ALERTLOGIC
Security. Compliance. Cloud.

# ALERT LOGIC CLOUD SECURITY REPORT

## Research on the Evolving State of Cloud Security

**Spring 2014**

# ALERT LOGIC CLOUD SECURITY REPORT

ALERTLOGIC
Security. Compliance. Cloud.

## Research on the Evolving State of Cloud Security

Spring 2014

EXECUTIVE SUMMARY

A LOOK AT THE DATA

KEY FINDINGS

FINDING NEW THREATS

WRAPPING UP

APPENDIX

ALERT LOGIC CLOUD SECURITY REPORT

# Executive Summary

ATTACKS

**INCREASED**

**ACROSS ALL INCIDENT TYPES**

in both on-premises and CHP environments.

## ENTERPRISES CONTINUE TO ADOPT CLOUD, FOCUS ON SECURITY

In early 2012, Alert Logic launched the first in a series of reports on cloud security, with the goal of creating the IT industry's first assessment of security in the cloud for businesses considering the use of cloud computing platforms. Alert Logic's approach to these assessments, based on data associated with a large concentration of cloud workloads—i.e., the Alert Logic customer base—has proven to be a pragmatic way of gaining insight into the evolving state of security in the cloud.

As cloud adoption grows, Alert Logic has observed a shift in security concerns. While cloud security remains a major concern, the business benefits of moving applications to the cloud are too compelling to resist. Now, having largely committed to a cloud strategy, IT professionals are redirecting their focus to finding the best ways to secure their cloud-based applications and data.

In the current *Cloud Security Report*, Alert Logic continues its practice of uncovering trends that threaten both cloud and on-premises environments. Two interesting observations have emerged. First, there has been an increase in attack frequency in both on-premises and cloud hosting provider (CHP) environments. Second, as more enterprise workloads move into cloud-hosted infrastructure, traditional on-premises infrastructure threats follow. These observations are intuitively consistent with the growing adoption of cloud services in the enterprise.

Insight

As **more enterprise** workloads move to the **Cloud**, traditional on-premises infrastructure **threats** follow.

### KEY FINDINGS FROM THE LATEST DATA SET

Drawing on security data obtained from both on-premises and CHP infrastructure end-users between April 1 and September 30, 2013, Alert Logic found the following:

- Attacks increased across all incident types, in both on-premises and CHP environments, with only one exception, suggesting more attacks of all types are occurring.

- CHP environments saw significant increases in attacks, with brute force attacks climbing from 30% to 44% of customers, and vulnerability scans increasing from 27% to 44%. These two types of incidents have historically been far more likely to target on-premises environments, but are now occurring at near-equivalent rates in both CHP and on-premises environments.
- Malware/botnet attacks, historically the most common attacks in the on-premises datacenter, are on the rise in CHP environments.

## CLOUD HONEYPOTS

In each edition of the *Cloud Security Report*, Alert Logic selects an area for additional investigation. For this report, we deployed honeypots in public cloud infrastructures around the world in order to observe the types and frequencies of attacks, and how the attacks vary geographically.

Key observations from honeypot data:

- The highest volume of attacks occurred in Europe, where honeypots experienced four times the number of attacks as the U.S., and double the number of attacks as Asia. Honeypots in Asia experienced more than twice as many attacks as those in the U.S.
- 14% of the malware collected through our honeypot network was considered undetectable by 51 of the world's top antivirus vendors.

## SUMMARY OF RESULTS

These results demonstrate that organizations moving to the cloud must implement enterprise-grade security solutions to protect their cloud workloads. These solutions must be cloud-deployable, and must contain advanced security content and analytics consistent with the attack vectors prevalent in the cloud. In other words, organizations cannot rely on legacy approaches to security to support their cloud infrastructure. They must find solutions that deliver protection specifically for the cloud.

## CLOUD HONEYPOTS:
Incident Attack Type by Region

For this *Cloud Security Report*, we deployed honeypots in public cloud infrastructures around the world.

### US HONEYPOTS

| | |
|---|---|
| Microsoft SQL Server | 12% |
| MySQL | 13% |
| HTTP | 23% |
| Microsoft DS Service | 51% |
| RPC | 0% |
| FTP | 0% |

### EUROPE HONEYPOTS

| | |
|---|---|
| Microsoft SQL Server | 13% |
| MySQL | 13% |
| HTTP | 13% |
| Microsoft DS Service | 35% |
| RPC | 13% |
| FTP | 13% |

### ASIA HONEYPOTS

| | |
|---|---|
| Microsoft SQL Server | 4% |
| MySQL | 6% |
| HTTP | 4% |
| Microsoft DS Service | 85% |
| RPC | 0% |
| FTP | 0% |

