ALERTLOGIC
Security. Compliance. Cloud.

REMOVING THE CLOUD OF INSECURITY

State of Cloud Security Report

Spring 2012

REMOVING THE CLOUD OF INSECURITY

State of Cloud Security Report

ALERTLOGIC
Security. Compliance. Cloud.

Spring 2012

STATE OF CLOUD SECURITY REPORT
Executive Summary 2

METHODOLOGY
Analyzing Real-World Data 4

PERCEPTION VS. DATA
Is the Cloud Really Insecure? 5
Incident Identification 6

SUMMARY OF RESULTS
Just the Facts 7

STATISTICS
Incident Occurrence and Frequency Rates 8

CONCLUSIONS
The Alert Logic Perspective 9

WRAPPING UP
The Data Tells the Story 10

APPENDIX
Data Tables 11

STATE OF CLOUD SECURITY REPORT

Executive Summary

Gartner surveyed MORE THAN 300 cloud computing users, asking them to rank their top three concerns. NEARLY 50% of respondents identified service provider security as their primary issue.[1]

Tier1 Research's 2011 report on the hosting market indicates that the majority of enterprises consider securing infrastructure as the most problematic aspect of the cloud.[2]

While there is clearly a heightened perception of risk in the cloud, are these fears supported by empirical data? The customers and partners of Alert Logic demand an answer to this question. This report is the first in a series of twice-yearly, data-driven analyses in which Alert Logic examines security trends across traditional on-premise and service-provider-managed environments. Alert Logic utilizes real-world security findings to understand the foundational differences between the classes of threats encountered in traditional on-premise deployments versus those found in service provider environments where cloud and hosted infrastructures are managed.

In analyzing the state of security, Alert Logic draws on security data from real end-user environments, both on-premise and managed by service providers, from its base of over 1,500 customers. In this report, the Alert Logic Security Research Team utilized twelve months of security event data captured from July 2010 through June 2011. Security incidents were identified through a combination of automated correlation and validation by certified security analysts. It should be noted that the sample is composed of data from customers who are making an active investment in security. As a result, the findings of this report may represent security-aware organizations and any conclusions drawn based on the data should be understood in that context.

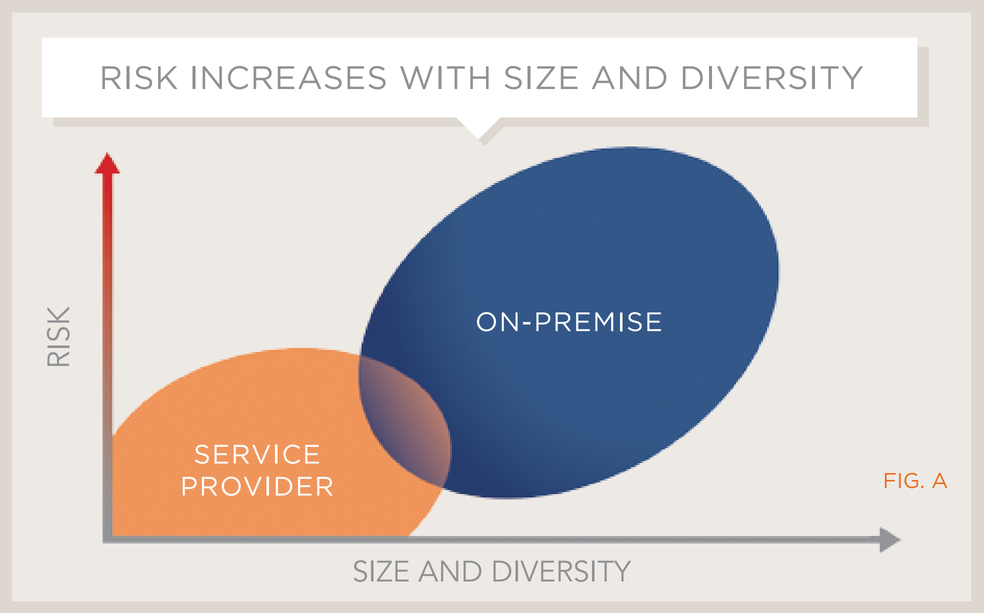


FIG. A

[1] Gartner Global IT Council for Cloud Services report (2010)

