly dynamic architecture in an environment without a perimeter? The research involved an in-depth exploration of this problem using a survey instrument and interviews with 204 executives from 80 companies throughout 2014. From this work we developed an information security framework for executives in this new environment.

INTRODUCTION

Cloud computing is an IT enterprise architecture that continues to gain broader adoption throughout the networked world. In legacy architecture solutions, the IT services are under proper physical, logical and personnel controls. Cloud computing moves the application software and databases to large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges. The critical problem is that these new opportunities to align with business leveraging cloud computing resulted in a co-mingled architecture of legacy, cloud and virtualized systems. With more businesses facing these new environments, our research question was: How do we secure increasingly dynamic architecture in an environment without a perimeter amidst increasingly coordinated and sophisticated threats? From this research the following two questions also arose and were addressed: Are there demonstrable solutions which fill this provisioning gap? What generalizable lessons and processes can we derive from examining these solutions? The research involved an in-depth exploration of this problem based on interviews with 204 executives from 80 companies throughout 2014. Based on this qualitative research design and survey data, we will describe an information security framework that was developed to help executives understand their positioning in terms of emerging threats as well as how this security provisioning gap can be significantly reduced. The

framework, architectural analysis and proposed solutions resulting from this study allows organizations to dynamically provision scalable security solutions along with their compute, network, and storage workloads. In an environment without a perimeter, this research offers insight by methodically identifying and characterizing the main problems companies are facing in this context as well as providing a practical framework and tools for making better security decisions. This paper proposes a different way of thinking about security with the growth of agile data architecture.

The cloud-security literature research primarily focuses on requirements and solutions for requirements (Honer, 2013). In this regard, research on Attack/Harm Detection is prolific (Chonka, et.al, 2012; Chonka, et. al., 2011; Monfared, et. al, 2011). Non-repudiation is widely discussed and cited (Nishikawa, et. al., 2012; Kumar., et. al., 2011; Chou, 2011) and Security Auditing has been deeply explored (Deshmukh, et. al., 2012; Gul, et. al., 2011; Munoz, et.al, 2012). By far the most researched topics are privacy, confidentiality, access and control (Chen, et. al., 2013; Cho, et al., 2012; Llanchezhian, et. al, 2012; Elham, et. al., 2012; Zhu, et. al., 2012). In his extensive literature review of the information security scholarship over the last decade, Honer (2013) identifies these areas as the topics most scholars are examining. However, in the applied business world, these issues are never dealt with in isolation and there is a need for broader thinking given the new agile architecture more companies are using.

Furthermore, solutions to the requirements studied in the literature range from authentication and authorization protocols, the use of Private Key Infrastructure, VM isolation, encryption and auditing schemes and processes (Popovi and Hocenski, 2010; Tran, et. al., 2011; Wang, et. al., 2013). Studies tend to isolate factors and analyze a mixture of sub-factors which provide valuable insight but have significant practical limits when it comes to scaling and organizational decision-making. In fact, current theory as indicated in the literature above, assumes there is a perimeter and therefore the need for dynamic scalability is not required. This research through the research questions and case methodology explores a systematic applied approach to scaling, particularly a mixed legacy, virtual and third party eco-system. These mixed eco-systems lack a perimeter and are dynamic. This research fills a much needed gap in providing a framework for exploring and securing this new environment.

The high-level security framework used for this study was developed and validated with Fortune 500 companies and is referred to as the Information Security Maturity Model (Figure 1).

FIGURE 1
THE INFORMATION SECURITY MATURITY MODEL

This model explains that over time companies can move from a reactive state in information security to a proactive state with respect to information security. The first column, called "Blocking and Tackling" refers to a completely reactive environment characterized by a lack of support, underfunding, lack of staff and lack of metrics for understanding what is happening in the IT environment with respect to information security. In this column, companies are typically just reacting after criminal behavior has occurred, often without early detection. The next column, called "Compliance Driven" refers to a corporate environment in which a control-based approach is taken but this is driven by audit and regulation rather than positioning for emerging threats. The final column called "the Risk Based Approach" refers to companies which are using big data and behavioral analytics to understand and position themselves for potential threats. In this approach, businesses have a risk framework in place, widespread automation is in place and they are linking events across disciplines using dynamic controls, metrics and processes aligned with business.

This research first will identify where the companies examined fit within this framework and then focus on identifying and characterizing the critical architectural issues faced by these companies. This is where the co-mingled architecture becomes a clear phenomenon as does the loss of the perimeter. Based on these results, solutions will be identified and critical considerations moving forward presented in order to advance our understanding and ability to deal with the dynamically changing information security challenges.

The structure of this paper develops the logic above. The next section will explain methodology used to seek answers to the research questions articulated. Following this, the companies examined will be characterized according to the information security maturity model and their common architecture problems characterized. The final section will explain solutions for executives and IT practitioners and expands the meaning of this research in terms of transferability. Based on this analysis, companies can similarly use the security framework presented as a tool for advancing further real-world solutions to these dynamic challenges.