A LOOK AT THE DATA

# Alert Logic's Methodology

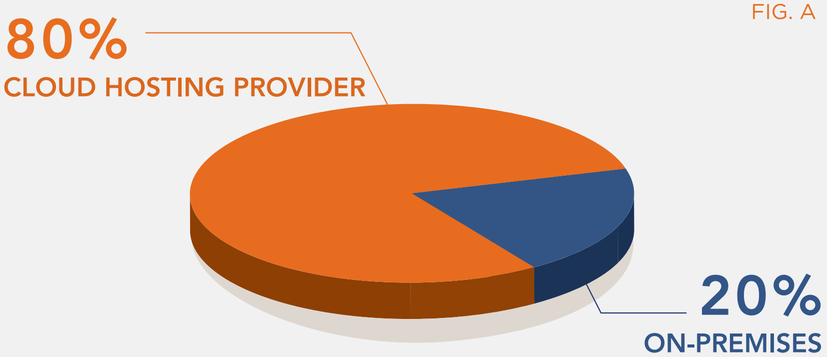
The data used in this report is from real-world security incidents captured in customer environments that are secured via Alert Logic's intrusion detection system (IDS)[1]. To correct for noise and false positives, Alert Logic utilizes a patented correlation engine that evaluates multiple factors to determine whether network-based events are authentic security incidents. Finally, a team of Global Information Assurance Certification (GIAC)-certified security analysts reviews each incident to ensure validity and to confirm the threat, further minimizing false positives.

Alert Logic regularly refines its threat detection process. This, along with the growing number of customers included in the analysis, means that comparisons between reports or time periods are only directionally valid.

Also in this report, honeypot data was gathered using low-interaction software that emulates a vulnerable OS. Common ports were left open to entice attackers to interact with the system. A low-interaction honeypot simulates services at a high level, is not a full operating system, and is typically easier to compromise than a hardened system. The type of activity observed in these instances is often from scripts, botnets, network probes, and malware installations that attempt to compromise the hosts/target. Alert Logic's honeypots monitored connections to common ports, and gathered statistics on IP, geo-location, and malware, if installed.

## ALERT LOGIC CUSTOMER DATA SET

FIG. A



ON-PREMISES? HOSTED? CLOUD?

### How Alert Logic categorizes its customer data

Alert Logic categorizes its data into two environments: on-premises (formerly called enterprise datacenter) and cloud hosting provider (CHP). On-premises customers own and manage their own IT infrastructure. CHP customers are an aggregation of customers utilizing solutions from a cloud or hosting partner, spanning from Infrastructure-as-a-Service to a managed or dedicated hosting environment. For a full list of the CHPs included in this report, see Appendix page 15.

[1] For future *Cloud Security Reports*, Alert Logic will incorporate security event and incident data from Alert Logic's Log Manager and Web Security Manager solutions to expand analysis and data sets.

## EVENT VS. INCIDENT

This report is based on 232,364 verified security incidents, identified from more than one billion events observed between April 1 and September 30, 2013. The customer set includes 2,212 organizations across multiple industries, located primarily in North America and Western Europe. CHP environments account for 80% of the customers, while the remaining 20% represent on-premises datacenters. Alert Logic categorizes an event as evidence of suspicious behavior detected via an IDS signature, and defines an incident as an event or group of events that has been confirmed as a valid threat based on advanced automated analysis by Alert Logic's correlation engine, and verification by certified analysts. Alert Logic also applied this data set to a year-over-year comparative analysis with the two previous six-month data sets.

## INCIDENT CLASSIFICATIONS

### Malware/Botnet

Malicious software installed on a host and engaging in unscrupulous activity, data destruction, information gathering or creation of backdoors.

### Brute Force

Exploit attempts enumerating a large number of combinations, typically involving multiple credential failures, in hopes of finding a weak door.

### Vulnerability Scan

Automated vulnerability discovery in applications, services or protocol implementations.

### Web App Attack

Attacks targeting the presentation, logic or database layer of web apps.

### Recon

Activity focused on ping sweeps, mapping networks, applications and/or services.

### App Attack

Exploit attempts against applications or services not running over HTTP protocol.

## INCIDENT METRICS

### Incident Occurrence

Percentage of customers experiencing a specific class of incident at least once during the study period. Provides a view of the probability of attack.

### Incident Frequency

Average number of incidents of each type per impacted customer. Provides an understanding of attacker persistence and tenacity.

### Threat Diversity

Average number of unique incident types (of the six classes reviewed) encountered by impacted customers in each environment. Provides a view of the sophistication required of a security program.

KEY FINDINGS:

# The Enterprise Cloud

Between 2013 and 2017,

PUBLIC IT CLOUD COMPUTING

spending will experience a compound annual growth rate of

23.5%

Web application attacks, brute force attacks, and vulnerability scans each impact

44%

of the cloud hosting customer base.

One of the most significant technology stories over the past several years has been the broad and rapid adoption of cloud computing as a viable platform. The majority of enterprises already have a formal cloud strategy in place, and analysts estimate that the growth rate of spending on cloud computing will soon exceed that of on-premises IT by a multiple of four to six. In September 2013, International Data Corporation (IDC)[2] predicted that, between 2013 and 2017, spending on public IT cloud computing will experience a compound annual growth rate of 23.5%. By 2017, IDC believes the spending on public IT cloud services will account for one-sixth of overall IT product spending, and will be responsible for almost half of all increases in the applications, system infrastructure software, platform as a service, and basic storage categories.

Other analysts concur. At its October 2013 Symposium/IT Expo, Gartner[3] forecasted that, by 2016, the bulk of new IT spending will be cloud-based rather than on-premises.