[2] Tier1 Research Global Managed Hosting Market Overview (2011)

KEY FINDINGS:

Findings from this study show that while there are differences between the classes and pervasiveness of incidents experienced in the on-premise and service provider environments, those differences may not necessarily line up with general perceptions about security:

- When compared to traditional in-house managed IT environments, service provider environments show lower occurrence rates for every class of incident examined.
- Service provider customers experienced lower threat diversity (i.e., the number of unique incident classes experienced by a customer) than on-premise customers.
- On-premise environments were twelve times more likely than service provider environments to have common configuration issues, opening the door to compromise.
- While conventional wisdom suggests a higher rate of Web application attacks in the service provider environment, Alert Logic found a higher frequency of these incidents in on-premise environments.

Part of the difference in risk level observed in these two environments can be explained by relevant IT surface area. While service providers often manage tens of thousands of servers and applications across multiple data centers, they are composed of vast numbers of individual customer or tenant environments. Each individual customer environment tends to have fewer application types residing on server-based operating systems (OSs) with tightly controlled network access, resulting in a relatively small relevant surface area for attack. In contrast, on-premise enterprise IT deployments tend to have a larger surface area due to their more diverse environments characterized by a broad array of OSs and applications, along with desktops, mobile devices and more network entry points.

What does this mean for security management decisions, especially in the context of migrating infrastructure to hosted and cloud deployments?

Security fears should not prevent organizations from taking advantage of hosting and cloud services. While security management is a critical issue when choosing a service provider, the decision should be based on a review of actual risks, not perceptions that are not supported by data.

Service providers, who tend to have detailed, repeatable management processes and infrastructure configurations, provide a good model for enterprises committed to maintaining on-premise infrastructure.

Service providers should focus their security management efforts on the threats most prevalent in their environment, while continuing to manage to best practices to create secure, highly available environments.

IT decision-makers should consider the benefits and risks of each model when deciding which workloads and applications to deploy in service provider environments and which to keep on-premise. In turn, internal resources can focus on the security posture of the area for which they maintain management responsibility.

METHODOLOGY:

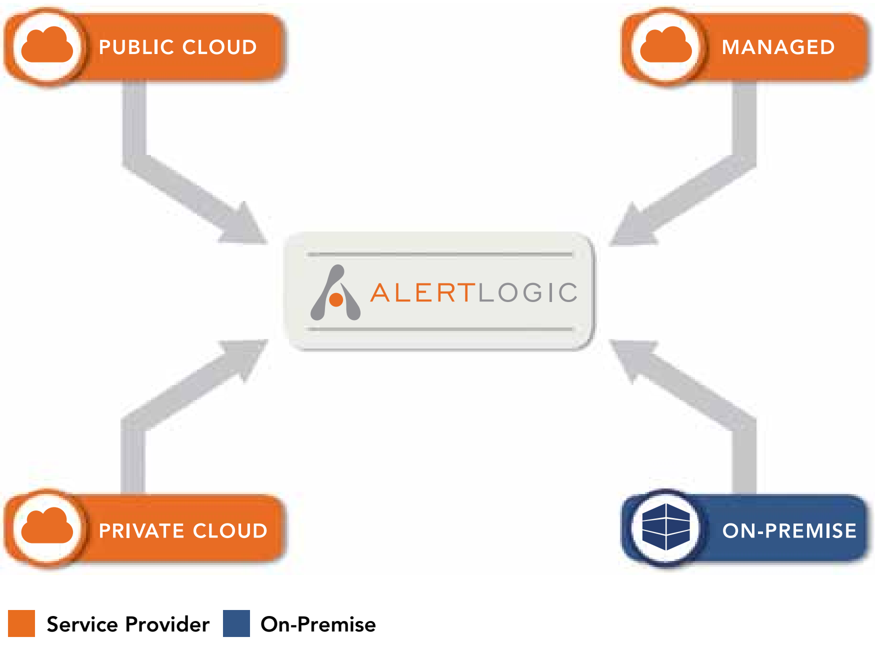
Analyzing Real-World Data

This report provides a comparative quantitative analysis of the classes and frequencies of incidents encountered in on-premise environments vs. service provider environments.

