ALERTLOGIC
Security. Compliance. Cloud.

TARGETED ATTACKS AND OPPORTUNISTIC HACKS

State of Cloud Security Report

Spring 2013

TARGETED ATTACKS AND OPPORTUNISTIC HACKS

State of Cloud Security Report

Spring 2013

STATE OF CLOUD SECURITY REPORT

Executive Summary

WEB APPLICATION ATTACKS REMAIN THE

MOST

SIGNIFICANT THREAT
for CHP environments.

1 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 as needed.

Insight

Cloud skeptics take note: These conclusions appear to be **reliable guideposts** for those deciding **when** and **how** to **move infrastructure** to the cloud.

CLOUD VS. ENTERPRISE DATA CENTER SECURITY

WHAT THE REAL-WORLD DATA CONTINUES TO TELL US

In a relatively short time, cloud computing, specifically Infrastructure-as-a-Service, has shifted from a new but unproven approach to an accepted, even inevitable, model. Driven by flexibility and efficiency, the question facing most organizations is not whether the cloud is part of their infrastructure plans, but which applications and workloads to move to the cloud and when. But even as the benefits of cloud and hosted models have become apparent, concerns persist about security, and an assumption lingers that the cloud is inherently less secure than an enterprise data center environment.

Alert Logic's *State of Cloud Security Report* tests this assumption by examining and comparing threat data from enterprise data centers and cloud hosting provider (CHP) environments where public, private and hybrid cloud infrastructure is hosted. The data, drawn from the production environments of Alert Logic's customers, provides insight into the attacks taking place in real-world settings, as opposed to theoretical conclusions driven from honeypot networks or simulated user environments. In February 2012, the first report in the series examined the occurrence and frequency of security incidents in both types of environments, as well as the overall threat diversity encountered in each. The Fall 2012 report followed suit.

For this latest update, Alert Logic examined six months of new data and again confirmed the findings of its earlier reports:

- The cloud is not inherently less safe than the enterprise data center environment.
- Attacks in CHP environments tend to be "crimes of opportunity" while those in enterprise data centers tend to be more sophisticated and targeted.
- Web application attacks are a significant threat vector in both environments.

The relative occurrence and frequency of incidents between CHP and enterprise data center environments has been largely consistent, with no major shifts in incident patterns over the past two years.

MORE THAN

45,000

SECURITY INCIDENTS

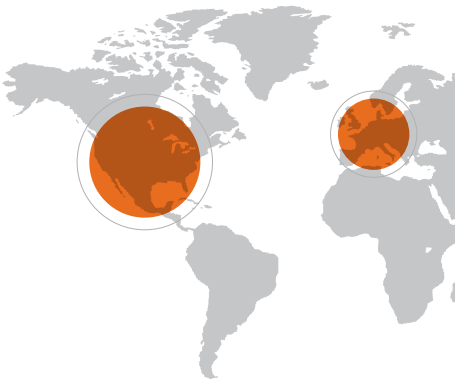
were verified and observed among Alert Logic customers between April 1 and September 30, 2012.

THE CUSTOMER SET INCLUDES

1,801

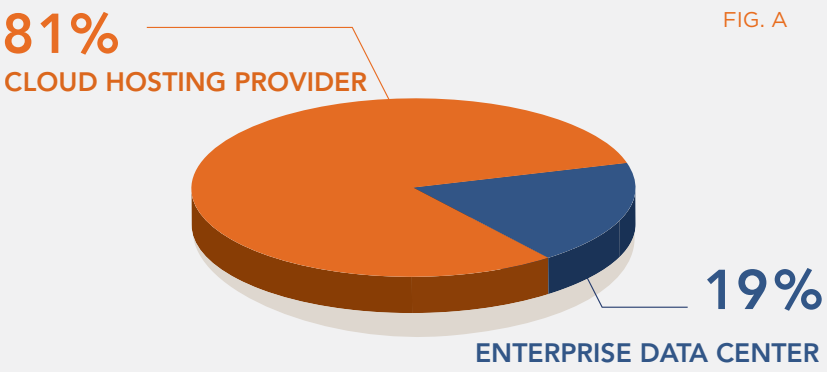
ORGANIZATIONS

across multiple industries, located primarily in North America and Western Europe.



ALERT LOGIC CUSTOMER DATA SET

FIG. A



ENTERPRISE? HOSTED? DATA CENTER? CLOUD?

How Alert Logic categorized its customer data

Alert Logic categorizes its data into two environments: enterprise data center and cloud hosting provider (CHP). Enterprise data center customers own and manage their own IT infrastructure. CHP customers are an aggregation of all customers utilizing Infrastructure-as-a-Service solutions from a CHP, spanning from the elastic cloud to managed or dedicated hosted environments. For a full list of the CHPs included in this report, see Appendix page 17.

KEY FINDINGS:

Incident Occurrence, Incident Frequency, Threat Diversity

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

Incident Occurrence
Percentage of customers experiencing a specific class of incident at least once during the study period.
Importance: Provides a view of probability of being attacked.

Incident Frequency
Average number of incidents of each type, per impacted customer.
Importance: 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.
Importance: Provides a view of the sophistication required of a security program.