Widespread acceptance of cloud computing in enterprise IT increases the need to secure cloud infrastructure in a way that rivals protection of the traditional datacenter. To meet this requirement, IT and security professionals must understand two key dimensions—the types of threats targeting cloud computing environments, and whether traditional security technologies can perform effectively in cloud environments.

Since 2011, Alert Logic has been analyzing incident data to identify the differences between on-premises and CHP environments. Alert Logic's production environment monitors and analyzes the security of data and systems in both on-premises datacenters and CHPs (where public, private and hybrid cloud infrastructure is hosted). After examining actual incident data, our first *Cloud Security Report* in February 2012 demonstrated that fears of the cloud being inherently insecure could largely be put to rest. While we uncovered variances between the two environments with respect to the types of incidents observed, these differences related largely to the types of workloads deployed and the diversity of infrastructure employed. Subsequent reports have reinforced these findings and conclusion.

## LATEST DATA SET

The data analyzed for this *Cloud Security Report* continues to underscore the conclusion that the cloud is not inherently less secure than traditional on-premises environments. It also reveals an interesting new set of observations. The key findings here are that attacks seem to be increasing across all environments, and, in parallel, the types of attacks experienced in the cloud are increasingly consistent with the types of attacks experienced in

[2] http://www.idc.com/getdoc.jsp?containerId=prUS24298013
[3] http://www.gartner.com/newsroom/id/2613015

FIG. B

## INCIDENT OCCURRENCE: PERCENT OF CUSTOMERS IMPACTED

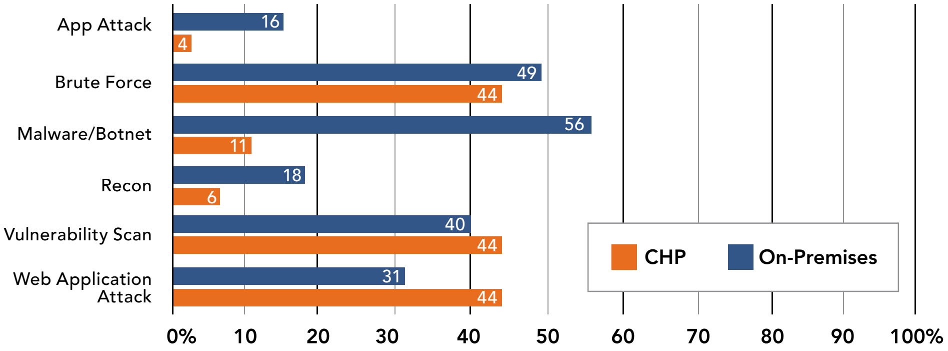


FIG. C

## TOP THREE INCIDENT CLASSES

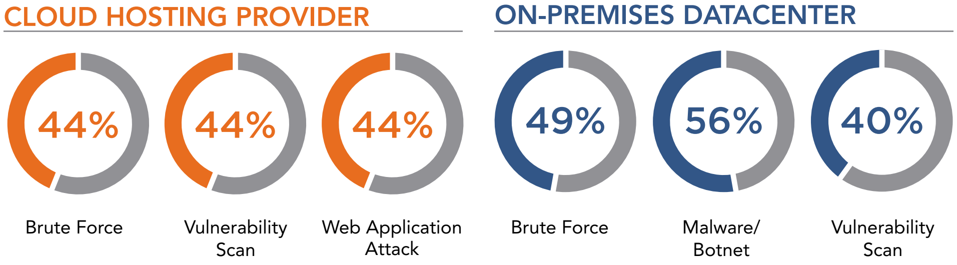
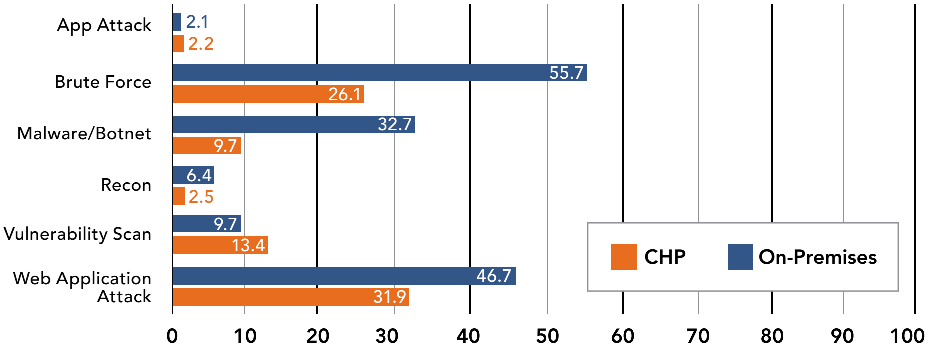
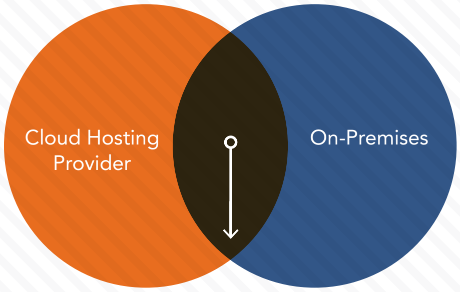


FIG. D

## INCIDENT FREQUENCY: AVERAGE NUMBER OF INCIDENTS PER IMPACTED CUSTOMER



## WHAT WE SEE ACROSS ALL ENVIRONMENTS



### 01

Brute force attacks and vulnerability scans are now occurring at near-equivalent rates in both cloud and on-premises environments.