The analysis for both the service provider and on-premise cohorts is based on incident data detected in actual customer environments secured by Alert Logic, not from surveys, lab environments, or honeypots. Alert Logic captures security events in these environments through network-based, signature-driven intrusion detection systems (IDS). To correct for noise and false positives, Alert Logic utilizes a patented expert system that evaluates seven factors in determining if one or more network-based events elevate to the level of an authentic security incident (See Fig. D). Further, a team of GIAC-certified security analysts reviews each incident to ensure validity and to confirm the threat or compromise, providing an additional layer of scrutiny to minimize false positives.

VISIBILITY ACROSS MULTIPLE ENVIRONMENTS

FIG. B



The service provider cohort is composed of hosted and cloud environments managed by one of the Alert Logic service provider partners.

These providers include more than half of the top 30 service providers headquarted in North America and are listed in the appendix.

The on-premise cohort represents environments deployed on the customer's premises. Alert Logic on-premise customers come from a broad range of organizations, cutting across all verticals, with a concentration of enterprises in highly regulated industries such as health care, finance, energy and retail/e-commerce. As expected, on-premise deployments were typically larger than service provider deployments, featuring a broader set of applications and operating systems. The majority of both cohorts are located in North America and Western Europe.

PERCEPTION VS. DATA:

Is the Cloud Really Insecure?

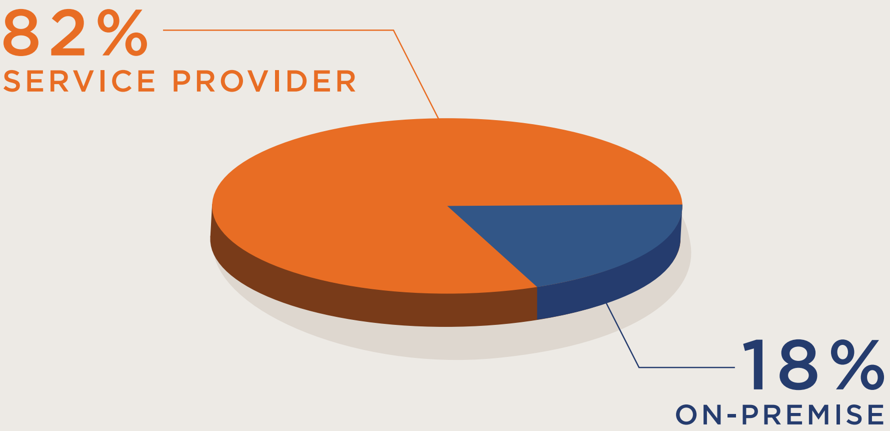
Improved agility and financial benefits have driven the growth of the Infrastructure-as-a-Service (IaaS) model. However, a perception remains that IaaS offerings from service providers pose greater security risks than traditional on-premise deployments.

While there is clearly a heightened perception of risk, do managed and cloud environments hosted by service providers actually experience different classes of threats, or different frequencies of incidents?

As providers of Security-as-a-Service to over 1,500 organizations with IT infrastructure housed either in on-premise environments or with managed service providers, Alert Logic draws on an extensive warehouse of security event data to examine this assumption and is uniquely poised to assess the validity of popular beliefs regarding the relative security of service provider environments.

ALERT LOGIC CUSTOMER DATA SET

FIG. C



ON-PREMISE? HOSTED? SERVICE PROVIDER? CLOUD?

