



**AN EMPIRICAL  
ANALYSIS**  
OF REAL WORLD THREATS

**State of Cloud Security Report**

---

**Fall 2012**

---

# AN EMPIRICAL ANALYSIS OF REAL WORLD THREATS



## State of Cloud Security Report

Fall 2012

---

STATE OF CLOUD SECURITY REPORT	
Executive Summary	2
CLOUD VS. ON-PREMISE SECURITY	
Insight Into Attacker Behavior	3
Key Findings: Incident Occurrence, Incident Frequency, Threat Diversity	3
ALERT LOGIC	
Methodology and Customer Data Set	4
General Insights by Attack Class	5
THE DETAILS: DATA AND OBSERVATIONS BY INCIDENT CLASS	
Incident Occurrence	6
Incident Frequency	7
Threat Diversity	7
Industry Data	8
Country Data	10
Drilling Down on Web Application Attacks	11
“FROM RECON TO BREACH” INFOGRAPHIC	12
WRAPPING UP	
The Data Tells the Story	14
APPENDIX	
Data Tables	15

---

## STATE OF CLOUD SECURITY REPORT

# Executive Summary

WEB APPLICATION ATTACKS  
REMAIN THE

# MOST

## SIGNIFICANT THREAT

for service provider environments.



## Insight

More than **HALF** of the Web application attacks we observed came from freely downloadable tools.

## CLOUD VS. ON-PREMISE SECURITY

## An Empirical Analysis of Real World Threats

Is the cloud inherently insecure? Are on-premise IT environments a safer option for security-conscious organizations? Recognizing that these questions are critical to customers considering moving infrastructure into service provider-hosted and cloud environments, in February 2012 Alert Logic launched the first in a series of semi-annual reports on cloud security, based on analysis of threat data from its customers' production environments. Reviewing 12 months of operational data, including more than two billion events and over 60,000 security incidents, Alert Logic concluded that the cloud is inherently no less secure than the on-premise environment.

For this second report, Alert Logic took the same approach: analyzing operational data from business customers in both on-premise and service provider environments and comparing the occurrence, frequency and diversity of incidents across seven categories of security threats.

The results of this study underscore Alert Logic's earlier conclusion that the cloud is as safe as on-premise environments. Additional analysis shows that the type of infrastructure (service provider vs. on-premise) is a better determinant of the type and frequency of attacks than the target's industry segment.

This second report also reinforces Alert Logic's previous finding that Web application attacks are a significant threat for customers in all environments. Web application attacks are once again the number-one incident type experienced in the cloud, and the second most common incident type in on-premise environments. Based on these findings, we have taken a deeper look at Web application attacks in this report. Given that more than half of the Web application attacks we observed came from freely downloadable tools such as Havij, our findings reinforce the need to put a greater focus on this attack vector.

## INSIGHT INTO ATTACKER BEHAVIOR

Targeted attacks are highly publicized. But our data suggests that the majority of malicious activity is opportunistic rather than targeted—attackers are looking for vulnerable targets, rather than selecting specific organizations to attack. This is demonstrated by:

- A high level of reconnaissance activity
- Geographic origins of reconnaissance activity
- The similarity of data across industries

The implication of these observations is that security managers should assume that vulnerabilities will be discovered and exploited, regardless of an organization's likelihood of being specifically targeted.

## KEY FINDINGS: INCIDENT OCCURRENCE, INCIDENT FREQUENCY, THREAT DIVERSITY

In this study period, service provider-managed environments did not encounter a greater level of threats than on-premise environments. All factors in the analysis supported this conclusion.

Web application attacks remain the most significant threat for service provider environments (53 percent of customers impacted) and the second most significant threat in on-premise environments (44 percent of customers impacted). **Further analysis of Web application attacks reveals that the majority were perpetrated using common and freely available tools.**

In the context of making precise comparisons between our first and second reports, it is worth noting that Alert Logic's security research team makes ongoing improvements and refinements to its threat detection process. Because of this, there will always be changes between reporting periods that preclude direct quantitative comparisons with data analyzed in different periods. While direct quantitative comparison may not be possible, the two sets of data are similar, and differences should be looked at directionally, if not as precise measures.

The bottom line remains the same as in the initial report: While there are many factors to weigh when deciding whether to move infrastructure to the cloud, an assumption of insecurity should not be among them.

The first Alert Logic *State of Cloud Security Report* evaluated three factors—Incident Occurrence, Incident Frequency and Threat Diversity. We are continuing these three vectors of analysis in this report.



### Incident Occurrence

The percentage of customers experiencing each type of incident. Customers are included if they experienced a specific class of incident at least once during the study period. *(How many customers were impacted by each incident class?)*



### Incident Frequency

The average frequency of incidents of each type, per impacted customer. *(How many times did impacted customers experience each type of incident?)*



### Threat Diversity

The threat diversity in each group, i.e., the number of unique incident types (of the seven classes reviewed) encountered by the customers in each environment. *(How many different types of incidents did impacted customers experience?)*

## ALERT LOGIC:

## Methodology and Customer Data Set

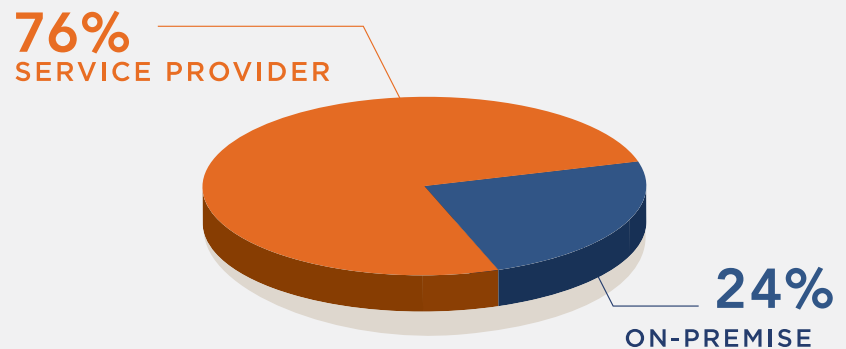
## ALERT LOGIC METHODOLOGY

The data used in this report is actual incident data detected in 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 multiple factors in determining if one or more network-based events elevate to the level of an authentic security incident. 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.