Insight

Web application attacks remain the **most significant threat** for **Cloud Hosting Provider environments.**

INCIDENT OCCURRENCE

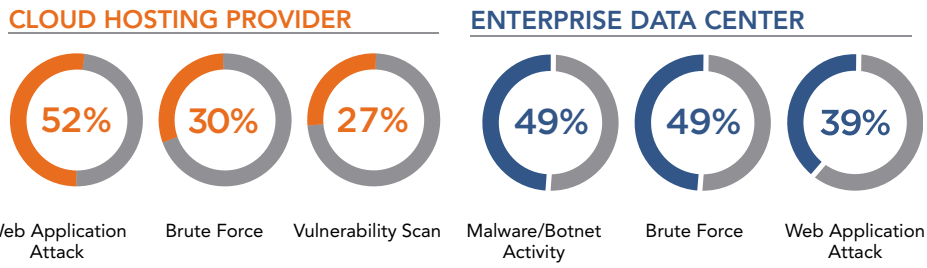
Web application attacks remain the most significant threat for CHP environments (52 percent of customers impacted). They also represent a substantial threat in enterprise environments (impacting 39 percent of customers). *This is the only threat category in which a higher proportion of CHP customers are impacted than enterprise data center customers.* The majority of these attacks are perpetrated using common and freely available tools, such as Havij, which enable less sophisticated hackers to easily launch attacks.

It is not a surprise that brute force is a leading attack vector—30% of CHP environments and 49% of enterprises experienced incidents—as it represents a tried and true technique where persistence pays off. For much the same reason, we observed a high occurrence of vulnerability scans (27% CHP, 28% enterprise).

Enterprise environments are more likely to be struck by targeted rather than opportunistic attacks. Given all of the concerns around security in the cloud, enterprise data centers still house most of an organization's high-value data—intellectual property, trade secrets, sensitive personal information—making them attractive targets for purposeful, criminal attacks. An example of targeted attacks: malware/botnet, which is far more prevalent in workstation-heavy enterprise data center environments, where 49% experienced attacks vs. only 5% in CHP environments.

FIG. B

INCIDENT OCCURRENCE:
TOP THREE INCIDENT CLASSES

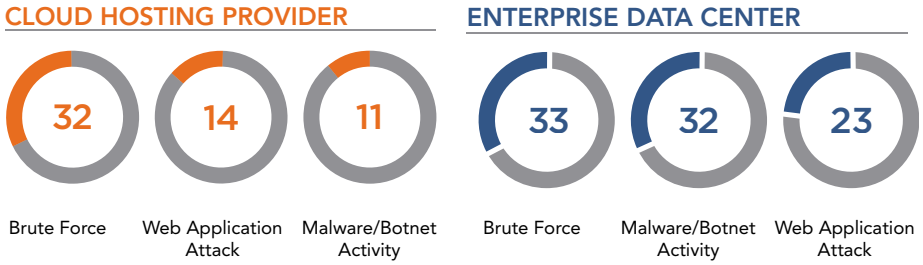


INCIDENT FREQUENCY

Since brute force often involves trying many different credential combinations and is serial by nature, it is not surprising that the average frequency of attacks is highest in this category. This is also a category in which frequency was nearly identical across both cloud hosting provider and enterprise data center environments. The number of incidents per impacted customer was higher in the enterprise data center environment in all other categories, and the differences were often quite pronounced.

FIG. D

INCIDENT FREQUENCY:
TOP THREE INCIDENT CLASSES



THREAT DIVERSITY

Threat diversity is low, with impacted customers experiencing 2.0 different types of threats. It is, however, somewhat higher among enterprise data center customers (2.5) than among CHP customers (1.8). The overall threat diversity numbers are lower than they were in Alert Logic's Fall 2012 report, likely due to Alert Logic's reclassification of some types of incidents. (Reconnaissance attacks that were combined with vulnerability scans are now classified as one incident—a vulnerability scan.)

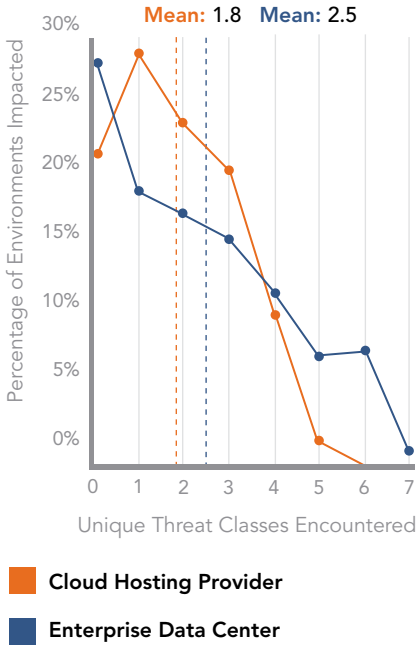
Lower threat diversity does not necessarily indicate that one environment is safer than the other. It does suggest that organizations with a less diverse set of threats may be able to more narrowly focus on certain types of incidents, rather than focus equally on all types of incidents in the threat portfolio. The ability to narrow the security focus is highly dependent on an environment and on the particular security experience within that environment.

THREAT DIVERSITY

For enterprise data center environments, customers experienced an average of 2.5 types of incidents. Cloud hosting provider customers experienced an average of 1.8 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. C



ALERT LOGIC:
Methodology

MORE THAN

45,000

SECURITY INCIDENTS

were verified and observed among Alert Logic customers between April 1 and September 30, 2012.

1 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 as needed.