How Alert Logic categorized its customer data

For its analysis, Alert Logic has categorized security data into two environments: on-premise and service provider. On-premise customers own and manage their own IT infrastructure. Service provider customers are an aggregation of all customers utilizing Infrastructure-as-a-Service solutions from a service provider, spanning from the elastic cloud to managed or dedicated hosted environments.

Incident Identification

2.2 BILLION security events observed during the study period were automatically evaluated and correlated through Alert Logic's expert system and reviewed by Alert Logic's security analysts.

MORE THAN 62,000 INCIDENTS were verified and classified into seven incident categories.

EVENT VS. INCIDENT

EVENT: Evidence of suspicious behavior detected via an IDS signature.

INCIDENT: Validated threat deemed to require a response, identified by correlating one or more events.

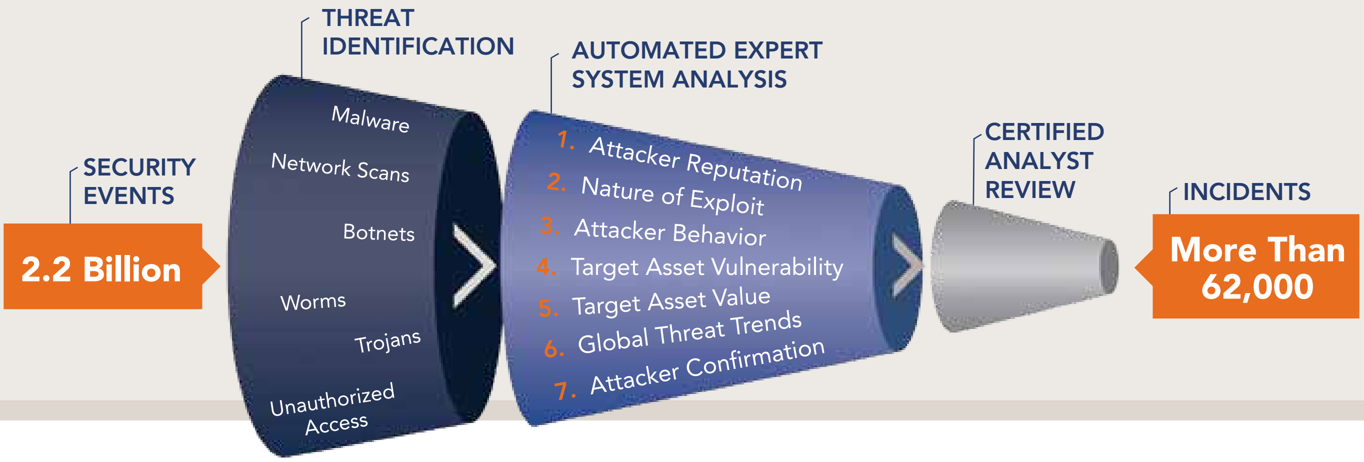
EXAMPLE: A single port scan is an event. A series of port scans over time from a host recognized as an attack source is an incident.

ALERT LOGIC SECURITY INCIDENT CATEGORIES

INCIDENT CLASS	DEFINITION	EXAMPLES
Application Attack	Exploit attempts against applications or services that are not running over HTTP protocol.	Buffer overflow
Brute Force	Exploit attempts enumerating a large number of combinations, typically involving numerous credential failures.	Password cracking attempts
Malware/ Botnet Activity	Malicious software installed on a host engaging in unscrupulous activity, data destruction, information gathering or creation of backdoors. Included in this category is botnet activity: post-compromise activity displaying characteristics of command and control communication.	Conficker, Zeus botnet, command and control botnet communication activity
Misconfiguration	Network/host/application configuration issues that introduce possible security vulnerabilities, typically a result of inadequate hardening.	Missing patches and writable anonymous FTP directories
Reconnaissance	Activity focused on mapping the networks, applications and/or services.	Port scans and fingerprinting
Vulnerability Scan	Automated vulnerability discovery in applications, services or protocol implementations.	Unauthorized Nessus scan
Web Application Attack	Attacks targeting the presentation, logic or database layer of Web applications.	SQL injection

FIG. D

INCIDENT IDENTIFICATION APPROACH



SUMMARY OF RESULTS:

Just the Facts

To assess whether on-premise and service provider environments experience different levels of risk, Alert Logic evaluated three factors:

Occurrence: The percentage of customers in each cohort experiencing each class of incident defined in the Security Incident Categories chart. Customers are included if they experienced a specific class of incident at least once during the study period.