As part of its ongoing process, Alert Logic regularly refines its threat detection based on changing threat activity. During this reporting period, Alert Logic fine-tuned the detection signatures used in its expert system, adding several new logic branches.

## ALERT LOGIC CUSTOMER DATA SET

FIG. A



### ON-PREMISE? HOSTED? SERVICE PROVIDER? CLOUD? How Alert Logic categorized its customer data

In this report, Alert Logic studied incident data from over 1,600 customers in a broad range of industries. For its analysis, Alert Logic has categorized its 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. 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.



ALERT LOGIC:

# General Insights by Attack Class

Our research yielded the following general observations for the security incident categories used in our analysis:

INCIDENT CLASS	OBSERVATIONS	DEFINITION	EXAMPLES
APPLICATION ATTACKS	Stem from the large number of leaked older toolkits taking advantage of the existing exploitable vulnerabilities.	Exploit attempts against applications or services that are not running over HTTP.	Buffer overflow
BRUTE FORCE ATTACKS	Are on the increase because of the number of password and user lists that have been compromised and released to the open Internet.	Exploit attempts enumerating a large number of combinations, typically involving numerous credential failures.	Password cracking attempts
MALWARE/BOTNET ACTIVITY	Is primarily introduced to enterprise entities through spam delivery or a direct hack. Malware is used to compromise hosts and send secured data to remote locations.	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
MISCONFIGURATIONS	In general are rarely observed, suggesting that when it comes to the basics, organizations practice reasonably good security hygiene.	Network/host/application configuration issues that introduce possible security vulnerabilities, typically a result of inadequate hardening.	Missing patches and writable anonymous FTP directories
RECONNAISSANCE ATTACKS	Are on the rise. As botnets increase, so do the number of compromised hosts first found through reconnaissance techniques.	Activity focused on mapping the networks, applications and/or services.	Port scans and fingerprinting
VULNERABILITY SCANS	Are a more invasive form of reconnaissance and often follow simpler reconnaissance incidents.	Automated vulnerability discovery in applications, services or protocol implementations.	Unauthorized Nessus scan
WEB APPLICATION ATTACKS	By SQL injection remain the number one attack, due to an increased awareness and knowledge of SQL injection techniques, and their ease of use and effectiveness against high-profile targets.	Attacks targeting the presentation, logic or database layer of Web applications.	SQL injection

THE DETAILS:

# Data and Observations by Incident Class

**WEB APPLICATION ATTACKS AND BRUTE FORCE ATTACKS WERE THE TOP TWO INCIDENT TYPES FOR ALL ENVIRONMENTS.**

**1.5 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**

**70,000**

**SECURITY INCIDENTS**

were verified and classified into seven incident categories: application attack, brute force, malware/botnet activity, misconfiguration, reconnaissance, vulnerability scan and Web application attack.

### EVENT VS. INCIDENT

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

**INCIDENT:** An event or group of events that have been confirmed as a valid threat based on advanced automated analysis by Alert Logic's expert system, and verified by certified analysts.

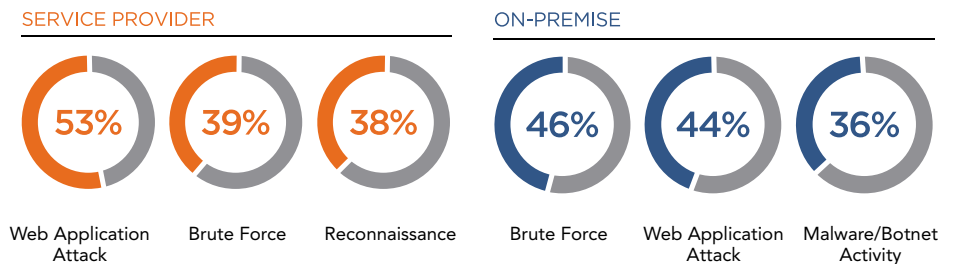
### INCIDENT OCCURRENCE

Web application and brute force attacks were the two most common incident types experienced in both on-premise and service provider environments. For service providers, reconnaissance was the third most significant attack vector. For on-premise environments, malware/botnet activity holds this position.

While the proportion of customers impacted in the top threat categories—Web application, brute force, reconnaissance and vulnerability scans—was not appreciably different between on-premise and service provider environments, we saw larger differences in other incident types. For malware/botnet activity, application attacks and misconfigurations, a far greater percentage of on-premise customers experienced incidents.

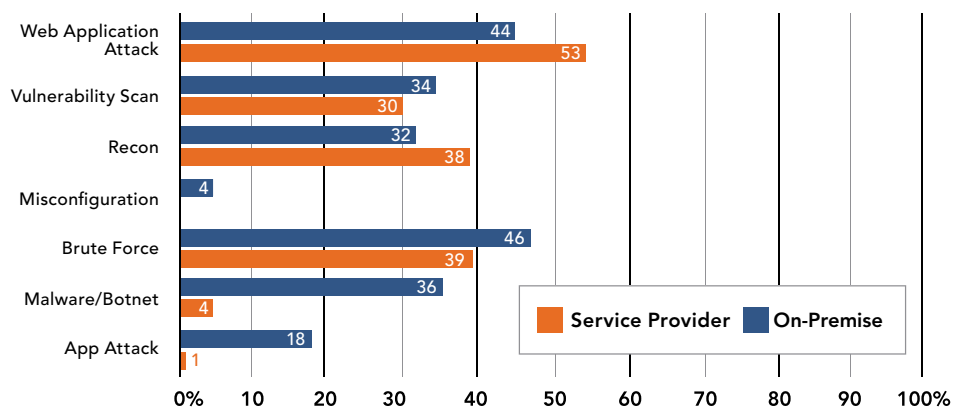
INCIDENT OCCURRENCE: TOP THREE INCIDENT CLASSES

FIG. B



INCIDENT OCCURRENCE: TOP THREE INCIDENT CLASSES

FIG. C





In each environment, certain types of incidents were more prevalent.