ALERT LOGIC METHODOLOGY

The data used in this report is real-world incident data detected in customer environments secured by Alert Logic, not from surveys, lab environments or honeypots. Alert Logic captures security events through an intrusion detection system (IDS). To correct for noise and false positives, Alert Logic utilizes a patented correlation engine that evaluates multiple factors to determine whether network-based events rise to the level of an authentic security incident. Finally, a team of GIAC-certified security analysts also reviews each incident to ensure validity and to confirm the threat or compromise, further minimizing false positives.

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

EVENT VS. INCIDENT

This report is based on 46,475 verified security incidents, derived from more than one billion events observed between April 1 and September 30, 2012.

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.

GENERAL INSIGHTS:

Observations By Incident Class

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

INCIDENT CLASS	OBSERVATIONS	DEFINITION	EXAMPLES	RECOMMENDATIONS
APPLICATION ATTACK	**These attacks stem from the large number of leaked older toolkits taking advantage of the existing exploitable vulnerabilities.** > Enterprise data center customers (15%) are more likely to experience these attacks than CHP customers (3%). > Enterprise environments have more end-user and legacy applications; CHP environments more typically host web applications.	Exploit attempts against applications or services not running over HTTP protocol.	Buffer Overflow	> Patch management and good coding practices reduce the vulnerabilities available for exploit through this vector. > Monitoring tools such as IDS and log review can identify these attacks while in progress or after they have been executed.
BRUTE FORCE	**This relatively unsophisticated exploit type remains common. Brute force attacks tend to be precursors to crimes of opportunity rather than deeply targeted attacks.** > These attacks are becoming more common because of the number of password and user lists that have been compromised and released to the open Internet. > SSH brute force attempt by address is the leading method used, accounting for 57% of such attacks. > The greater occurrence among enterprise data center environments (49%) vs. CHP environments (30%) is due to the presence of more individual credentialed users in the enterprise environment.	Exploit attempts enumerating a large number of combinations, typically involving multiple credential failures, in hopes of finding a weak door.	Dictionary Password Cracking	> Sound management practices are a primary defense against brute force attacks. > Organizations need to institute a strong password policy, especially for public-facing applications. > Frequent review of systems logs will identify unsuccessful logins, and determine whether they came from the same source.

GENERAL INSIGHTS:

Observations By Incident Class (cont'd)

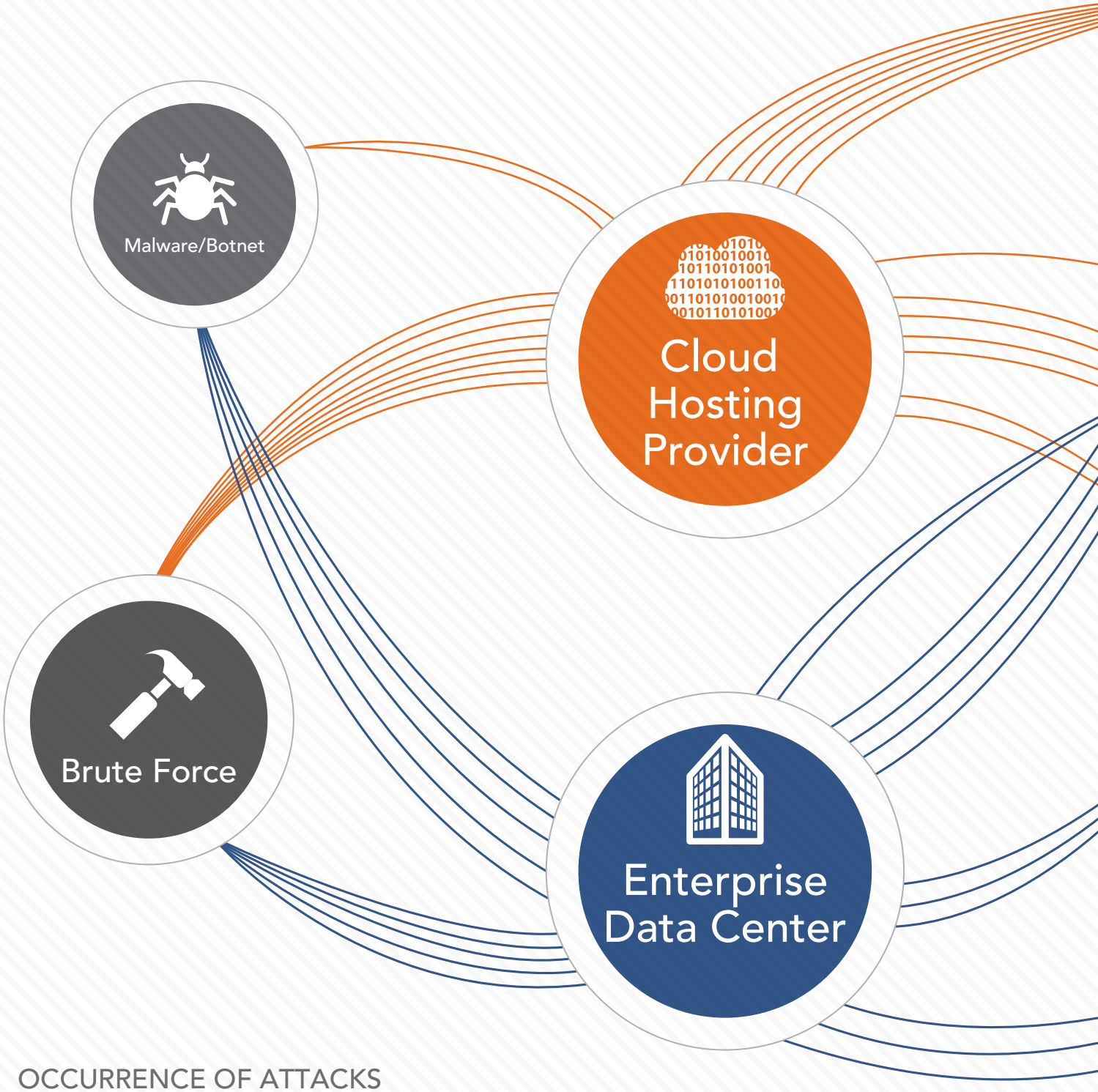
INCIDENT CLASS	OBSERVATIONS	DEFINITION	EXAMPLES	RECOMMENDATIONS
MALWARE, BOTNET ACTIVITY	**Malware remains an effective tool to compromise hosts and exfiltrate data, especially for hosts where web applications do not provide a point of entry.** > Malware is primarily introduced to enterprise entities through spam delivery or a direct hack. > Malware is used to compromise hosts and send secured data to remote locations. > There are a wide (and continuously growing) variety of malware types available on the market. > Because of the number of end-user workstations in this environment, this form of attack is far more prevalent among enterprise data center (49%) than cloud hosting provider (5%) customers. > Customers in a CHP environment are more vulnerable to having a server turned into a bot used to distribute malware and act as a launch pad for attacks on the enterprise.	Malicious software installed on a host for the purpose of engaging in unscrupulous activity, data destruction, information gathering or creation of backdoors. This category includes botnet activity—post-compromise activity displaying characteristics of command and control communication.	Conficker, Zeus	> Antivirus software remains a standard practice for detecting some portion of malware activity. > Reviewing log data can help identify suspicious activity across an organization's infrastructure. > More advanced technologies such as anomaly detection can provide further insight into malware activity.
RECONNAISSANCE	**Reconnaissance is often an initial attempt to find points of entry into target hosts, or to identify systems vulnerable to compromise.** > As botnets increase, so do the number of compromised hosts first found through reconnaissance techniques. > Enterprise data center environments (23%) are more likely to experience a reconnaissance attack than are cloud hosting provider customers (9%). > Alert Logic has observed a decrease in reconnaissance activity in its customer base, largely because of a change in the way in which it characterizes attacks. Compound attacks involving reconnaissance and vulnerability scans are now classified as vulnerability scans.	Activity focused on ping sweeps, mapping networks, applications and/or services.	Port Scans, Fingerprinting	> Monitor reconnaissance activity to identify attackers and enable appropriate updating of firewall and access policies.