Frequency: The average frequency of incidents, by class, for impacted customers, indicating how often customers experience an incident of a particular category.

Threat Diversity: The threat diversity in each group, i.e., the number of unique incident classes (of the seven categories reviewed) encountered by the customers in each cohort.

These measures, in combination, help define the critical elements of a security program. The class and frequency of events help determine the core elements of a program; higher threat diversity requires a more complex and involved security program to adequately protect assets.

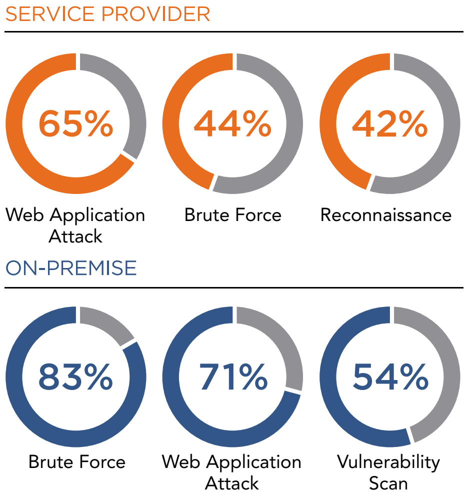
Analysis of these three factors shows that even in security-conscious environments, virtually every environment will encounter meaningful threats. Further, service-provider managed-environments encountered more favorable results in all three of the criteria analyzed in this report. It should be noted that some of this could be explained by the differences in size and platform diversity of cloud vs. on-premise environments.

The rate of **occurrence** in an on-premise environment is more likely to be greater than the occurrence rate for service provider customers. This observation is true for all threat categories.

The **frequency** of experienced incidents is higher for on-premise environments across most of the threat categories.

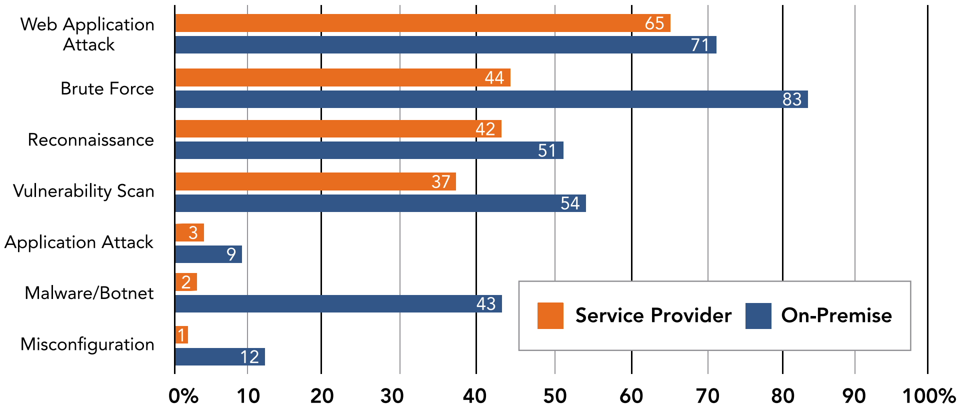
The **threat diversity** for on-premise environments is greater than the threat diversity for service provider environments.

TOP THREE INCIDENT CLASSES FIG. E



OCCURRENCE: PERCENT OF ALERT LOGIC CUSTOMERS EXPERIENCING SECURITY INCIDENTS FIG. F

By Class of Incident



STATISTICS:

Incident Occurrence and Frequency Rates

While service-provider-managed environments encountered lower rates and frequency of security incidents across all categories, there are notable differences in the data. Alert Logic observed a far greater percentage of misconfiguration-based incidents in the on-premise environment.