### 02

Malware/Botnet attacks, historically the most common attacks in the on-premises datacenter, are on the rise in CHP environments

### 03

Application, malware/botnet and recon attacks remain much more likely to occur on-premises than in CHP environments.

## KEY FINDINGS:

# The Enterprise Cloud (cont'd)

on-premises environments. In previous editions of the *Cloud Security Report*, in addition to quantifying attacks in both on-premises and CHP environments, we documented differences in attack types between the two types of environments. This most recent data is showing a convergence in attack types between on-premises and CHP environments. Our hypothesis is that the reason for this convergence is the fact that traditional enterprise workloads are increasingly moving to the cloud.

Even so, there remains some diversity in attack types between CHP and on-premises environments. Web application attacks, brute force attacks, and vulnerability scans were the most pronounced attacks experienced in CHP environments, each impacting 44% of the cloud hosting customer base. Malware/botnet attacks (56%) and brute force attacks (49%) were the most prominent threat vectors in on-premises datacenter environments. And while application attacks, malware/botnet attacks and recon attacks remain much more likely to occur on-premises than in CHP environments, the rates of occurrence of web application attacks and vulnerability scans in CHP environments exceed those in on-premises environments by 13% and 4%, respectively.

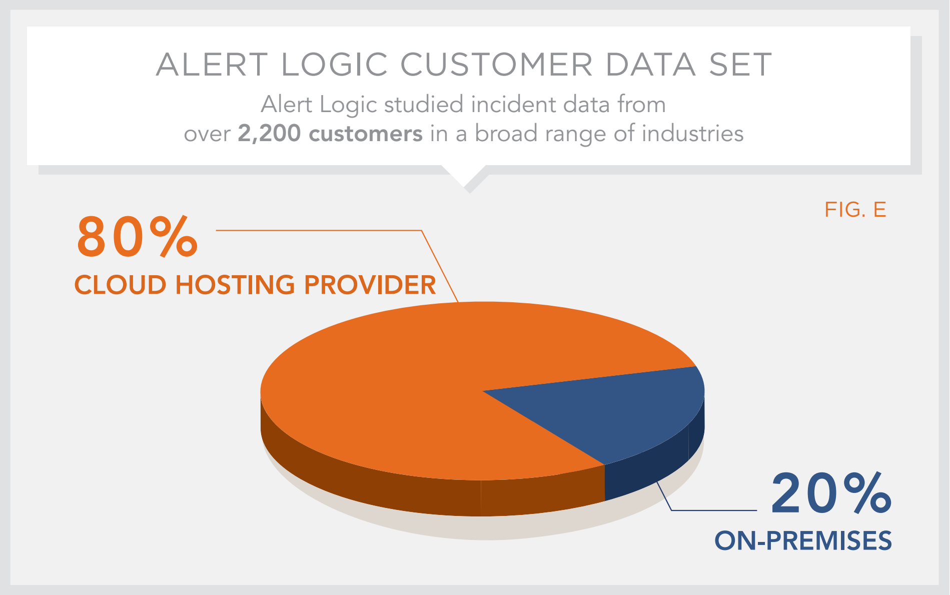
For impacted customers, i.e., those that were the target of an attack, the frequency of attack in most categories was also generally greater among on-premises customers. Overall, threat diversity (the average number of distinct incident classes encountered by impacted customers among the six categories reviewed) is roughly equivalent in both the CHP and on-premises environments.

## TRENDS OVER TIME: CLOUD HOSTING VS. DATACENTER

From the macro view, Alert Logic saw incidents increase across both environments. On-premises environments are still more likely to be attacked than cloud environments, but there has been a consistent increase in cloud attacks as well. As cloud adoption continues to accelerate, brute force attacks—which increased in on-premises environments as well—have surged among CHPs, likely due to the increasing presence of "theft-worthy" data in the cloud. Vulnerability scans, typically coupled with brute force attacks in terms of attack style and process, increased dramatically in both environments. The percentage of customers impacted by vulnerability scans increased from 27% to 44% among CHPs, and from 28% to 40% in on-premises datacenters. Malware/botnet attacks, highly prevalent in the desktop-rich on-premises datacenter environment, remain relatively low among CHPs. They

### Key Observations

**Cloud environments** require **more sophisticated** security programs than in prior years.


ALERT LOGIC CUSTOMER DATA SET

Alert Logic studied incident data from over **2,200 customers** in a broad range of industries

FIG. E

have, however, more than doubled, which could be attributed to cloud-based virtual desktop infrastructure, mobile applications, or end-point applications.

In the Spring 2013 *Cloud Security Report*, Threat Diversity was 1.8 and 2.5 for CHP and on-premises, respectively. While threat diversity for on-premises customers was unchanged when compared to the 2013 report, it rose to 2.3 in cloud environments based on growing workloads. This growth in threat diversity is another indicator that cloud environments now require more sophisticated security programs than in prior years.