METHODOLOGY

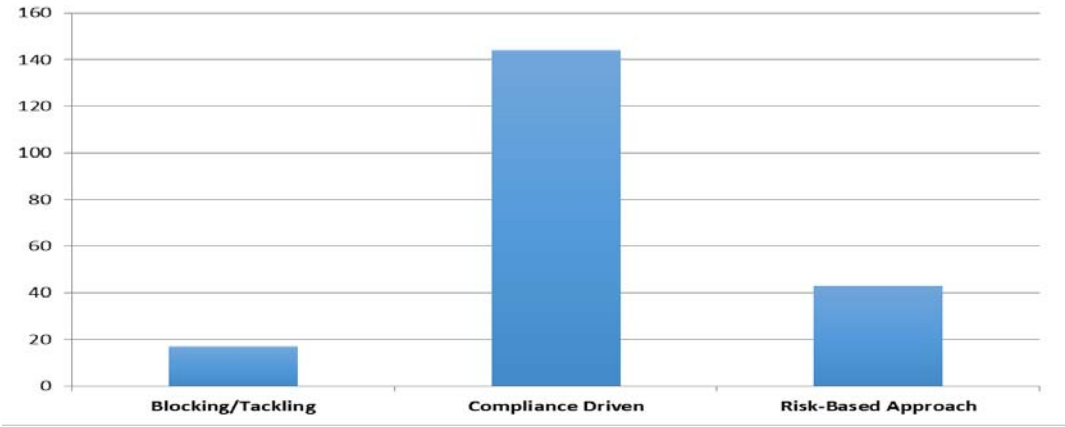
The data collection strategy used in this investigation is known as triangulation, involving multiple methods for collecting historical and longitudinal data (Yin, 1994; Strauss and Corbin, 2015). Multiple sources of data (e.g. participant observation, open / structured interviews, etc.) were collected through structured and semi-structured interviews with 204 executives at 80 Fortune 500 companies from January 1, 2014 to November 1, 2014. The interviews helped this research to gain an understanding of the executive's perception, to identify the key common problems, and to understand how to address these problems through dynamic and agile solutions. Coding included highlighting issues that appeared more than 8 times in the interviews as part of the construct and to develop the framework for analysis as well as the recommended solutions. The executives also were surveyed to validate and gauge their perception of their organization within the information security maturity framework. The names of organizations have been kept confidential and anonymized in the reporting of the results, particularly given the sensitivity of the information security area. Finally, an architectural analysis was performed for the organizations to further characterize and identify the common problems.

RESULTS

Out of the 204 individuals polled (Figure 2) executives validated this framework and even identified where their organization fit into the model. In this self-reported categorization, 17 identified themselves in the Block and Tackle category, 144 in the Compliance Driven category and 43 in the Risk-Based Approach. Interestingly, the interviews revealed that the "Compliance Driven" groups all reported they were moving toward a "Risk Based" approach but would use audit or tie it to regulation to build things they needed in order to get there. This indicated that one primary impediment was the CFO and other leadership understanding the importance of this approach for strategic development of the business. The

use of audit and regulation occurred when the IT and Information security groups needed funding for special projects in order to achieve business alignment. The most heavily used regulations were typically those just coming out at the time of this investigation such as Payment Card Industry (PCI) 3.0 and guidelines by the Federal Financial Institutions Examination Council (FFIEC) in terms of managing virtualization.

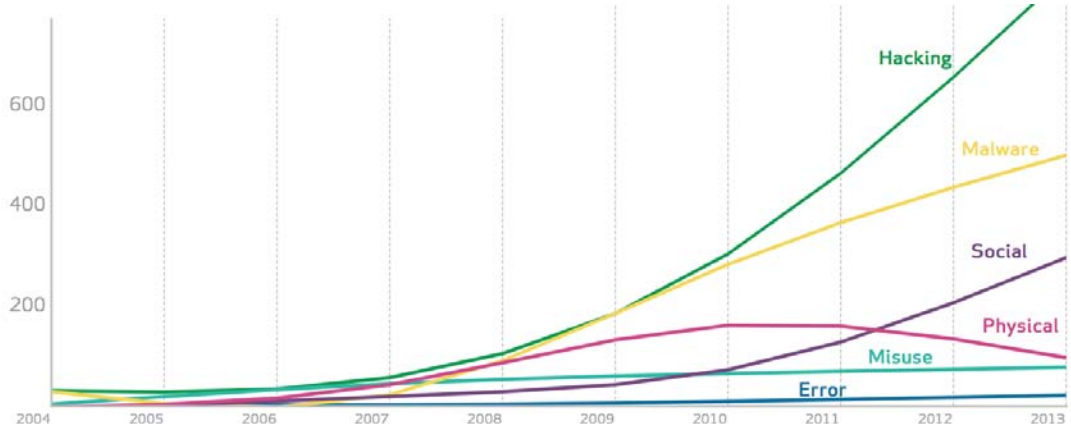
FIGURE 2
FIRM'S APPROACH TO SECURITY BASED ON THE INFORMATION SECURITY MATURITY MODEL