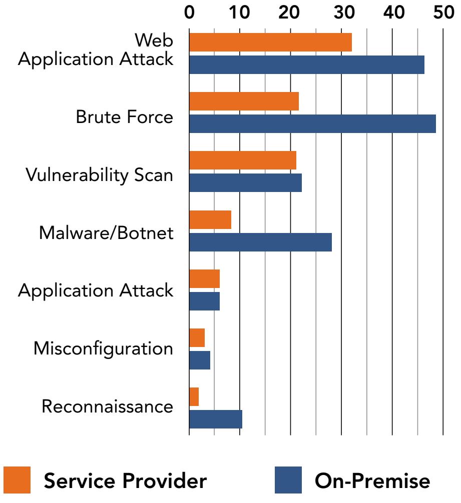
The average number of misconfiguration-related incidents per impacted customers are roughly equivalent: 3.0 instances in hosted/cloud, 4.0 on-premise. However, 12% of on-premise customers experienced a misconfiguration incident while only 1% of service provider customers did.

FREQUENCY: FIG. G

NUMBER OF INCIDENTS PER IMPACTED CUSTOMER

By Class of Incident

July 2010 - June 2011



The most significant spread was found in **malware/botnet incidents**. On-premise environments were overwhelmingly more likely to encounter such incidents in their environments when compared to service-provider-managed environments, with 43% of on-premise environments versus 2% of service-provider-managed environments.

Both on-premise (71%) and service provider (65 %) customers are highly likely to have experienced **Web application attacks**, and impacted customers in both environments were likely to have experienced a high number of such attacks over the period of study (on-premise 46.6, service provider 32.4).

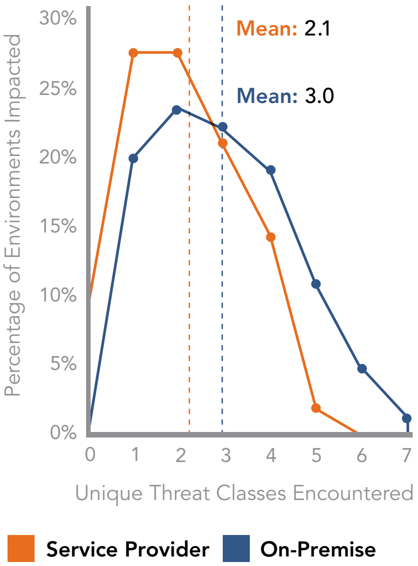
Brute force incidents are even more commonly experienced in an on-premise environment than Web application attacks, with 83% of customers receiving an average of 47.3 such attacks. While brute force incidents in the service provider realm are significant (44% of customers experienced them), the difference between the two environments is surprising. With more public-facing targets (websites) in the service provider environment, the reverse might have been expected.

Vulnerability scans are observed among 37% of service provider customers and 54% of on-premise customers.

THREAT DIVERSITY:

Threat diversity is the third element that Alert Logic analyzed. While a lower threat diversity by itself does not mean an inherently less risky environment, a higher threat diversity indicates that a broader set of attack vectors are at play.

DISTRIBUTION OF UNIQUE THREATS FIG. H



Alert Logic found lower threat diversity in service provider environments than in on-premise environments. During the period of this study, service provider customers averaged threats in 2.1 categories (out of the seven categories analyzed), while on-premise customers experienced 3.0.

CONCLUSIONS:

The Alert Logic Perspective

A belief persists that service provider environments are less secure than on-premise environments, but this is simply not supported by Alert Logic data.

Alert Logic analysis indicates that service provider environments tend to be less prone to a broad range of security incidents than on-premise environments. Further, service provider environments tend to experience a narrower range of attack vectors. Possible explanations include the presence of more standardized system configurations in the service provider world, a narrower range of use cases among service provider customers, and the relative maturity of the IaaS industry.