A higher percentage of customers in on-premise environments experienced brute force, vulnerability scan, application attack, malware/botnet and misconfiguration incidents.

For Web application attacks and reconnaissance incidents, a slightly greater percentage of service provider customers were affected. Service provider environments represent good targets for reconnaissance attacks, as scanning an IP range touches a large number of possible targets.

### INCIDENT FREQUENCY

For every incident class, the number of incidents per impacted customer was higher in the on-premise environment. In some cases these differences were quite large.

While roughly half of all customers—whether service provider or on-premise—were likely to have experienced a **Web application attack**, the average number of such attacks was 61.4 among on-premise customers. For service provider customers, it was 27.8.

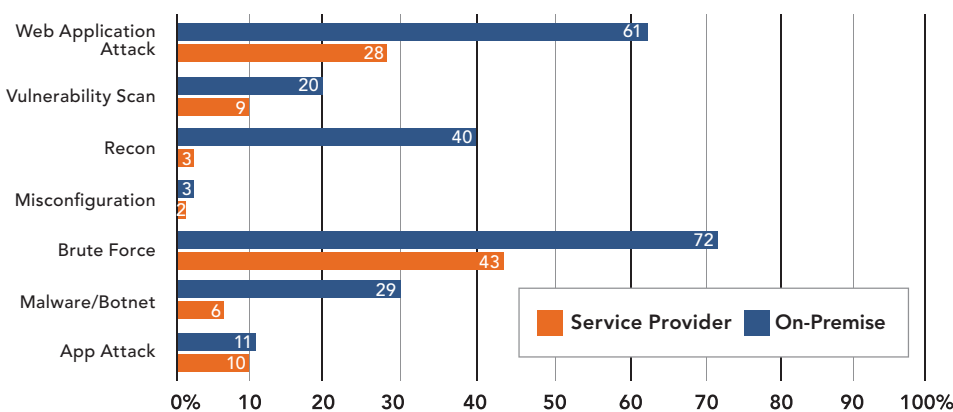
**Brute force attacks**, while similarly experienced by on-premise (46%) and service provider (39%) customers, also showed a wide disparity in frequency. On-premise customers

averaged 71.7 such attacks, while impacted service provider customers were hit with an average of 42.6 brute force attacks.

For **reconnaissance attacks**, the difference was also significant. Service provider customers experiencing reconnaissance attacks averaged 2.7 such attacks; for on-premise customers, the average was 40.

FIG. D

INCIDENT FREQUENCY:  
NUMBER OF INCIDENTS PER IMPACTED CUSTOMER



### THREAT DIVERSITY

For on-premise environments, customers experienced an average of 2.9 types of incidents. Service provider customers experienced an average of 2.1 incident types. While a lower threat diversity does not necessarily indicate an inherently safer environment, it does suggest a narrower range of threats, requiring a different security posture.

DISTRIBUTION OF UNIQUE THREATS

FIG. E





## THE DETAILS:

# Data and Observations by Incident Class (cont'd)

---



## Insight

Type of infrastructure is a **more important** determinant of type and frequency of attack than industry sector.

In this second *State of Cloud Security Report*, Alert Logic added two new areas of analysis:

1. Industry Segmentation
2. Country of Attack Origin

### INDUSTRY DATA

Alert Logic categorized its customer data along industry lines, grouping customers into twelve categories. The incident occurrence for these industries, across both environments, is shown below. The top five industries on the list yielded enough data to make meaningful observations.

Alert Logic researchers made the following observations:

*In general, the type of infrastructure (on-premise versus service provider) is a more important determinant of type and frequency of attack than the targeted customer's industry sector.*

Businesses with on-premise IT environments consistently experienced more frequent attacks across a more diverse set of threats, compared to businesses with cloud-based IT infrastructure.

The divergence in attack frequency between on-premise and service provider environments was wide:

- For IT Services, impacted service provider companies experienced 17.6 Web application attack incidents per customer, compared to 159.2 for on-premise environments.
- For E-commerce, the gap was also significant: 29.5 for service providers versus 103.3 for on-premise. (However, the percent of customers impacted was almost twice as large in the service provider E-commerce sector than in the same sector for enterprises.)
- Other instances where the on-premise attack frequency far outweighed that among service provider customers were reconnaissance incidents in E-commerce: 129.5 (on-premise) versus 1.7 (service provider); brute force attacks in IT Services: 218.4 (on-premise) versus 25.8 (service provider); and reconnaissance attacks in Financial Services: 62.6 (on-premise) versus 1.6 (service provider).

FIG. F

While industry differences were less significant than the type of environment, we observed some interesting industry-specific variations:

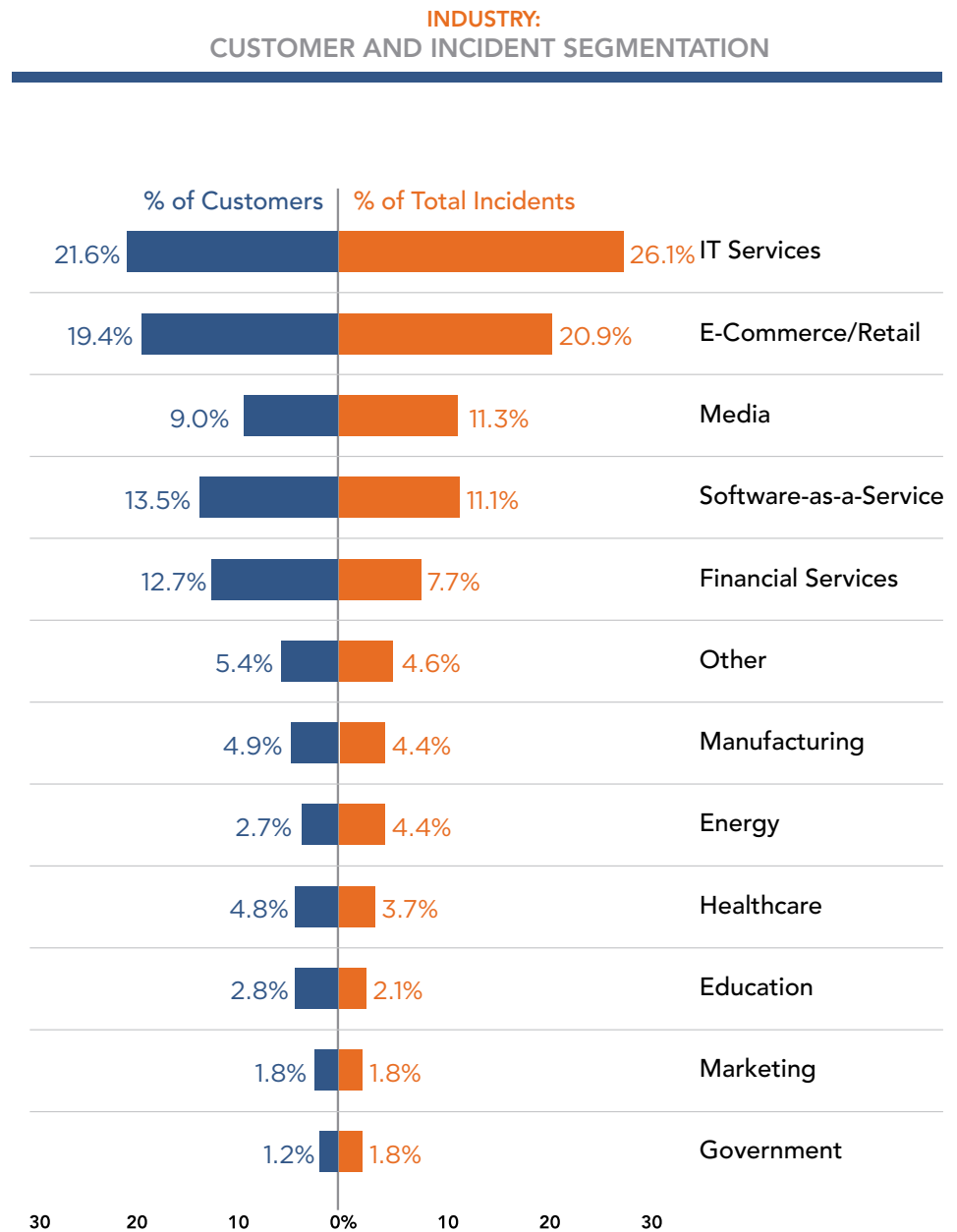
**IT Services** companies that have a public presence experienced a large number of Web application attacks. There are also constant brute force attempts to gain access to these environments, likely because of the number of individuals with escalated privileges, access to servers and network configurations that make them useful to attackers.

**E-commerce** and **SaaS** environments are frequent targets of scanning, much of which is due to compliance assurance by third-party testers.

Malware is seen more frequently in **Financial Services**, possibly due to large numbers of desktop endpoints in banking environments and the volume of financial transactions conducted daily from personal computers.

A significant number of **Media** companies are being targeted by hacktivists with a public agenda against government regulation of the Internet.

**Energy** and **Healthcare** enterprises seem to be among the most heavily targeted industry segments, but Alert Logic researchers consider this conclusion to be preliminary based on the lower representation of these industries in the data set.

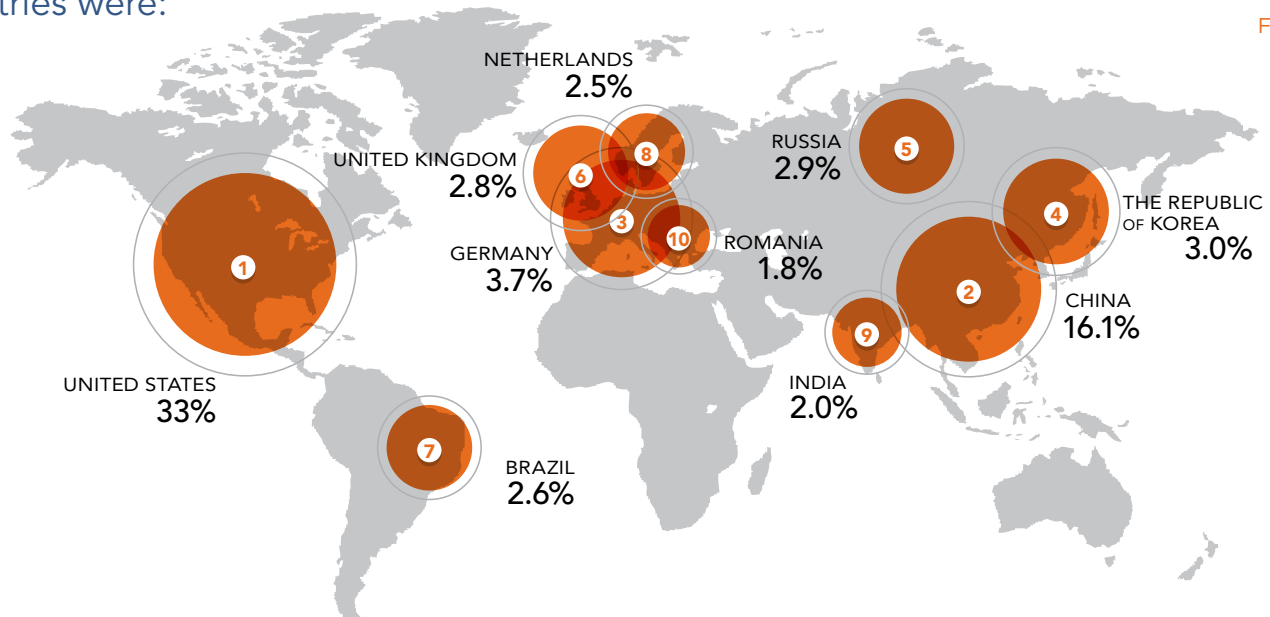


## THE DETAILS:

## Data and Observations by Incident Class (cont'd)

## COUNTRY DATA

During this report period, Alert Logic recorded incidents originating in 165 countries, with the U.S. and China accounting for nearly half of the total number. The top ten countries were:



The **United States** was the country of origin for 33 percent of the incidents analyzed in this study and is responsible for 35.4 Web application attacks per impacted customer. We believe that this may be the result of the U.S. having a large number of unsecured personal computers with access to broadband connections that are attractive targets for hackers in other countries as well as botnet attacks.