In addition, the tracking of threats and the threat landscape was a critical component of managing evolution in this framework. Most executives were "choosing their battles" given limited resources. The Verizon 2014 Data Breach report (Figure 3) was often cited to identify these "battles". This report shows that in the past few years, threats and breaches have become far more sophisticated. The malware and social media attacks were clearly on an up-tick and part of the dynamic environment most companies were developing. Importantly, cyber criminals were bypassing traditional security systems, so executives continued to mention the feeling that "the perimeter is gone" so they have to not only protect their internet facing applications in front of their clients but also have to protect their infrastructure. This was used as a basis for beginning to diagram the legacy versus current infrastructure to characterize what this means. What emerged was a clear identification, amongst the organizations interviewed, of a co-mingled architecture. In addition, what was clearly discovered was that in modern day attacks the security solutions of yesterday will not address the new attacks of cybercriminals of today. So from these conversations three issues clearly emerged across those interviewed:

a. Threats from all directions were increasing
b. Traditional security tools were being bypassed by cybercriminals
c. Threats were increasingly coordinated across different vectors

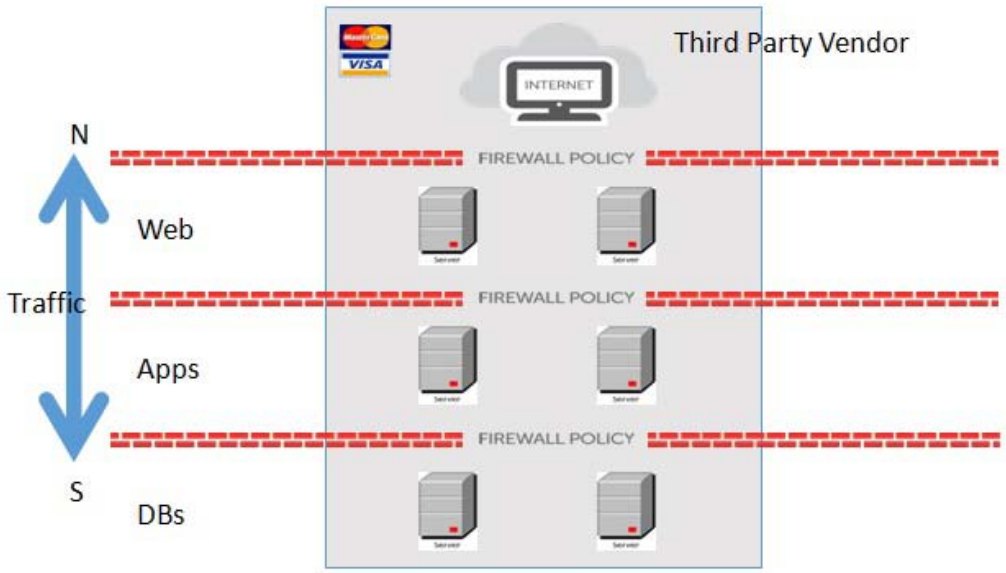
FIGURE 3
INCREASING SOPHISTICATION OF BREACHES



Source: Verizon 2014 Data Breach Investigation Report

Consequently, executives were asking how can I protect the brand, reputation and assets of an organization in this dynamic environment? How do I stay on top of the emerging threat landscape? How do I put in place controls, processes, some types of automation to scale and meet the business requirements? Importantly, as seen in the Mandiant report (Mandiant, 2014), the median number of days that attackers were on the system before detection was 229 days. While this was down 6% from last year according to this report, this not only validates the "loss of a perimeter" but also demonstrates the bypass of traditional tools, the high level coordination of attacks and the need for the Risk-Based Approach in the Information Security Maturity model. The problem that continued to bubble up was: "How do we secure increasingly dynamic architecture in an environment without a perimeter amidst increasingly coordinated and sophisticated threats?"