FIG. F

INCIDENT OCCURRENCE OVER TIME:
CLOUD HOSTING PROVIDERS

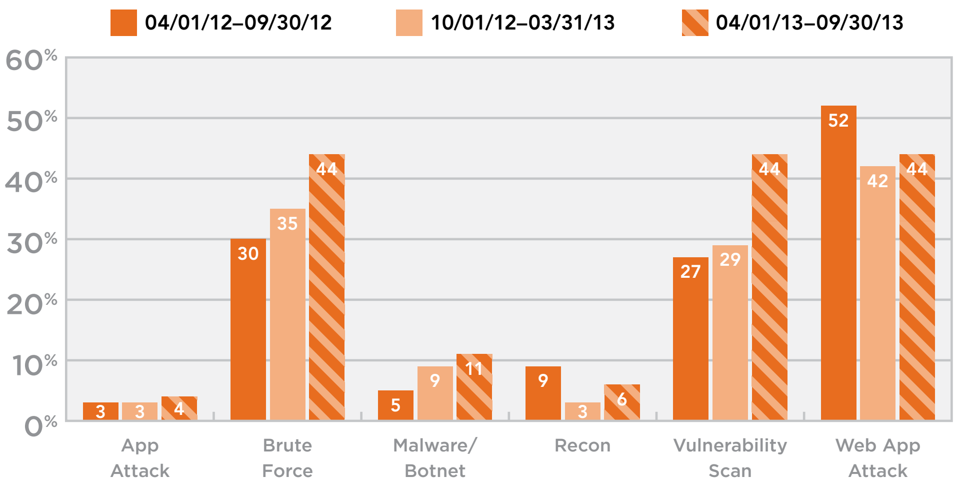
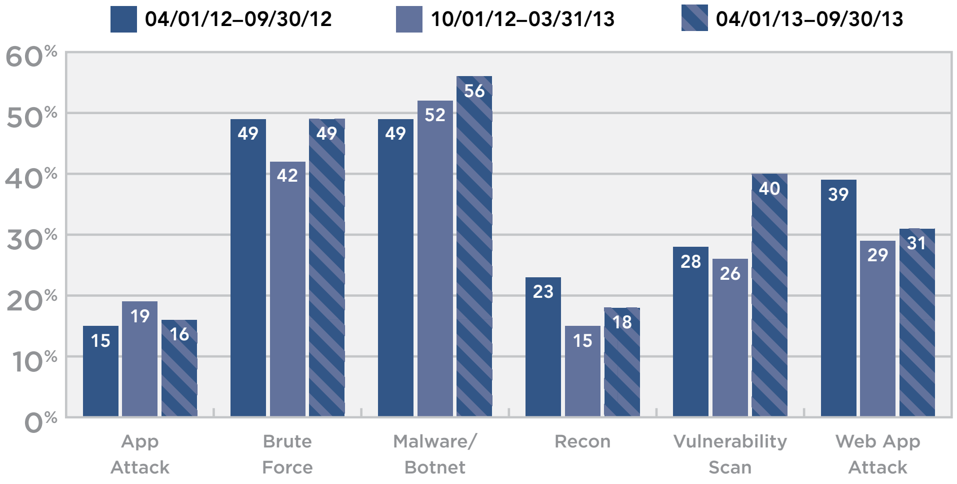


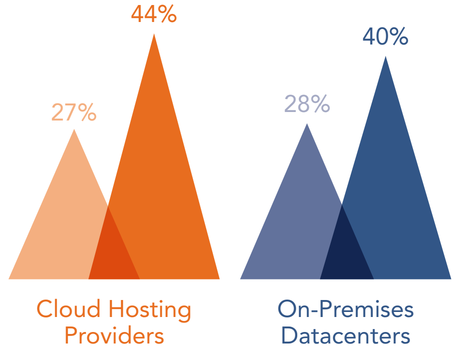
FIG. G

INCIDENT OCCURRENCE OVER TIME:
ON-PREMISES



BRUTE FORCE ATTACKS which increased in on-premises environments as well—have surged among CHPs, likely due to the increasing presence of **"THEFT-WORTHY"** data in the cloud.

Vulnerability scans increased in both environments:



FINDING NEW THREATS:

# Cloud Honeypots

## CLOUD HONEYPOTS

A honeypot is a decoy system configured to be intentionally vulnerable, deployed to gather information about attackers and their exploitation methods. While honeypots are not typically the target of highly sophisticated attacks, they are subject to many undefined attacks, and provide a window into the types of threats being launched against the cloud.

**Honeypots allow researchers to:**

- Collect new and emerging malware
- Identify the source of the attacks
- Determine attack vectors
- Build a profile of the target industry if using specific industry domains

Honeypots are also deployed in the corporate space to find attacks that hit a particular company and/or industry. These honeypots are built on the edge of a corporate network, and made deliberately vulnerable so that they will be compromised.

**Data collected:**

- Provides detail on the IP addresses of the source location
- Identifies malware in order to reverse engineer
- Creates signature content for protecting the application stack—network, systems, and application—via IDS, log analytics, and web application firewalls
- Provides insight into the types of attacks and associated characteristics

In order to uncover attack trends in the cloud, Alert Logic deployed honeypots in public cloud infrastructures around the world to observe the types and frequencies of attacks, as well as how the attacks vary geographically.