**China** accounted for 16 percent of the attacks, ranking second. We noted an especially high frequency of incidents per customer impacted for reconnaissance attempts originating in China. This suggests a scenario in which hackers in China are doing reconnaissance, identifying vulnerable workstations in the bandwidth-rich U.S., adding those machines to botnets and using them to launch attacks on nearby targets.

**China, India, The Republic of Korea** and **Russia** were the source of many reconnaissance and brute force attacks, perhaps being launched from compromised machines in regions that tend to have older, unpatched operating systems.

**Germany** has one of the largest concentrations of command and control servers in the world. This is a result of a large number of hacking groups residing in an area, combined with the increasing number of regional data centers. **Russia** has a large number of application attacks driven by an active black market for binary exploit code. **India** and **The Republic of Korea** are significant contributors to incidents only because of brute force attempts.

Threat diversity by country is universally low: among customers attacked from one country, most experience fewer than two types of incidents from that country. This is lower than the threat diversity for both on-premise (2.9 different types of threats) and service provider (2.1 different threat types) customers.

There are also different types of and motivations for attacks in different regions; for example, reconnaissance to access data and proprietary information from China versus profit-driven application attacks from Russia.

## TWO-THIRDS OF ALL ATTACKS CAME FROM FREELY DOWNLOADABLE TOOLS.



### Insight

The most common tool, **HAVIJ**, utilizes SQL injection and was **responsible for 44%** of all Web application attacks.

### DRILLING DOWN ON WEB APPLICATION ATTACKS

Web application attacks are prevalent and frequent, and are implicated in many data breaches. In this report, we analyzed the tools used to launch these attacks and found that a majority of attacks are launched via identifiable tools, many of which are free, easily available and easy to use.

There are some differences between service provider and enterprise environments: 20 percent of service provider customers experience attacks that use Havij, compared to only 8 percent in enterprise environments. On the other hand, impacted enterprise customers typically experienced four times more incidents, compared to impacted service provider customers.

Some of the attack tools used are open source or easily obtained (Havij, SqlMap, NetSparker, Nessus, w3af, loginpwnz). Others are vulnerability-specific or software-specific attacks (shopxp scanner, tomcat scanner). Still others are less easily identified and more generic in nature. The popularity and ease of use of Havij sets it apart from the rest in terms of the threat it poses; it enables relatively unsophisticated attackers to launch attacks. SqlMap is one of the most powerful SQL injection tools, but requires a more skilled attacker to execute effectively.

The impact of a successful attack for each of these tools varies significantly. A successful Havij or SqlMap (or loginpwnz) attack, for example, results in the download of an entire database, and even the ability to run code on a SQL server. Conversely, a successful w3af, nessus or generic incident would only identify a vulnerability, and would not cause direct damage.

### OCCURRENCE: SOURCE OF WEB APP ATTACKS

**67%**  
TOOLS

Havij	43.5%
Generic	5.8%
shopxp_scanner	5.7%
sqlmap	3.6%
NetSparker	1.9%
cmd.exe	1.4%
mranderson	1.3%
loginpwnz	1.2%
SQLi-:::	1.0%

**33%**  
CUSTOM  
ATTACK



FIG. H

# FROM RECON TO BREACH: GLOBAL ROADMAP OF A COMPROMISE

Compromises and Breaches are often the result of sophisticated, multi-step, distributed attacks spanning numerous geographies