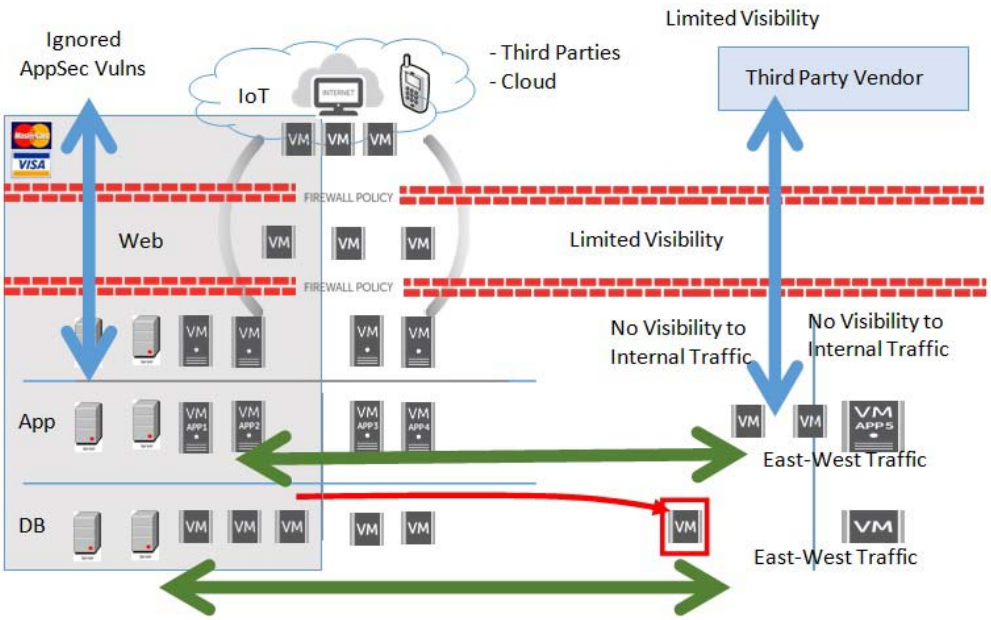
FIGURE 4
HISTORICAL ARCHITECTURE DATA



In order to further elucidate and characterize this problem (subsequently providing potential solutions) we need to look specifically at the architecture. Figure 4 shows historically how systems were built in a legacy environment. They were built in a controlled and relatively "siloed" way in which it was easy to put up a firewall and then open up to the internet as business needs expanded. In aligning with business, IT had to figure out ways to expose the system more externally and in this construct auditors would come in, look at General Computing Controls and define a scope of action to ensure compliance (whether it was new PCI requirements, HIPPA , GLBA, or EU). One of the things happening with this historically is that IT had complete visibility in terms of traffic. The company could see what was going in and going out as it was all filtered through their domain and flowed through internet structure supporting that as indicated in Figure 4. This meant that north – south traffic was transparent and the business problem was: how do we move faster to connect with more strategic opportunities?

However, in present architecture, companies have responded to strategic opportunities for business growth leveraging emerging technologies leading to the evolution of the agile data center. This was referred to by those interviewed as an "IT audit nightmare" or "A hot mess". In this architectural environment we started to see cloud technologies emerge in response to business requirements so virtualization increased as did connections with business partners and third parties (Figure 5). In other words, the security problem was traffic visibility as third party and business partners provide zero traffic visibility across their infrastructure. The security problem is that now companies have a legacy environment co-mingled with a virtualized environment and this problem is compounded with mergers and acquisitions. Aligned with executive perception, the perimeter has effectively disappeared.

FIGURE 5
EVOLUTION OF AGILE DATA CENTER



This began, from an architecture standpoint, as companies started to build all types of new solutions on top of each other to meet rapidly changing business needs. From a security perspective this means that an external auditor comes in and says, "We think this is in scope this year" and yet the scope changes dynamically to areas which are outside corporate control and the question of "scope," therefore, changes. So now, companies have a virtualized environment co-mingled with a new environment and multiple internet facing applications which we know are going to meet significant threats. The problem is now not only managing north-south traffic but managing east-west traffic as well. This is an enormous problem

because, companies do not have visibility into east-west traffic. The internet applications and supporting pieces for this are decoupled so visibility is completely lost. As a result, threats can remain undetected for 229 days as mentioned earlier. To compound this problem it is estimated that east-west traffic will increase by 80% by 2016 (Mandiant, 2014).

With this architectural evolution, the challenge is having certain groups trying to address a business requirement leveraging a third party vendor that needs to access the internal environment in which we now have multiple virtual machines. There is no visibility into these third party internet facing application or often even an articulated understanding of the security controls in place because all they show is compliance, not controls. Therefore, this opens up the entire environment to eco-system breaches across the system. Often times this reality results in an IT auditor saying, "third party vendors is now in scope". Therefore, companies have to figure out how to coordinate and work together to arrive at solutions. So firms need a way to put together processes and tools for coordination and align to business to support hyper growth of emerging technologies and agile environments. Companies have to effectively secure an environment without a perimeter.

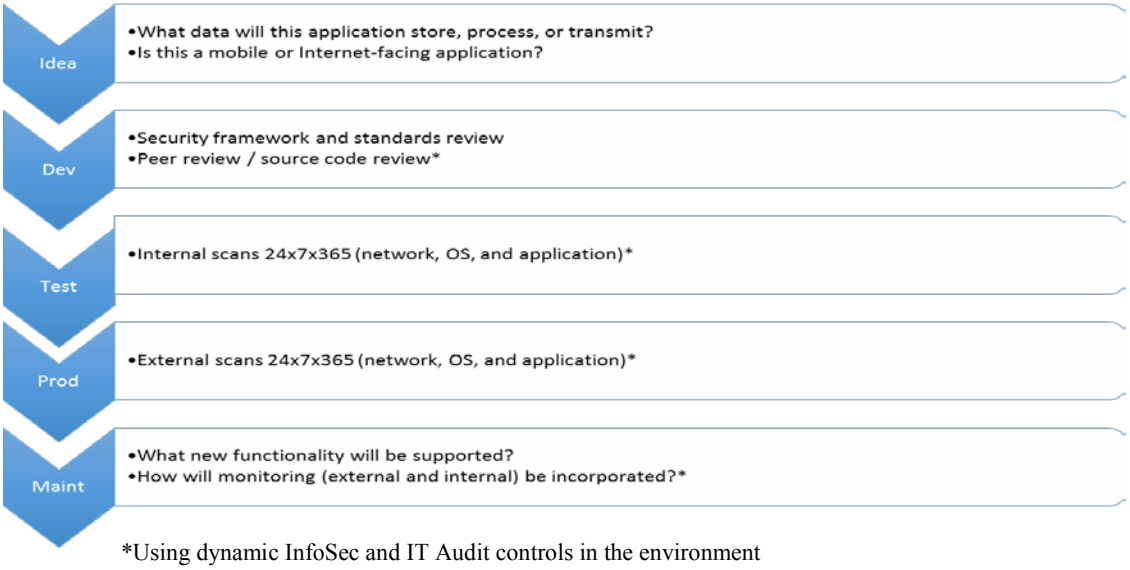
SOLUTIONS

Now that the architectural problem has been identified and characterized, what are organizations doing and how can they address this challenge? Firstly, executives indicated they were having much more frequent meetings with IT audit and IT security to approve budgets more quickly. In addition, there were several approaches that consistently arose:

- Agile Environment Development
- Big Data User Behavioral Analytics
- Automation
- Evaluation of Cyberliability Insurance

Organizations were still moving forward and embracing emerging technologies but these were the methods used to achieve a more risk-based approach given these dynamic environments. The Cyberliability insurance is beyond the scope of this investigation but we will explore the first three and within these methods discuss concrete tools.

FIGURE 6
ALIGNING SECURITY WITH BUSINESS AND PROJECT MANAGEMENT



*Using dynamic InfoSec and IT Audit controls in the environment

Firstly, organizations are aligning information security with IT audit and the Project Management Organizations as part of agile environment development practice. In this regard they developed more streamline checklists to assist in development and build-out. Figure 6 shows an example. As you move through the development process there are exit criteria involved and these are aligned with risk. In using this method it is critical to understand how to automate this to make it the least intrusive to a developer or auditor. Importantly, it provides an opportunity to educate developers on security and helps developers understand how to build security into any type of development. The critical point is constantly asking, "Is the PMO aligned with security requirements?

Secondly, in term of big data and behavioral analytics it is essential to have the ability to scan internal and external applications 24/7 365 days a year. Again this is a monitoring and an educational tool. In this regard, dashboards, risk frameworks and prioritizing remediation were critical. This became part of the risk-based approach in recognition of the fact that cybercriminals test corporate environments for a while as indicated by the Mediant Report (2014) which mentioned an average of 229 days. In addition, decision-makers in an agile environment need constant evidential matter to "bubble things up" for reporting. Figure 7 provides threat landscape models. Given that IT must align to the business requirements there is a need to know what the threat vector is, create a problem statement for that vector, identify the tools that need to be implemented and show the observations, risks and gaps. Figure 7 provides a tool for doing this. This also identifies specific tools that will help with the automation and analytics. For example, the first quadrant identifies Whitehat for scanning. The second identifies tools such as V-armour in response to PCI 3.0 compliance with a virtualization component. Using this checklist, items are listed out in terms of priority vectors of concern. This enables executives to tie innovation to risk and make informed decisions regarding datacenter and internet application protection in a dynamic and agile environment as businesses build out a "system of systems". This also allows executives to go after the budget they need for success.

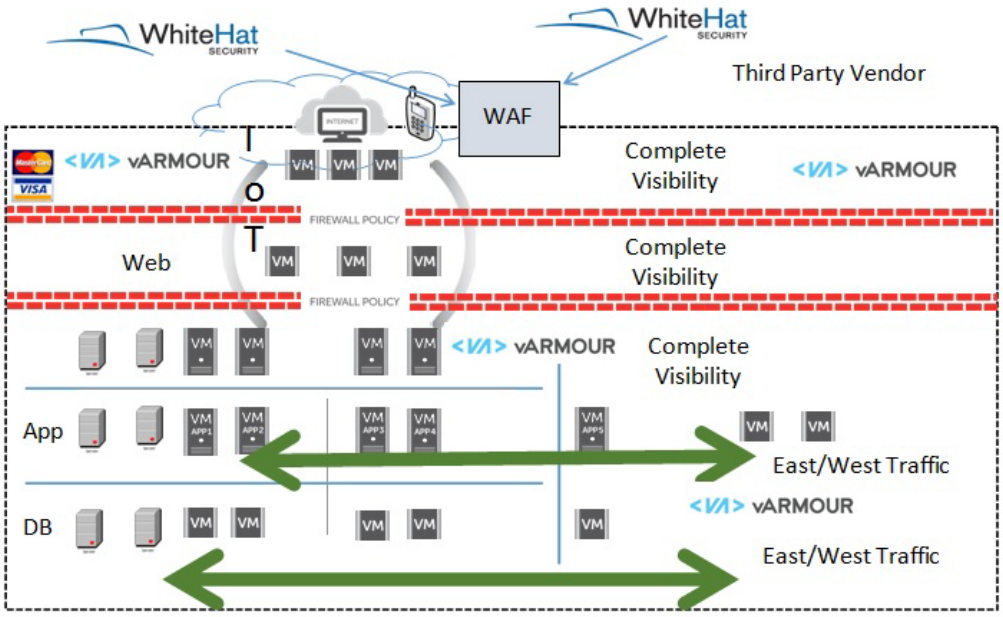
Finally, this ties to the "IT audit nightmare" or dynamic infrastructure with east-west traffic. For example, one way to do this is using the WhiteHat Application Program Interface (API) feed (identified in quadrant 1 of Figure 7) embedded into the web application firewall which enables scanning that can also then tie into a ticketing system – that way there is a source of record in-house in this integrated environment enabling behavioral analytics. We know cybercriminals will break into system but this is the "first line of defense". In addition, with V-armour integrated into the system if a 3rd party vendor has a breach then V-armour-gives you the ability to look at east west traffic under one fabric. Now Information security can start sifting through the data faster!!! As we are looking at data sets and building reporting off of the frameworks presented we are going to find different behaviors emerging. Figure 8 describes the architecture incorporating the new tools and processes.