> It's not that the cloud is inherently secure or insecure. It's really about the quality of management applied to any IT environment.

While this data certainly casts doubt on conventional wisdom and concerns about security in the service provider environment, Alert Logic does not believe that it leads to a simple "service provider vs. on-premise" conclusion. While we observed differences between the two environments, we believe that there are several factors that help explain these variances:

- The typical size of a customer/user in each environment
- The types of workloads found in each environment
- The diversity of each environment
- The presence of user endpoints in the on-premise environments

All of these differences speak to the relationship between risk level and IT surface area in any environment.

OPPORTUNITY TO IMPROVE SECURITY POSTURE

FIG. I

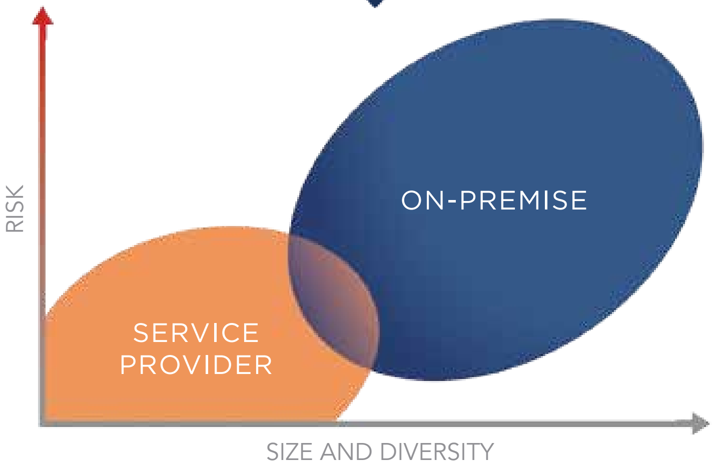


Fig. I represents a conceptual framework for thinking about these differences. While service providers manage vast networks with tens of thousands of servers and applications, the relevant surface area a prospective buyer of IaaS solutions should consider is that of the individual customer environment. In Alert Logic's experience, those individual customer environments skew to a smaller and simpler footprint as measured by a number of nodes and applications, and breadth of operating systems. In contrast, on-premise environments managed by the typical enterprise span a much broader array of endpoints, applications and operating systems.

Service provider environments, with smaller deployments, inherently avoid some of that risk and therefore are a good choice for appropriate workloads.

Organizations making decisions about cloud and hosted infrastructure can exploit these differences to improve their security posture and make the most effective use of IT resources.

Smart enterprises should take advantage of the service provider model for certain workloads.

Those workloads can take advantage of the service provider's highly repeatable configurations and processes and demonstrated ability to manage to best practices (evident in the far lower misconfiguration rates observed). These characteristics allow service providers to very effectively manage security for a focused set of threats.

For example, a Web-based server application and related databases containing sensitive customer data may be a good fit for migrating to a hosted or cloud environment. The segregation of server-based applications and assets from a diverse and porous on-premise network with numerous mobile clients and desktops, which are often targets of highly prevalent malware and botnet infection, can create an inherently more secure environment for that application. At the same time, in-house IT resources can focus on the unique challenges in their environment.

Service-provider-managed environments are not magic bullets and not all are created equal.

Alert Logic data and experience suggest that much of the improvement in risk profile in the service provider customer data comes from a lower complexity and diversity and better management of the basics, most notably configuration management. The primary decision an enterprise must make is whether they wish to replicate those best practices or if they wish to let someone else handle them. Selection of a service provider should include careful evaluation of the security policies and solutions that are available from the providers under consideration.

Service providers must be aware that while they benefit structurally from more limited and well-defined workloads, enterprise security concerns will not disappear.

Lower threat diversity today doesn't mean that service providers will not face increasing threat diversity in the future. To protect against leading threat vectors, service providers are best served by focusing time and energy on the most pervasive risks in their customer environments: Web application attacks, brute force and reconnaissance. In addition, service providers should continue to build on their demonstrated competence in managing to best practices around fundamental security hygiene, such as configuration management and operating system hardening.