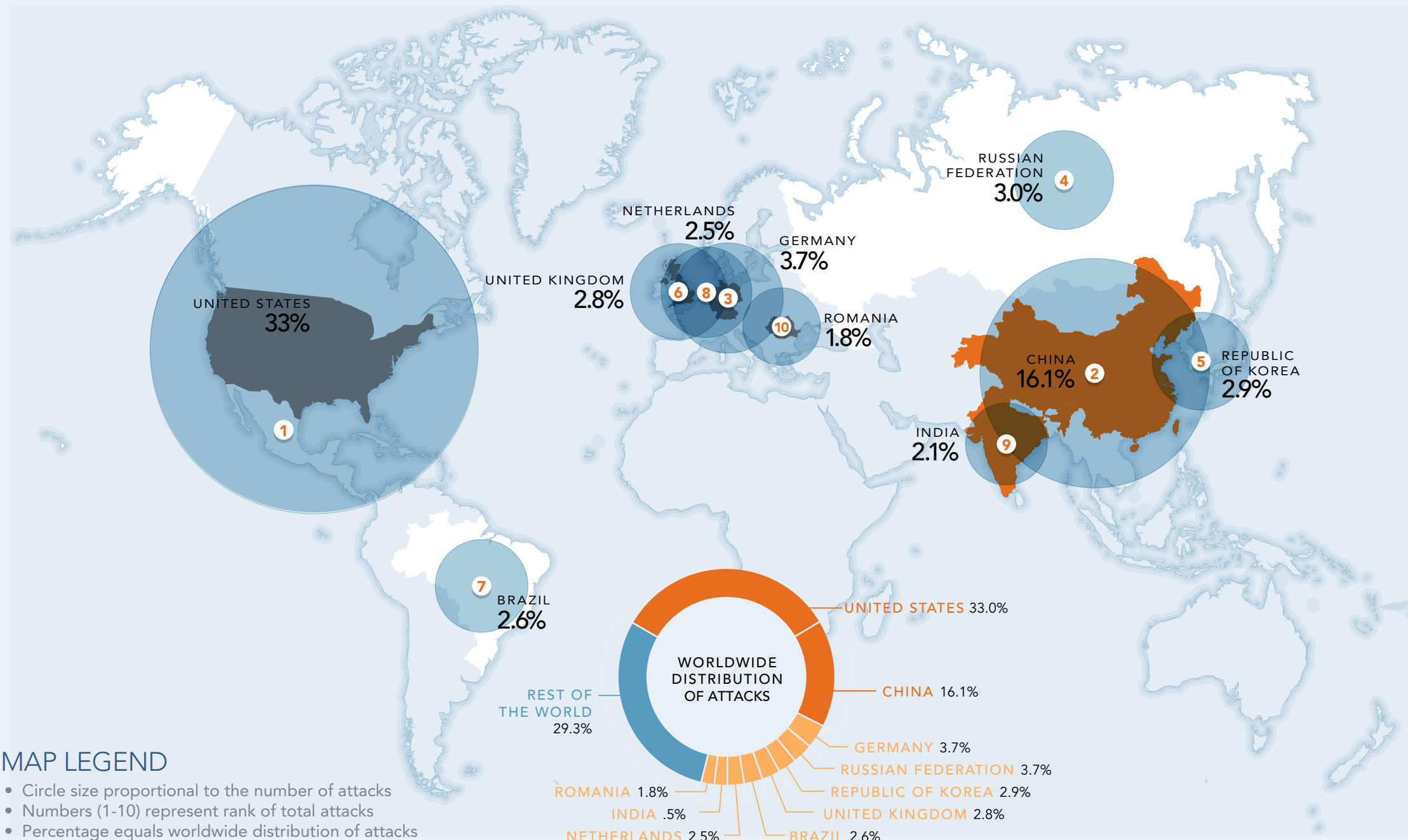
## TYPICAL ATTACK SEQUENCE



**Asia:** Initial reconnaissance and brute force attacks often originate from southeast Asia (notably China and India) to identify potential targets

**US and Europe:** Botnet farms proliferate in areas with deep broadband penetration, serving as launch pads for attacks

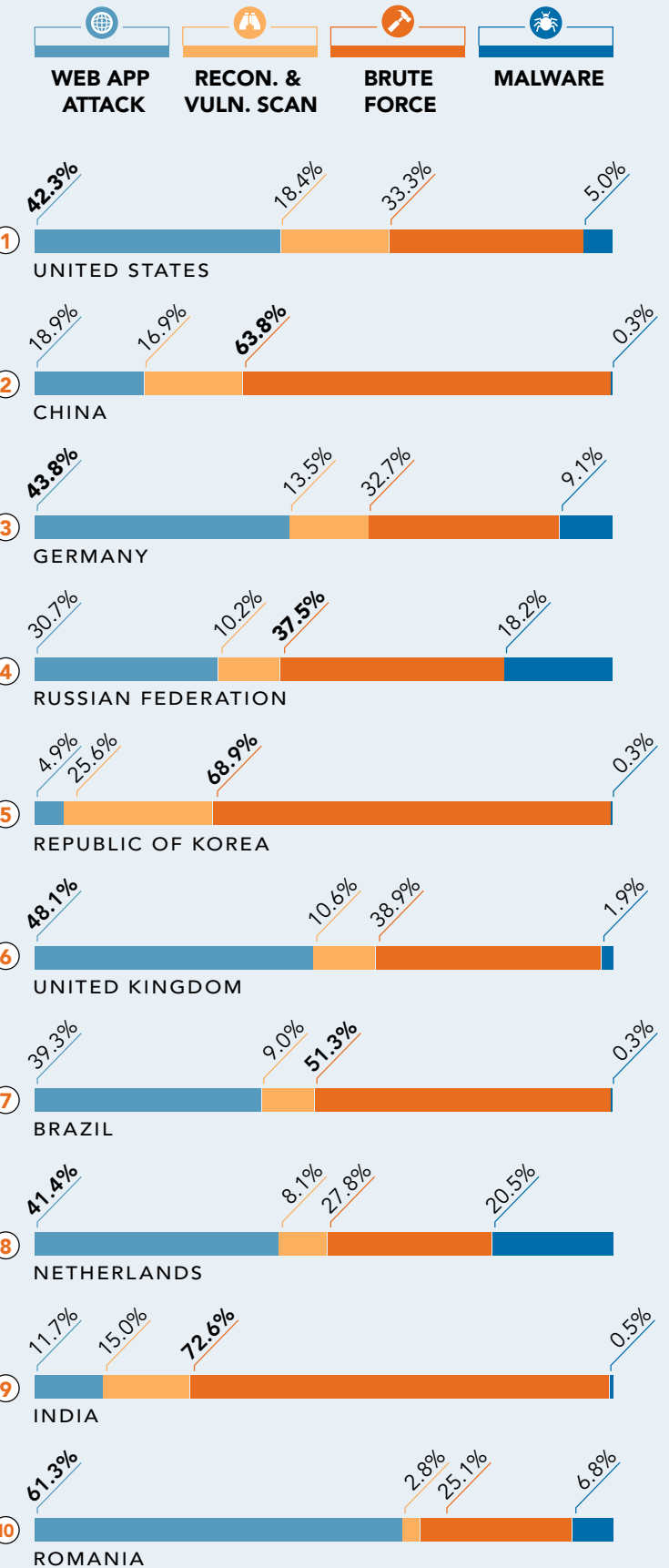
**US and Europe:** Attacks focus on accessing and exfiltrating valuable data such as personal information and payment records



### MAP LEGEND

- Circle size proportional to the number of attacks
- Numbers (1-10) represent rank of total attacks
- Percentage equals worldwide distribution of attacks

## DISTRIBUTION OF ATTACK TYPES



## WRAPPING UP

# The Data Tells the Story

---

In its initial *State of Cloud Security Report* (February 2012), Alert Logic found that differences in the types and frequency of incidents experienced in the on-premise and service provider environments did not align with general perceptions about cloud security. In fact, service provider environments showed lower occurrence rates than on-premise environments for every class of incident examined.