INCIDENT CLASS	OBSERVATIONS	DEFINITION	EXAMPLES	RECOMMENDATIONS
VULNERABILITY SCAN	**Many scans are run on behalf of the customer as part of a compliance regimen such as PCI, but malicious attempts occur as well. They should be monitored to detect attempts by attackers to find exploitable vulnerabilities.** > Vulnerability scans are a more invasive form of reconnaissance, and often follow simpler reconnaissance incidents. > Some incidents categorized as vulnerability scans combine both a reconnaissance attack and a vulnerability scan. > Cloud hosting provider (27%) and enterprise data center (28%) environments are equally subject to vulnerability scans.	Automated vulnerability discovery in applications, services or protocol implementations.	Unauthorized Nessus Scan	> Monitor scan activity to identify unauthorized scans, log their source to identify malicious hosts, and consider precautionary blocking with network firewalls.
WEB APPLICATION ATTACKS	**Web application attacks remain one of the most significant incident types in all environments.** They are predominant as an attack vector in cloud hosting provider environments (52% of customers impacted), likely due to the prevalence of web applications. They are also a problem in enterprise data center environments (39% impacted). No one is immune to web application attacks. Attacks take advantage of poor coding and patch administration. Attacks by SQL injection remain the major culprit for web application attacks. This is due to an increased awareness and knowledge of SQL injection tools such as Havij, which in our last report accounted for over 40% of the SQL injection attacks, and their ease of use and effectiveness against high-profile targets.	Attacks targeting the presentation, logic or database layer of web apps.	SQL injection	> All organizations should consider a combination of secure coding practices, thorough patch management, and active defense, such as a web application firewall, to eliminate vulnerabilities and prevent exploits.

TARGETED ATTACKS AND OPPORTUNISTIC HACKS

A Look At The Threats Facing Cloud Hosting Providers & Enterprise Data Centers

> Cloud Hosting Provider (CHP) environments are not inherently less safe than Enterprise Data Center (EDC) environments, but data shows that attacks on CHP environments tend to be crimes of opportunity while attacks on EDC environments tend to be more sophisticated and targeted.



OCCURRENCE OF ATTACKS

> Size of circle indicates percentage of customers impacted.

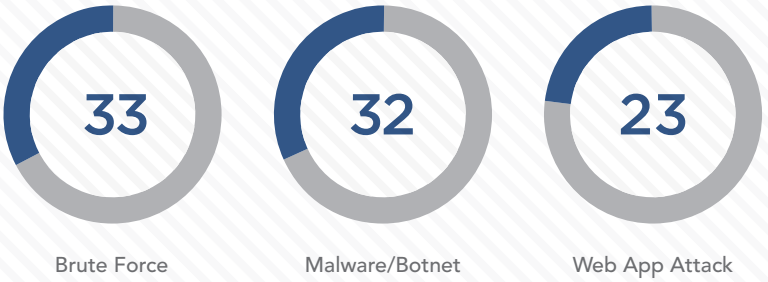
> Number of lines indicates attack volume.