By utilizing strong product management disciplines to determine which IaaS solutions are offered and supported, service providers can play a role in minimizing the threat diversity in cloud environments by limiting the IT surface area for potential attacks. Managing security programs requires service providers to maintain continued visibility into the threats encountered by customers and continuous improvement in identifying and defending against those threats.

Security management is not a discrete goal to be achieved and considered complete; it is an ongoing process that is fundamental to providing IT infrastructure management as a service.

WRAPPING UP:
The Data Tells the Story

With security visibility into both on-premise and service provider environments, Alert Logic findings offer a unique perspective on managing IT security. Whether in the cloud or an on-premise environment, effectively securing IT infrastructure is largely about the quality of management:

- Focusing on basic hygiene, Web application security and configuration issues
- Strategically isolating workloads in the most appropriate environment
- Building and maintaining security expertise for workloads retained on-premise

Despite the widespread perception that the cloud presents an increased security risk, fears that the cloud is inherently insecure are not supported by the data. ■

APPENDIX: Data Tables

OCCURRENCE: PERCENT OF CUSTOMERS EXPERIENCING SECURITY INCIDENTS

By Class of Incident Jul 2010 – Jun 2011	SERVICE PROVIDER	ON-PREMISE
Web Application Attack	65%	71%
Brute Force	44%	83%
Reconnaissance	42%	51%
Vulnerability Scan	37%	54%
Application Attack	3%	9%
Malware/ Botnet Activity	2%	43%
Misconfiguration	1%	12%

FREQUENCY: NUMBER OF INCIDENTS PER IMPACTED CUSTOMER

By Class of Incident Jul 2010 – Jun 2011	SERVICE PROVIDER	ON-PREMISE
Web Application Attack	32.4	46.6
Brute Force	22.4	47.3
Vulnerability Scan	21.8	22.9
Malware/ Botnet Activity	8.4	28.1
Application Attack	6.2	6.2
Misconfiguration	3.0	4.0
Reconnaissance	2.4	10.1

TOP THREE INCIDENT CLASSES

SERVICE PROVIDER	ON-PREMISE
1. **Web App. Attack** (65%)	1. **Brute Force** (83%)
2. **Brute Force** (44%)	2. **Web App. Attack** (71%)
3. **Reconnaissance** (42%)	3. **Reconnaissance** (54%)

THREAT DIVERSITY: DISTRIBUTION OF UNIQUE THREATS

THREAT DIVERSITY	SERVICE PROVIDER	ON-PREMISE
0	9%	0%
1	27%	20%
2	27%	23%
3	21%	22%
4	14%	18%
5	2%	11%
6	0%	5%
7	0%	2%
Mean No. of Threat Classes Encountered	2.1	3.0

SERVICE PROVIDER PARTNERS INCLUDED IN STUDY

SERVICE PROVIDER PARTNER	WEBSITE
ATOS Origin	atos.net
CyrusOne	cyrusone.com
Datapipe	datapipe.com
DediPower	dedipower.com
Hosting.com	hosting.com
Hostway	hostway.com
Internap	internap.com
Latisys	latisys.com
LayeredTech	layeredtech.com
LogicWorks	logicworks.net
Megapath	megapath.com
NaviSite	navisite.com
OpSource	opsource.net
Peer1	peer1.com
Rackspace	rackspace.com
Sungard Availability Services	sungardas.com
Visi	visi.com
Windstream	windstreambusiness.com

ALERTLOGIC
Security. Compliance. Cloud.

CONTRIBUTORS

Lead Analysts
Tyler Borland
Mukul Gupta, PhD
Jacob Martinson
Johnathan Norman

Author
Maureen Rogers

Editors
Celeste Monroe
John Whiteside

ALERTLOGIC
Security. Compliance. Cloud.

Alert Logic, Inc.
1776 Yorktown, 7th Floor
Houston, TX 77056

www.alertlogic.com