FIGURE 1
STREAMLINED CHECKLIST FOR BUILD-OUT

Threat Vector	Problem Statement	Tools Implemented	Current Observations, Risks, and Gaps
Application Security	**Web application vulnerabilities lead to significant issues when P1s aren't resolved with current SLAs.**	• Training for developers (internal and third parties) • External and internal scans 24x7x365 (WhiteHat) • Penetration testing (3rd party quarterly tests) • Source code analysis (WhiteHat SCA) • Behavior analytics (RSA and Shape Security) • WAF (Integrate with WhiteHat rules)	• **There is 14% attrition with the developers.** • P1 appsec vulns are increasing by 12% a week. • **Integrate WhiteHat vulns with the WAF for automation.**

Network/OS/ Systems	**PCI 3.0 states that virtualized environments are in scope.** The company needs to meet agile business requirements. The company needs to detect laterally moving traffic between the data centers, zones, supporting networks, and cloud integration.	• Elasticity and agility to spin up/down environments (vArmour) • Network and OS scanner (Nessus) • PCI 3.0 management of physical and virtualized environments (vArmour) • File integrity monitoring (OSSEC agents) • Monitoring internal (east/west) malicious traffic (vArmour)	• PCI 3.0 states that all virtualized environments that store, process, and transmit cardholder data are in scope. • **vArmour allows you to manage both physical and virtual PCI environments under one policy and one enterprise software solution.** • OSSEC agents are not being used and configured properly.
Innovation	Automobiles Bitcoin Cloud (third party integration) IoT (eg. Wearables, Appliances, HVAC, Garage Doors) Virtualization	• Partner with manufacturers – insert InfoSec legal requirements into contract agreements • Application scanning 24x7x365 (WhiteHat) • Cloud integration (vArmour) • IoT (WhiteHat and vArmour) • Physical and virtualized management (vArmour)	• **System of systems* will be in scope for PCI, HIPAA, GLBA, PII, Privacy, EU Data Protection.**
Emerging Threats (Internal)	The company needs a ways to identify, monitor, and combat emerging threats once cyber criminals break the perimeter.	• Monitoring 'east / west traffic' (vArmour)	• **Internal traffic anomalies are increasing by 15% per month. Anomalous traffic patterns are moving between Zone X and Y and four data centers at 2:21am daily.**
External Mobile Security Applications	Mobile device usage is increasing by 54% year over year. **15 mobile applications are being developed by external teams** that are out of corporate compliance and do not meet mandatory industry regulations.	• Behavior analytics software (RSA) • Monitoring mobile app stores (Risk I/Q) • WhiteHat source code analysis (SCA) • Cyber threat research (FOX-IT)	• Mobile source code being developed by third party organizations is not compliant with corporate InfoSec policies and industry regulations.
Mobile Security (Internal/ BYOD)	The company needs to support the BYOD policy.	• Access controls (LDAP/AD) • MDM (Good Technology)	• Need to determine how the MDM solution will scale over the next 12 months.

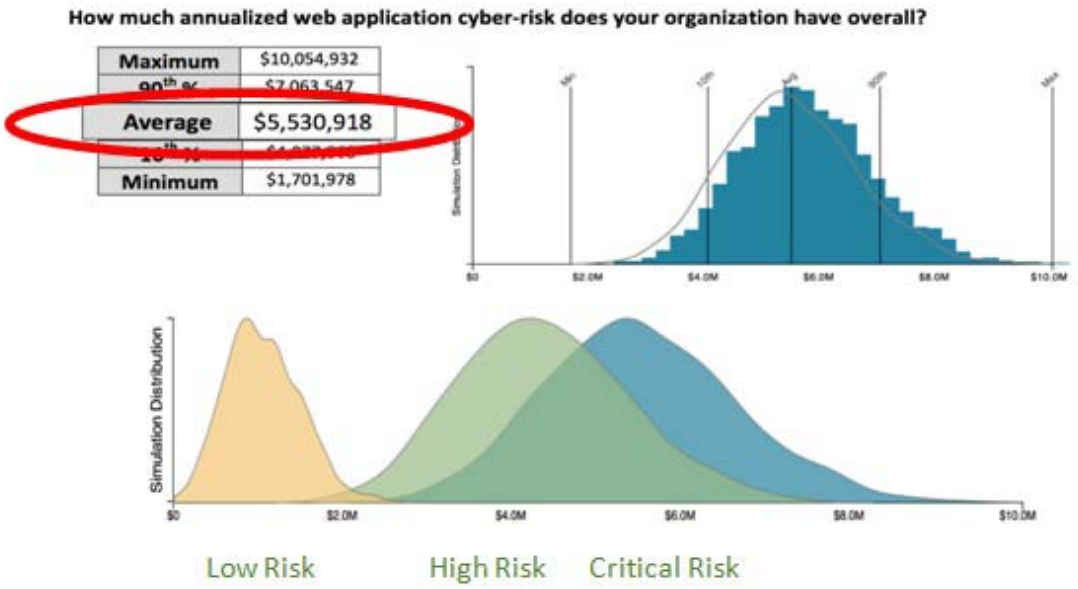
FIGURE 8
ARCHITECTURE, PROCESSES AND TOOLS TO ADDRESS CHALLENGES OF PROTECTING AN AGILE DATA CENTER