ALERTLOGIC

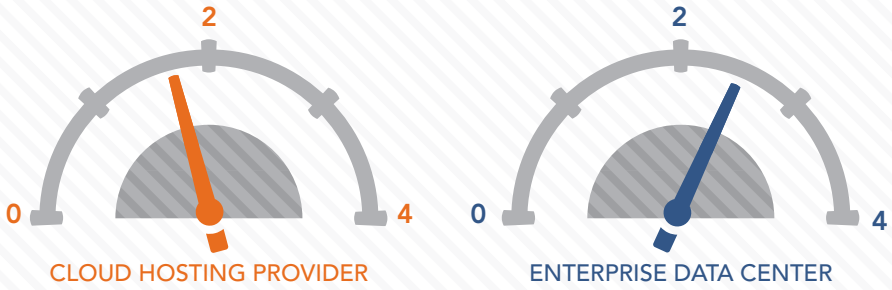
AVERAGE FREQUENCY OF ATTACK
Top Three Incident Classes

CLOUD HOSTING PROVIDER

ENTERPRISE DATA CENTER



AVERAGE NUMBER OF UNIQUE ATTACK TYPES
Threat Diversity



INCIDENT DESCRIPTIONS

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.

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.

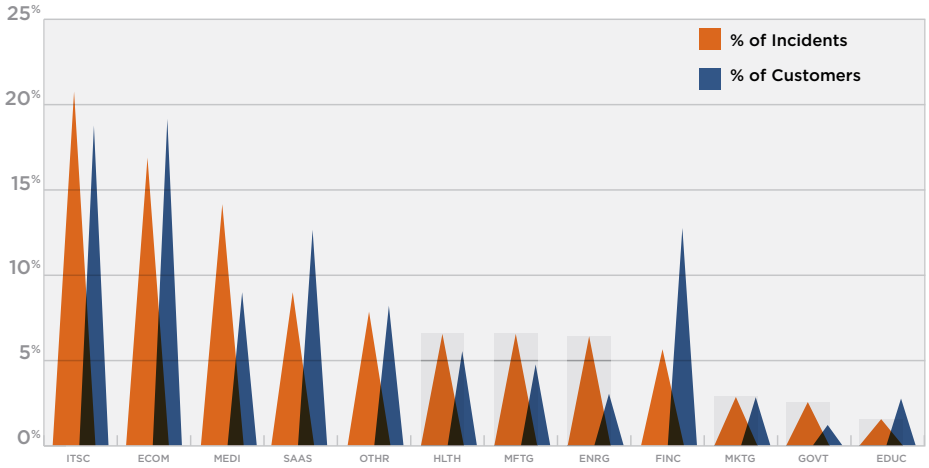
Vulnerability Scan
Automated vulnerability discovery in applications, services or protocol implementations.

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

INDUSTRY:

Does Industry Matter?

Alert Logic examined threat data by industry to identify any notable differences that would suggest particular vulnerabilities or patterns of attack. Our findings suggest that where your IT infrastructure resides (enterprise data center or CHP environment) is a better indicator of threat profile than industry or type of business.



Nonetheless, some differences do occur that are interesting to note. Alert Logic's financial services customers represent nearly 13% of its data set, yet fewer than 6% were attacked. Given the high-profile and attractive target that the financial services industry represents, this is a somewhat counterintuitive finding. However, Alert Logic's financial services customers are typically smaller, less visible organizations. In contrast, media, which represents 9% of Alert Logic's customer set, accounts for 14% of the incidents. In general, media organizations are less security conscious than those in other industries, while at the same time the interesting content they hold is of widespread interest.

INDUSTRIES IN DEPTH

In this report, Alert Logic takes a closer look at three industries. Financial services and healthcare were selected because these industries are highly security conscious, because of the stores of confidential data they house and because they are highly regulated. With the growing interest in cloud services, we have also chosen to drill down on security information in the Software-as-a-Service (SaaS) vertical.

Financial Services

Financial services is composed of a wide range of entities: commercial and investment banks, credit unions, credit card companies, consumer finance companies, money management firms, brokerages, securities exchanges, insurance companies and government entities such as Fannie Mae and Freddie Mac. Roughly 13% of the analyzed client base falls into this industry.

For obvious reasons, financial services firms represent a high-value target for attacks, and are generally a target of choice rather than a target of opportunity. Not only are they "where the money is," they also maintain vast repositories of highly confidential customer data. These organizations are highly visible, and the vast majority of the population has some type of relationship with at least one financial services firm.

One characteristic of the financial services industry that impacts their IT infrastructure, and their security posture, is the increasing number of customers who engage in online transactions—bill paying, statement receipt, funds transfer, portfolio management, stock trading—many of which can now be done through a web application or a mobile device.

It is not surprising, then, that a number of studies of the financial services industry have found so many high-profile security incidents. In April 2012, *Wall Street & Technology* catalogued a series of recent attacks on financial services firms. Some of the biggest names in the industry had been victims of recent hacking incidents, including industry giants CitiBank and NASDAQ. In September 2012, Deloitte Touche published the results of a study that found that

INDUSTRY:

Industries in Depth

one in four financial services firms had suffered some type of security breach in the last year. Deloitte also found that these organizations are security conscious: nearly half of those surveyed actively manage their vulnerabilities to cyber threats, and more than 80% actively conduct research on emerging threats so that they can proactively counter them.