Overall, the highest volume of attacks occurred in Europe, where honeypots had four times the number of attacks as the U.S., and double the number of attacks as Asia. This is likely due to the presence of highly organized crime circuits, which are basically malware factories, in Russia and Eastern Europe. Malware produced in these "factories" is typically tested in Europe before deployment in the U.S. Similarly, honeypots in Asia experienced more than twice as many attacks as those in the U.S. This finding came as something of a surprise, given that the U.S. is generally considered a more valuable target.

Worldwide, attacks on Microsoft-DS (Port 445) accounted for the majority (51%) of honeypot incidents. Microsoft-DS (port 445) supports direct hosted "NetBIOS-less" SMB traffic and file-sharing in Windows environments, and it represents an easy target, when open, for accessing files and providing the ability to infect systems. The remainder of the attacks was split relatively evenly among Microsoft-SQL (Port 1433), MySQL (Port 3306), HTTP (Port 443), RPC (Port 135) and FTP (Port 21).

When disaggregated by region, the honeypot data tell a more nuanced story. In Asia, the preponderance of attacks (85%) targeted Microsoft-DS. This is likely attributable to the large amount of pirated (and unpatched) Microsoft software in use in this region. In contrast to other areas, a significant proportion of attacks (23%) in the U.S. were made on HTTP. This is perhaps because the U.S. in general has more widespread web adoption, and hosts more web and cloud services than other countries[4].

Also, 14% of the malware collected through the honeypot network was considered not detectable by 51 of the world's top antivirus vendors. This does not mean that the malware is considered a zero-day; rather it indicates that a malicious attacker repackaged an older variant of malware such as Zeus or Conficker.

While highly sophisticated attacks are unlikely to be launched against honeypot environments, analyzing honeypot data enables us to monitor the types of threats being launched against the cloud, such as the types of malware being deployed, and what specific layers are being attacked (e.g., the operating system, databases). In some instances, looking at honeypot data provides an early-warning system for new malware, or emerging variations of old malware, such as Conficker. By having a better understanding of what attacks are trying to exploit, and how, Alert Logic

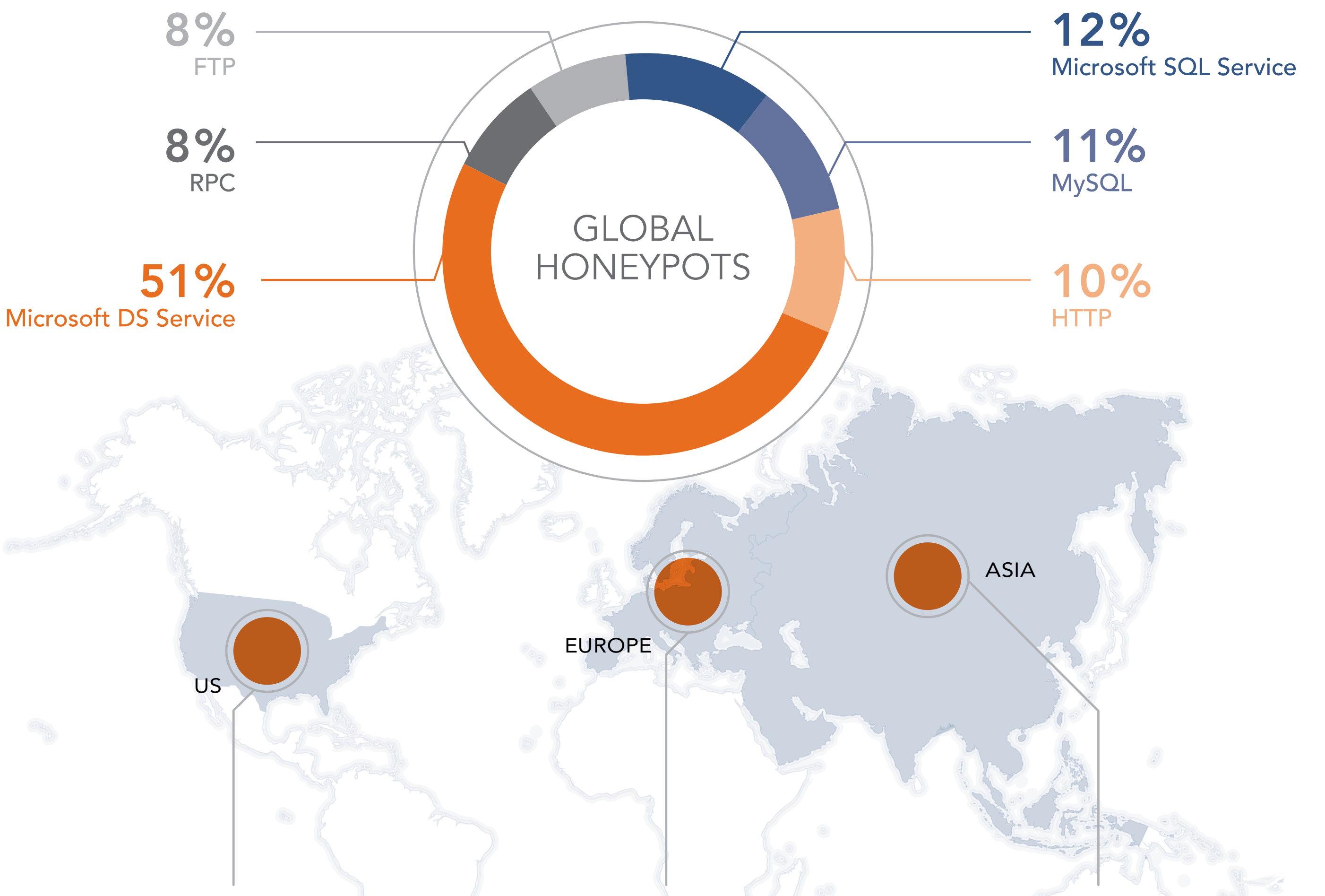
[4] http://venturebeat.com/2013/10/23/where-the-worlds-top-100000-websites-are-hosted-infographic