This provides new dynamic opportunities for datacenter protection. Companies could develop behavior scores and event frequency information. The data from Whitehat (API Feed) can then show if an attack is a script kiddie or a cybercriminal hitting at 400 thousand clicks per second. This enables security to more quickly identify types of threats particularly give data that can now be provided on velocity, even from east-west traffic.

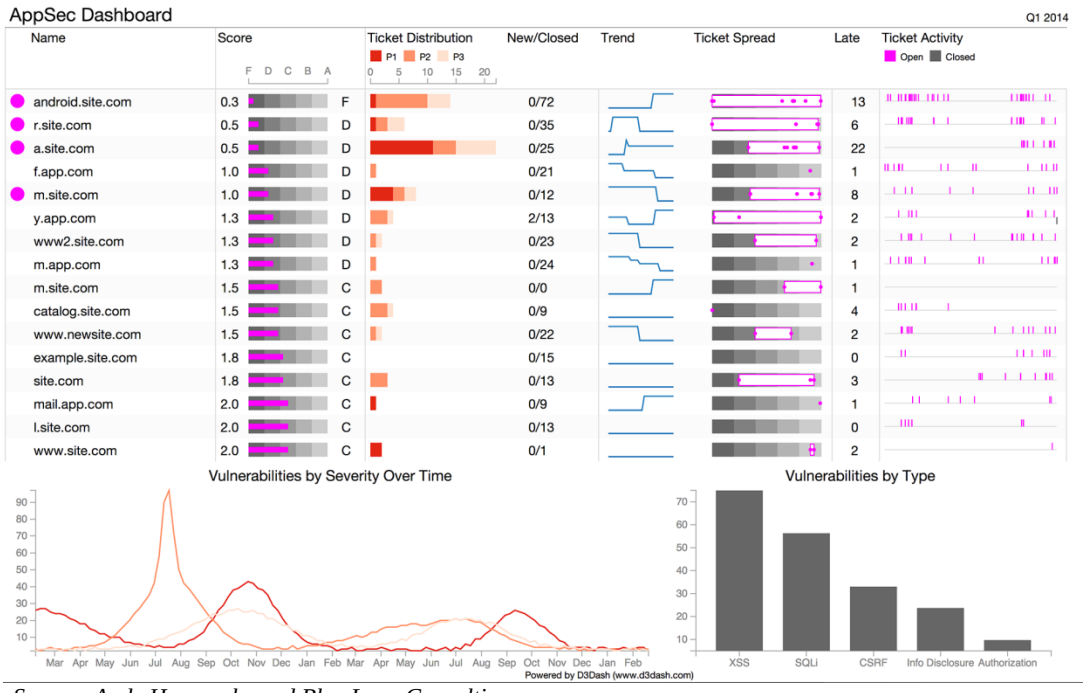
Importantly, as we look at data analysis we need to think about how to combine events. Cybercriminals are not doing one attack but typically are engaged in a combined effort. As a practitioner, security doesn't want to be inundated with alerts but deal with streamlined reports. This is one element of automation and reporting that can be tied to the risk approach: Dashboards. Figure 9 shows a dashboard in business terms, using the risk framework to quantify losses in dollars. This is a critical reporting advancement pulled from a whitehat report which can be used to educate, make decisions and ensure that budget is allocated correctly commensurate with risk. Figure 10 shows a dashboard for developers – using D3 Dash. This uses API from Whitehat as well and unlike Figure 9 is not for a CEO or CFO but more for a VP of engineering. It shows tickets and distribution providing insight into the segments of security. It even shows that there is a 14% attrition of developers so decision-makers can tie attrition loss to peak and valleys in organization as well as the training required for secure development.

FIGURE 9
DASHBOARD REPORTING IN BUSINESS TERMS



Source: CXOWare Whitehat Security and Blue Lava Consulting

FIGURE 10
REPORTING DASHBOARD FOR DEVELOPERS



Source: Andy Hoernecke and Blue Lava Consulting

CONCLUSIONS AND LESSONS FOR DECISION-MAKERS

So what does this mean for decision-makers? Firstly, it is important that executive leadership start understanding what is going on in their organizations in terms of information security and this must be explained in business terms and aligned with business. Secondly, criminals are mobilizing and the numbers and breaches validate this. Thirdly, we must look at new technologies and ask how they are aligned to emerging threats. In this regard agile development, user behavioral analytics and automaton must be tied to a big data platform. Importantly, user-behavior analytics must be architected into all future design. Finally, it is critical to audit frequently in order to understand how a business is aligned to emerging threats by ensuring companies build in dynamic controls that go beyond compliance.