In reviewing its financial services customer data, Alert Logic observed that the occurrence of web application attacks for financial services firms (34%) was significantly lower than for the overall customer base (49%). In keeping with Deloitte's findings of security consciousness in financial services firms, Alert Logic's researchers believe the lower levels of web application attacks are due to the strong security postures this industry maintains. They are thus less subject to opportunistic attacks from unsophisticated hackers using automated tools, such as Havij, which automates SQL injection attempts. Instead, they are targeted by more sophisticated hackers with careful plans for gaining access to data. Typical of these attacks are malware infections, phishing attempts, DNS redirects and clickjacking, techniques deployed by sophisticated criminals.

The difference between web application attack occurrence for CHP financial services customers (37%) and enterprise data center financial services customers (25%) is similar to the web application attack spread in the general Alert Logic customer population (52% CHP vs. 39% enterprise data center), and for the same reasons cited in the general discussion.

Brute force attacks in financial services were also lower than among the overall Alert Logic customer set. (25% of financial services customers were impacted vs. 34% in the full customer set.) Financial services firms represent a less attractive target for brute force attacks because of the industry's generally high security standards. Two-factor authentication is common, locking sites after several attempted logins. Brute force attacks were more common for enterprise data center customers (38%) than for CHP customers (20%), again in keeping with the observations about the overall data set: enterprise data centers generally have more end-user applications with access to sensitive data that could be exploited.

For targeted malware/botnet attacks, financial services (20%) had higher rates than the overall Alert Logic customer set (13%) for both occurrence and frequency. In both cohorts, this was due to more malware attacks in enterprise data center customers (53% of financial services enterprise data center customers vs. only 8% of financial services CHP customers). Alert Logic attributes this to the availability of malware, such as Zeus and Citadel, that is designed directly for the financial services environment. These forms of malware do not target individual websites; they target employees in hopes that they will be better able to breach security through infected workstations.

Most financial institutions have excellent security postures: they implement all levels of access controls, lock down firewalls, perform intrusion detection, etc., and thus prevent many threats at different levels of the "defense in depth" scale. However, they are and will continue to be a high-value target. With the sophistication of today's malware, financial services would benefit from anticipating attacks by doing more proactive research, e.g., getting samples of malware to reverse-engineer. Some of the larger financial services institutions already do this. The smaller ones should also be working with a third party if they lack the internal resources for this type of research.

Key Observations

Financial Services

> Financial services represents a very attractive target, and organizations in this sector should expect to be targeted regularly.

> Attack patterns suggest the use of more sophisticated malware versus brute force or script-generated web application attacks.

> With high rewards attracting sophisticated attackers, financial services organizations should consider investing in research activities to stay ahead of hackers.

INDUSTRY:

Industries in Depth (cont'd)

Healthcare

The healthcare industry is large and getting larger. In 2011, it accounted for roughly 18% of the US Gross Domestic Product, and is expected to consume about 20% by the year 2021. Approximately 6% of Alert Logic's customer base is part of this industry.

Like financial services organizations, healthcare organizations offer high-value targets to hackers. They hold vast amounts of highly confidential personal and financial data, are highly visible, and the vast majority of the population has some type of relationship with at least one healthcare entity. A growing trend is the increasing number of customers who engage in online transactions—accessing their records, making appointments, ordering prescriptions, making payments—some of which can now be done through a mobile device. As a result, healthcare IT infrastructures are increasingly the home of more sensitive data and more access points. Personally identifiable information often found in health records has been traced as the source for many instances of identity theft, as they typically contain all the needed information (name, addresses, social security numbers, employers and even banking information in some cases). As a result, healthcare is also a highly regulated industry. In the US, HIPAA has placed stringent requirements on maintaining patient confidentiality, with substantial penalties when this is violated.

Attacks on healthcare organizations are prevalent. The U.S. Health and Human Services Department has reported that over the past two years, data breaches compromised nearly 20 million patient records. Many of these breaches involved human error or malfeasance (stolen laptops, employee information theft). But in other cases, servers were hacked (resulting in the theft of such sensitive data as Social Security numbers).

The frequency of brute force attacks was higher in healthcare (52.7 per impacted customer) than in general (31.9 per customer), especially so among CHP environments, where the frequency of attack was almost double that of the general Alert Logic customer population (70.1 vs. 31.5). Alert Logic attributes this to the potential payoff of accessing high-value information.

In analyzing incident data for its healthcare customers, Alert Logic observed that web application attacks were somewhat lower (38%) than in the overall customer set (49%). Forty-one percent of CHP customers in healthcare experienced a web application attack; 30% of enterprise data center customers were impacted. Most of the healthcare sites in Alert Logic's customer base are an informational presence only, and most patient data is not accessible through web applications.

Malware/botnet attacks in healthcare (16%) were marginally higher than in the overall customer base (13%). What stands out here, however, is the difference in occurrence between enterprise data center (60% impacted) and CHP (5% impacted) customers. This is due to the presence of employee workstations in enterprise data center environments, which are targeted because they may contain data or provide access to stores of data.