In this report, we find once again that the service provider environments where cloud infrastructure is hosted are not inherently less secure than on-premise environments.

With the addition of industry segmentation, Alert Logic finds that variations in threat activity among industries are less important than the environment where infrastructure is located. It is not safe to assume that one's industry is not targeted by attackers, or that an organization is too small to be targeted. Alert Logic's analysis suggests that attackers are using reconnaissance techniques to identify and exploit vulnerable targets wherever they can be found. Security planning should consider a range of technologies in order to provide defenses against these opportunistic threats. Alert Logic's analysis also demonstrates that attacks originate from all over the world, and simple geographic filtering is not a reasonable countermeasure.

The most significant finding of the report is the prevalence of Web application attacks. With the application vulnerabilities remaining commonplace and the growing availability and ease of use of automated attack tools, we expect to see the number of these attacks continue to rise, as they no longer require an especially skilled attacker. This observation is underscored by a study cited by analyst Ramon Krikken at the recent Gartner Security & Risk Management Summit. He noted a report showing that nearly one-third of all Web applications are vulnerable to SQL injection attacks, and recommended considering use of defense tools such as Web application firewalls (WAFs), along with secure application development practices.

Organizations should make sure that they use secure application development processes and tools to identify application vulnerabilities. Further, as Krikken cautioned,

given the high instance of cross-site scripting flaws, organizations need to go beyond relying on continuous development, testing and implementation of software patches—human interventions that are vulnerable to human error. Instead, they should consider active WAF technologies to block attacks. Access to security research and intelligence that informs security planning is also an important element of proactive defense.

Given the prevalence of unsophisticated attacks, such as brute force and reconnaissance, in both cloud and on-premise environments, and across all industries, the fundamentals apply: multi-layer security, close attention to basic management practices, such as patch management and upgraded operating systems, and use of monitoring and defensive technologies to identify and stop attacks.

When selecting cloud service providers, enterprises should consider the rigor and application of these fundamentals in their evaluation process. As we noted in the Spring 2012 *State of Cloud Security Report*, it is the quality of management applied to any IT environment that drives good security.



## Insight

The most significant finding of the report is the prevalence of Web application attacks.



## APPENDIX: Data Tables

### OCURRENCE: PERCENT OF CUSTOMERS EXPERIENCING SECURITY INCIDENTS

By Class of Incident Jul 2011 – Mar 2012	SERVICE PROVIDER	ON-PREMISE
Web Application Attack	53%	44%
Brute Force	39%	46%
Reconnaissance	38%	32%
Vulnerability Scan	30%	34%
Malware/Botnet	4%	36%
Application Attack	1%	18%
Misconfiguration	<1%	4%

### THREAT DIVERSITY: DISTRIBUTION OF UNIQUE THREATS

THREAT DIVERSITY	SERVICE PROVIDER	ON-PREMISE
0	22%	27%
1	28%	17%
2	23%	16%
3	19%	15%
4	7%	12%
5	1%	6%
6	0%	6%
7	0%	1%
Mean No. of Threat Classes Encountered	2.1	2.9

### FREQUENCY: NUMBER OF INCIDENTS PER IMPACTED CUSTOMER

By Class of Incident Jul 2011 – Mar 2012	SERVICE PROVIDER	ON-PREMISE
Web Application Attack	27.8	61.4
Brute Force	42.6	71.7
Vulnerability Scan	9.4	20.3
Malware/Botnet	6.1	28.6
Application Attack	9.9	11.3
Misconfiguration	2.4	2.9
Reconnaissance	2.7	40.0

### SERVICE PROVIDER PARTNERS INCLUDED IN STUDY

SERVICE PROVIDER PARTNER	WEBSITE
ATOS Origin	atos.net
CyrusOne	cyrusone.com
Datapipe	datapipe.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
Pulsant	pulsant.com
Rackspace	rackspace.com
Sungard Availability Services	sungardas.com
Visi	visi.com
Windstream	windstreambusiness.com

### TOP THREE INCIDENT CLASSES

SERVICE PROVIDER	ON-PREMISE
1. Web App. Attack (53%)	1. Brute Force (46%)
2. Brute Force (39%)	2. Web App. Attack (44%)
3. Reconnaissance (38%)	3. Malware/Botnet (36%)



## APPENDIX: Industry Data (top 5)

### IT SERVICES & CONSULTING: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	1.6%	10.5	11.2%	21.9
Malware/Botnet	3.9%	5.8	20.4%	48.6
Brute Force	36.2%	25.8	33.7%	218.4
Misconfiguration	0.4%	4.0	2.0%	6.0
Recon	33.9%	2.0	26.5%	18.7
Vulnerability Scan	24.9%	8.5	31.6%	29.5
Web App Attack	47.1%	17.6	36.7%	159.2

### E-COMMERCE/RETAIL: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	1.5%	1.0	13.5%	10.7
Malware/Botnet	3.8%	8.9	32.7%	27.8
Brute Force	38.7%	54.7	46.2%	46.1
Misconfiguration	0.4%	1.0	5.8%	1.0
Recon	34.6%	1.7	19.2%	129.5
Vulnerability Scan	33.1%	9.4	32.7%	30.2
Web App Attack	60.2%	29.5	38.5%	103.3

### MEDIA & ENTERTAINMENT: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	2.6%	4.7	31.3%	10.7
Malware/Botnet	2.6%	16.3	53.1%	14.2
Brute Force	30.2%	86.7	25.0%	66.4
Misconfiguration	0.00%	0.0	3.1%	4.0
Recon	40.5%	1.8	34.4%	4.0
Vulnerability Scan	37.1%	13.8	21.9%	19.9
Web App Attack	62.1%	53.0	31.3%	48.3