This research has identified that in terms of dynamic architecture the critical security problem is that the perimeter is forever gone. The information security maturity model demonstrates how organizations are evolving and where to head to achieve better results in terms of a dynamically safe environment within this new reality in which businesses have no defensible "perimeter" because of co-mingled systems. This model also serves as a mechanism for educating executives. Finally, dynamic and agile tools are required both in terms of decision-making processes, user behavior analytics, the development processes and ways to see across architecture to deal in a faster more effective way with cybercriminals and their coordinated efforts in an agile architecture eco-system.

REFERENCES

Chen, G., Miao, J., Xie, F. and Mao, H. (2013). A framework for storage security in cloud computing. Journal of Management and IT, 3:2, pp. 87-97.

Cho, G. H. and Lee, S. A. (2012) A secure service framework for handling security critical data on the public cloud. Guangzhou, China.

Chonka, A. and Abawajy, J. (2012). Detecting and mitigating HX-DoS attacks against cloud web services. 4th International CSS Symposium, Melbourne, Australia.

Chonka, A., Xiang, Y., Zhou, W. L. and Bonti, A. (2011) Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 34, 4 (July 2011), 1097-1107.

Chou, Y., Levina, O. and Oetting, J. (2011). Enforcing confidentiality in a SaaS cloud environment. 19th Telecommunications Forum (TELOR) Proceedings, Belgrade, Serbia. pp.90-103.

Deshmukh, A. A., Mihovska, A. and Prasad, R. A (2012).Cloud computing security schemes:- TGOS and TMS. Information and Communication Technologies (WICT), 2012 World Congress. Trivandrum, India. Oct. 30 2012-Nov. 2 2012, pp. 203-208.

Elham, H., Lebbat, A. (2012). HX-DoS attacks against cloud web services. Melbourne, Australia.

Gul, I., Ur Rehman, A. and Islam, M. H. (2011). Cloud computing security auditing. Gyeongju, Korea, June, 21-232011. pp. 143–148.

Honer, P. (2013). Cloud Computing Security Requirements and Solutions: A Systematic Literature Review. Thesis. University of Twente, Faculty of Engineering and Mathematics and Computer Science. Enschede, Netherlands.

Ilanchezhian, J., Varadharassu, V., Ranjeeth, A. and Arun, K. (2012) To improve the current security model and efficiency in cloud computing using access control matrix. Proceedings of the 3rd International Conference on Computing, Communications Technology and Networking, July 21-25, 2012, Tamilnadu, India. pp.750-765.

Kumar, P.S. and Sburamanian, R. (2011). Homomorpic Storage Secruity in Cloud Computing. Information International Interdisciplinary Journal. 14,10 (October 2011), 3465-3476.

Mandiant 2014 Threat Report (2014). Trends Beyond the Breach. https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf. Mandiant FireEye Consulting, Milipitas, CA.

Monfared, A.T. and Jaatun, M.G. (2011). Monitoring intrusions and security breaches in highly distributed cloud environments, IEEE 3rd international conference on cloud computing technology and science, Athens, Greece, pp 772–777.

Munoz, A., Gonzalez, J. and Mana, A. (2012). A Performance-Oriented Monitoring System for Security Properties in Cloud Computing Applications. Computer Journal, 55, 8 (Aug 2012), 979-994.

Nishikawa, K., Oki, K. and Matsuo A. (2012). SaaS application framework using information gateway enabling cloud service with data confidentiality. Software Engineering Conference (APSEC), 2012 19th Asia-Pacific, 4-7 Dec. 4-7, 2012. pp. 334-337. Hong Kong, China.

Popović, K. and Hocenski, Z. (2010). Cloud computing security issues and challenges. MIPRO, 2010 Proceedings of the 33rd International Convention, May 24-28, 2010, Opatija, Croatia. pp. 344-349.

Tran, D. H., Nguyen, H. L., Zha, W. and Ng, W. K. (2011). Towards security in sharing data on cloud-based social networks. 8th International Conference on Information, Communications, and Signal Processing (ICICS 2011), Singapore, Dec 2011.

Strauss & Corbin (2015). Basics of Qualitative Research: Grounded Theory Procedures and Techniques, 2nd Edition. Sage Publications. Thousand Oaks, CA.

Wang, S. C., Liao, W. P., Yan, K. Q., Wang, S. S. and Tsai, S. H. (2013). Security of cloud computing lightweight authentication protocol. Proceedings of the Second International Conference on Engineering and Technology Innovation 2012 (ICETI 2012), November 2-6, 2013, Kaohsiung, Taiwan. pp. 284-287.

Yin, Robert (1994). Case Study Research: Design and Methods. Sage Publications. Thousand Oaks, CA.

Zhu, J. and Wen, Q. (2012). SaaS access control research based on UCON. Digital Home (ICDH), 2012 Fourth International Conference, November 23-25, 2012. Guangzhou, China, pp.331-332.