Many security breaches in healthcare are caused by human error or employee violations. In addition to improving their overall IT security posture, by encrypting data and regularly auditing their security for compliance, healthcare organizations should develop and enforce strict policies on who has access to what data, and where and how that data can be stored (e.g., never on laptops).

Key Observations

Healthcare

> Compliance and regulatory requirements for healthcare are high, with severe penalties for noncompliance.

> The value of personal health data makes healthcare an attractive target.

> With so many organizations handling healthcare data, human error and insider violations remain an issue in this space. Along with security technology, policy management is important.

Software-as-a-Service (SaaS)

SaaS adoption has grown rapidly over the last decade, and is on its way to becoming the standard delivery model for software in many categories. As SaaS has grown, it has not been exempt from security attacks, and major players like Microsoft, Google and Salesforce have experienced serious breaches. For those moving to SaaS, security continues to be a major factor in the decision process.

Given the continued growth of SaaS, Alert Logic chose this as the third industry to analyze. For the most part, the attack profile for SaaS customers did not deviate from the attack profile for the overall Alert Logic customer set. Web application attacks were somewhat higher for SaaS providers (55% vs. 49%). Given that SaaS applications *are* web applications, this is to be expected. Many of the applications take credit card data or house data that is of general interest. In keeping with their own business model, the vast majority of the SaaS customers (94%) in Alert Logic's customer base are in CHP environments. It is interesting to note that, with respect to web application attacks, a greater proportion of the SaaS enterprise data center customers were impacted vs. the overall enterprise data center customer set (57% vs. 39%). Again, since a SaaS organization's business is based on web applications, this is not surprising.

Because their entire business takes place on a website, SaaS providers need to be on the leading edge with respect to security.

Key Observations

SaaS

> Web application attacks are higher than average in this space, given its reliance on the web for service delivery.

> For SaaS companies, security impacts not only data security but application availability, with security-related downtime potentially impacting revenue.

> Because SaaS providers rely so heavily on the cloud/hosted environments, SaaS IT staff need to be intimately familiar with the issues facing CHP environments.

Other Industry Points of Interest

- IT Services: The occurrence of malware/botnet incidents in enterprise data center environments (37%) far exceeded the occurrence rate in the overall customer set (13%). With their target-rich environments, housing administrative access across multiple organizations, IT Services represent an attractive target for attacks seeking inside credentials.
- eCommerce: Again with respect to malware/botnet attacks, there was an even more striking occurrence rate among enterprise eCommerce customers (45% vs. 13%). With credit card information on premise, attackers are again on the lookout for intra-company credentials. Enterprise data center environments are also more vulnerable to application attacks: 17% experienced an application attack, vs. 5% in the overall customer set.
- Media: Enterprise data center media companies follow a similar profile, deviating from the norm with respect to malware/botnet (59% vs. 13%) and application attacks (22% vs. 5%).
- Manufacturing: When compared with the total Alert Logic customer set, enterprise data center manufacturing customers experienced far higher occurrences of brute force (65% vs. 34%), reconnaissance (45% vs. 12%), and malware/botnet (50% vs. 13%) attacks.
- Energy: Both CHP (53%) and enterprise data center customers (73%) were subject to higher instances of brute force attacks than the overall Alert Logic customer base (34%). Energy is a high-profile industry, and the frequent target of hacktivists.

WRAPPING UP:

The Data Tells the Story

Insight

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

With this report, Alert Logic again observes consistent patterns when comparing security threats in cloud hosting provider and enterprise data center environments, and again concludes that the CHP is inherently no less secure than enterprise data centers.

What is important to note, however, is that the enterprise, with its more complex infrastructure and higher-value information, is more likely to be subjected to sophisticated, targeted attacks, such as malware.

In comparison, the CHP is more prone to opportunistic web application attacks. While our findings do not suggest that one environment is "more secure" than the other, it is useful to keep the differences in mind when considering which workloads to move to the cloud and what types of monitoring and security technology are most important.

While organizations need to consider the differences in threat profile between enterprise data center and cloud and hosted environments, Alert Logic sees consistent evidence that fears of inherent insecurity in the cloud should not drive infrastructure decisions. In both environments, the fundamentals of sound security practices continue to apply, though each environment should pay special attention to the areas where they are most vulnerable. For the enterprise, this is malware; for CHP customers, it is web application attacks.

APPENDIX:

Data Tables

Incident Occurrence, Frequency, Threat Diversity

Alert Logic Customers | April 2012 through September 2012

ALL ALERT LOGIC CUSTOMERS:

INCIDENT CLASS	Cloud Hosting Provider		ENTERPRISE DATA CENTER	
	Customers Impacted	Frequency	Customers Impacted	Frequency
Web App Attack	52%	13.6	39%	23.4
Brute Force	30%	31.5	49%	32.9
Vulnerability Scan	27%	4.8	28%	8.3
Malware/Botnet	5%	11.3	49%	31.6
Recon	9%	1.5	23%	14.6
App Attack	3%	2.6	15%	3.0
Threat Diversity	1.84		2.49	

HEALTHCARE:

INCIDENT CLASS	Cloud Hosting Provider		ENTERPRISE DATA CENTER	
	Customers Impacted	Frequency	Customers Impacted	Frequency
Web App Attack	41%	5.3	30%	4.2
Brute Force	29%	70.1	60%	19.3
Vulnerability Scan	14%	10.5	15%	55.7
Malware/Botnet	5%	23.5	60%	30.3
Recon	10%	2.0	15%	1.7
App Attack	3%	1.0	30%	1.7
Threat Diversity	1.63		2.33	