### SAAS/ONLINE SERVICES: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	1.0%	40.0	0.0%	0.0
Malware/Botnet	5.5%	5.0	20.0%	10.8
Brute Force	46.3%	45.1	40.0%	74.5
Misconfiguration	0.5%	5.0	0.0%	0.0
Recon	43.8%	4.5	35.0%	6.3
Vulnerability Scan	32.3%	10.5	30.0%	11.3
Web App Attack	51.2%	23.3	55.0%	44.9

**FINANCIAL SERVICES: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT**

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	0.7%	1.0	23.6%	4.1
Malware/Botnet	4.4%	2.7	43.1%	10.1
Brute Force	32.1%	20.9	44.4%	31.0
Misconfiguration	0.7%	1.0	4.2%	4.3
Recon	43.1%	1.6	31.9%	62.6
Vulnerability Scan	35.8%	6.2	31.9%	24.7
Web App Attack	50.4%	12.3	40.3%	17.4

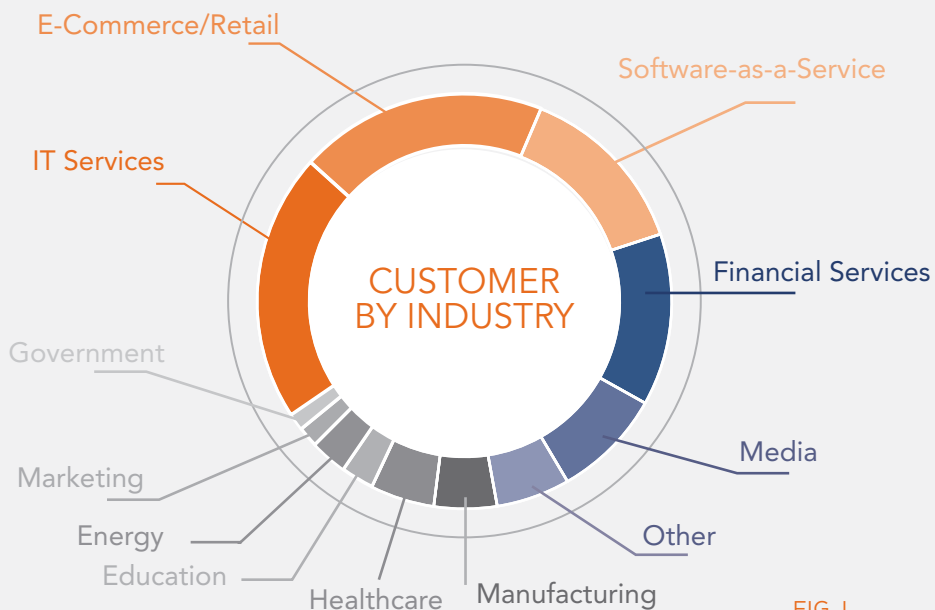


FIG. 1

## APPENDIX: Country Data

### ORIGINATING FROM THE UNITED STATES: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	0.5%	11.0	9.9%	4.7
Malware/Botnet	1.2%	3.3	26.8%	10.8
Brute Force	24.4%	16.8	23.3%	31.8
Recon	15.7%	1.9	11.4%	18.1
Vulnerability Scan	20.7%	7.5	21.3%	15.8
Web App Attack	38.8%	14.0	24.6%	35.4

### ORIGINATING FROM CHINA: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	0.1%	2.0	1.0%	1.8
Malware/Botnet	0.3%	1.0	3.5%	2.5
Brute Force	17.5%	22.4	20.5%	32.6
Recon	0.2%	49.7	4.8%	76.0
Vulnerability Scan	2.9%	6.3	11.1%	4.0
Web App Attack	21.4%	4.5	15.2%	17.1

**ORIGINATING FROM GERMANY: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT**

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	0.2%	3.0	3.5%	1.5
Malware/Botnet	0.5%	2.8	13.7%	4.3
Brute Force	11.9%	3.7	12.7%	6.9
Recon	0.2%	5.0	5.6%	5.6
Vulnerability Scan	5.7%	2.2	7.1%	2.8
Web App Attack	19.2%	3.8	12.9%	5.7

**ORIGINATING FROM THE RUSSIAN FEDERATION: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT**

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	0.0%	0.0	8.4%	2.2
Malware/Botnet	0.9%	1.9	19.8%	4.8
Brute Force	8.8%	4.8	10.6%	6.9
Recon	0.2%	6.7	2.8%	15.1
Vulnerability Scan	1.0%	1.4	3.8%	1.2
Web App Attack	10.0%	3.3	5.8%	11.0

**ORIGINATING FROM THE REPUBLIC OF KOREA: BY TYPE, SERVICE PROVIDER VS. ON-PREMISE ENVIRONMENT**

INCIDENT TYPE	SERVICE PROVIDERS		ON-PREMISE	
	Customers Impacted	Frequency	Customers Impacted	Frequency
App Attack	0.1%	1.0	0.8%	1.7
Malware/Botnet	0.0%	0.0	0.8%	2.0
Brute Force	12.0%	6.4	16.2%	8.0
Recon	3.7%	1.8	3.3%	21.6
Vulnerability Scan	2.0%	3.9	8.1%	2.8
Web App Attack	2.3%	1.6	2.8%	5.4



## **CONTRIBUTORS**

---

### **Lead Researcher**

Stephen Coty

### **Lead Analysts**

Michael Bentley

Tyler Borland

Mukul Gupta, PhD

Charles Tarun

### **Editors**

Maureen Rogers

John Whiteside



**ALERTLOGIC**

Security. Compliance. Cloud.

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

© Copyright 2012 Alert Logic, Inc. All rights reserved.

> [alertlogic.com](http://alertlogic.com)