is better able to tune security content to appropriately detect and protect against new attacks in the cloud. In addition, the use of honeypots provides additional visibility into what security solutions are best suited to defend against these types of attacks.

The bottom line is the honeypot results clearly indicate that an organization moving to the cloud must understand and pay close attention to their security and compliance requirements, and appropriately source a solution.

## TOTAL HONEYPOT ATTACKS BY REGION

FIG. H



### US HONEYPOTS

| | |
|---|---|
| Microsoft SQL Server | 12% |
| MySQL | 13% |
| HTTP | 23% |
| Microsoft DS Service | 51% |
| RPC | 0% |
| FTP | 0% |

### EUROPE HONEYPOTS

| | |
|---|---|
| Microsoft SQL Server | 13% |
| MySQL | 13% |
| HTTP | 13% |
| Microsoft DS Service | 35% |
| RPC | 13% |
| FTP | 13% |

### ASIA HONEYPOTS

| | |
|---|---|
| Microsoft SQL Server | 4% |
| MySQL | 6% |
| HTTP | 4% |
| Microsoft DS Service | 85% |
| RPC | 0% |
| FTP | 0% |

WRAPPING UP:

## The Data Tells the Story

Despite apprehension about security risks, mass adoption of cloud platforms continues to grow, and with it comes an increase in attacks. Overall, the data presented in this edition of the *Cloud Security Report* indicates that the threats in the cloud are growing in two dimensions: the total number of attacks is increasing, and attacks that were historically directed at on-premises environments are now moving to the cloud. Although, comparatively, on-premises environments are more frequent targets, this should not undermine the fact that attacks directed at CHPs have increased significantly and are expected to continue at a rate that matches the accelerated pace of cloud adoption and the continued migration of more valuable workloads to the cloud.

Whether looking at attacks in on-premises or cloud hosting environments, whether analyzing production environments or pure research honeypots, across the spectrum we see the volume and persistence of attacks continuing to increase.

As these attacks increase in persistence, they are also increasing in sophistication. The threat diversity for the cloud has increased to rival that of on-premises environments. And new threats uncovered by our honeypot research demonstrate how top antivirus software vendors cannot be solely relied upon to detect attacks. The continued focus by hackers on infiltrating IT infrastructure underscores the importance of adopting the right security procedures and tools, and of continuously evaluating and adjusting those procedures and tools as attackers find new ways to thwart defense.

### WHERE TO GO FROM HERE

To enjoy the benefits of the cloud without security compromise, organizations must understand the different roles and responsibilities that exist between a CHP and the company deploying their own (or third-party) applications in the cloud. CHPs deliver core security from their datacenters up to specific layers (e.g., the hypervisor for the compute layer). Responsibility for the application and its underlying host/operating system and network falls to the customer. This makes it an absolute necessity that customers educate themselves on their business and application requirements for security and compliance, map these requirements to the right CHPs, and source the right products and build the right processes to manage events, incidents and ongoing security in the cloud. It's also important to note that cloud providers differ in their default security settings. Some take an "all doors closed" approach, while others default to requiring users to define their own security (i.e., there is no security protection by default).

### Key Observation

Cloud providers **differ** in their default security settings. Some take an **"all doors closed" approach**, while others default to **requiring users to define their own security**.

As attackers adjust their attack postures, organizations must respond across the spectrum. Cloud environments are designed to operate differently than legacy enterprise architectures (e.g., with respect to network architecture, provisioning, and scaling). It is important to find proven cloud security solutions to protect mission critical applications, confidential data, and the underlying infrastructure that supports those applications, including network, compute, database, and identity management. An overall solution should address:

- Network: Firewall, Intrusion Detection, and Vulnerability Scanning provide detection and protection, while also lending visibility into security health.
- Compute: Anti-Virus, Log Management and File Integrity Management protect against known attacks, provide compliance and security visibility into activity within an environment, and understand when files have been altered—maliciously or accidentally.
- Application: A Web Application Firewall will protect against the largest threat vector in the cloud: web application attacks. Encryption technologies are ubiquitous for data in-flight protection, and some companies select encryption for data-at-rest when necessary, assuming applications can support it.
- Application Stack: Security Information Event Management (SIEM) can address the big data security challenge by collecting and analyzing all data sets. When deployed with the right correlation and analytics, this can deliver real-time insight into events, incidents, and threats across a cloud environment.