FINANCIAL SERVICES:

INCIDENT CLASS	Cloud Hosting Provider		ENTERPRISE DATA CENTER	
	Customers Impacted	Frequency	Customers Impacted	Frequency
Web App Attack	37%	6.6	25%	9.7
Brute Force	20%	20.5	38%	18.4
Vulnerability Scan	24%	3.0	32%	6.4
Malware/Botnet	8%	3.3	53%	11.6
Recon	10%	1.9	17%	11.2
App Attack	2%	1.7	12%	1.4
Threat Diversity	1.61		2.40	

SAAS/ONLINE SERVICES:

INCIDENT CLASS	Cloud Hosting Provider		ENTERPRISE DATA CENTER	
	Customers Impacted	Frequency	Customers Impacted	Frequency
Web App Attack	54%	10.9	57%	41.0
Brute Force	39%	21.7	50%	29.7
Vulnerability Scan	26%	3.4	21%	25.7
Malware/Botnet	8%	1.1	21%	1.0
Recon	3%	3.3	29%	4.0
App Attack	3%	1.5	0%	0.0
Threat Diversity	1.93		2.50	

APPENDIX:

Data Tables

Incident Occurrence

Alert Logic Customers | April 2012 through September 2012

INCIDENTS: ALL INDUSTRIES	APP ATTACK	MALWARE	BRUTE FORCE	RECON	VULNERABILITY SCAN	WEB APP ATTACK
IT Services - Total	5%	12%	32%	13%	28%	48%
Cloud Hosting Provider	3%	5%	29%	11%	28%	51%
Enterprise	12%	37%	42%	18%	28%	41%
eCommerce - Total	5%	7%	33%	8%	31%	57%
Cloud Hosting Provider	4%	2%	31%	6%	29%	58%
Enterprise	17%	45%	45%	19%	40%	48%
Media - Total	6%	14%	31%	11%	35%	57%
Cloud Hosting Provider	3%	4%	29%	10%	37%	60%
Enterprise	22%	59%	41%	16%	31%	44%
SaaS - Total	3%	5%	40%	9%	26%	55%
Cloud Hosting Provider	3%	3%	39%	8%	26%	54%
Enterprise	0%	29%	50%	21%	21%	57%
Financial Services - Total	4%	20%	25%	12%	26%	34%
Cloud Hosting Provider	2%	8%	20%	10%	24%	37%
Enterprise	12%	53%	38%	17%	32%	25%
Manufacturing - Total	1%	14%	44%	24%	24%	55%
Cloud Hosting Provider	0%	3%	37%	17%	23%	57%
Enterprise	5%	50%	65%	45%	25%	50%
Energy - Total	19%	61%	67%	41%	20%	33%
Cloud Hosting Provider	6%	29%	53%	12%	12%	35%
Enterprise	24%	76%	73%	54%	24%	32%
Healthcare - Total	8%	16%	35%	11%	14%	38%
Cloud Hosting Provider	3%	5%	29%	10%	14%	41%
Enterprise	30%	60%	60%	15%	15%	30%
Education - Total	4%	13%	38%	6%	21%	50%
Cloud Hosting Provider	3%	3%	26%	8%	21%	56%
Enterprise	11%	56%	89%	0%	22%	22%

INCIDENTS: ALL INDUSTRIES	APP ATTACK	MALWARE	BRUTE FORCE	RECON	VULNERABILITY SCAN	WEB APP ATTACK
Marketing - Total	0%	2%	27%	8%	24%	51%
Cloud Hosting Provider	0%	2%	24%	5%	24%	55%
Enterprise	0%	0%	43%	29%	29%	29%
Government - Total	10%	19%	33%	14%	33%	62%
Cloud Hosting Provider	8%	15%	38%	0%	31%	69%
Enterprise	13%	25%	25%	38%	38%	50%
Other	4%	14%	31%	12%	27%	45%
Cloud Hosting Provider	2%	7%	27%	12%	28%	44%
Enterprise	12%	42%	46%	15%	19%	50%
Total Customer Set	5%	13%	34%	12%	27%	49%
Cloud Hosting Provider	3%	5%	30%	9%	27%	52%
Enterprise	15%	49%	49%	23%	28%	39%

Service Provider Partners Included In Study

SERVICE PROVIDER PARTNER	WEBSITE	SERVICE PROVIDER PARTNER	WEBSITE
Atos	atos.net	**Megapath**	megapath.com
CyrusOne	cyrusone.com	**NaviSite**	navisite.com
Datapipe	datapipe.com	**OpSource**	opsource.net
HOSTING	hosting.com	**Peer 1**	peer1.com
Hostway	hostway.com	**Pulsant**	pulsant.com
Internap	internap.com	**Rackspace**	rackspace.com
Latisys	latisys.com	**Sungard Availability Services**	sungardas.com
Layered Tech	layeredtech.com	**VISI**	visi.com
Logicworks	logicworks.net	**Windstream Hosted Solutions**	windstreambusiness.com

CONTRIBUTORS

Lead Researcher
Stephen Coty

Lead Analysts
Tyler Borland
Mukul Gupta, PhD
Patrick Snyder

Editors
Maureen Rogers
John Whiteside

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

> alertlogic.com