The design and configuration of these types of services will be driven by requirements, including an organization's security and compliance standards, application and data sensitivity, risk assessment, and the policies implemented by the service providers an organization selects.

## EDUCATION FOR THE REST

While the cloud delivers many benefits including agility, performance, scalability, and cost management, organizations that have historically been less security conscious or technically sophisticated, along with those whose security expertise does not include cloud-specific security solutions, can be at risk if they do not properly research their deployment requirements and find proven solutions. Organizations must also factor in the rise of "Shadow IT." "Shadow IT" is defined as individual employees and business groups deploying applications in the cloud that have not yet been vetted by IT to ensure the organization's security and compliance standards are met. Given this, security consciousness and standards need to be raised throughout the enterprise to balance the value of the cloud with the requirements of good security and compliance. An organization's security posture must extend from edge devices to the heart of the business—the datacenter—whether that datacenter is on-premises, within the cloud, or hybrid.

APPENDIX:

# Data Tables

## Incident Occurrence/Frequency Table

Alert Logic Customers | April 1, 2012–September 30, 2013

### CLOUD HOSTING PROVIDER (CHP) VS. ON-PREMISES

| INCIDENT CLASS | CLOUD HOSTING PROVIDER | | ON-PREMISES | |
|---|---|---|---|---|
| | Customers Impacted | Frequency | Customers Impacted | Frequency |
| App Attack | 4% | 2.2 | 16% | 2.1 |
| Brute Force | 44% | 26.1 | 49% | 55.7 |
| Malware/Botnet | 11% | 9.7 | 56% | 32.7 |
| Recon | 6% | 2.5 | 18% | 6.4 |
| Vulnerability Scan | 44% | 13.4 | 40% | 9.7 |
| Web App Attack | 44% | 31.9 | 31% | 46.7 |
| Threat Diversity | 2.3 | | 2.5 | |

### INCIDENT TYPES OVER TIME

| INCIDENT TYPES | APRIL 1, 2012–SEPTEMBER 30, 2012 | | OCTOBER 1, 2012–MARCH 31, 2013 | | APRIL 1, 2013–SEPTEMBER 30, 2013 | |
|---|---|---|---|---|---|---|
| | CHP | On-Premises | CHP | On-Premises | CHP | On-Premises |
| App Attack | 3% | 15% | 3% | 19% | 4% | 16% |
| Brute Force | 30% | 49% | 35% | 42% | 44% | 49% |
| Malware/Botnet | 5% | 49% | 9% | 52% | 11% | 56% |
| Recon | 9% | 23% | 3% | 15% | 6% | 18% |
| Vulnerability Scan | 27% | 28% | 29% | 26% | 44% | 40% |
| Web App Attack | 52% | 39% | 42% | 29% | 44% | 31% |

## TOTAL HONEYPOT ATTACKS BY REGION

| INCIDENT TYPES | ASIA | | US | | EUROPE | |
|---|---|---|---|---|---|---|
| | Attacks | Percentage | Attacks | Percentage | Attacks | Percentage |
| HTTP | 19,639 | 4% | 52,191 | 23% | 126,906 | 13% |
| mySQL | 28,675 | 6% | 30,145 | 13% | 127,622 | 13% |
| SQL Server | 21,235 | 4% | 26,800 | 12% | 126,518 | 13% |
| SMB | 407,754 | 85% | 114,252 | 51% | 340,502 | 35% |
| RPC | 2,699 | 1% | 1,047 | 0% | 125,997 | 13% |
| FTP | 160 | 0% | 86 | 0% | 125,917 | 13% |

## Service Provider Partners Included In Study

| SERVICE PROVIDER PARTNER | WEBSITE | SERVICE PROVIDER PARTNER | WEBSITE |
|---|---|---|---|
| **Amazon Web Services (AWS)** | aws.amazon.com | **Microsoft Azure** | azure.microsoft.com |
| **Atos Origin** | atos.net | **MegaPath** | megapath.com |
| **CyrusOne** | cyrusone.com | **NaviSite** | navisite.com |
| **Datapipe** | datapipe.com | **PEER 1 Hosting** | peer1.com |
| **Dimension Data** | dimensiondata.com | **Pulsant** | pulsant.com |
| **HOSTING** | hosting.com | **Rackspace** | rackspace.com |
| **Hostway** | hostway.com | **RigNet** | rig.net |
| **Internap** | internap.com | **Rook Consulting** | rookconsulting.com |
| **Latisys** | latisys.com | **Sungard Availability Services** | sungardas.com |
| **Layered Tech** | layeredtech.com | **VISI** | visi.com |
| **Logicworks** | logicworks.net | **Windstream Communications** | windstreambusiness.com |

ALERTLOGIC
Security. Compliance. Cloud.

CONTRIBUTORS

**Lead Researcher**
Stephen Coty

**Lead Analysts**
Patrick Snyder
Kevin Stevens

**Editors**
Rahul Bakshi
Maureen Rogers
Sheridan Scott

ALERTLOGIC

Security. Compliance. Cloud.

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

**UK OFFICE**
1 Farnham Rd
Guildford
Surrey
GU2 4RG
United Kingdom