Cloud: Threat Landscape Review
Global adoption of cloud computing is ever-increasing. Organisations are turning to cloud solutions for financial reasons, scalability, reliability and manageability. Forrester have predicted that businesses will spend $190 billion on cloud services by 2020, compared to $70 billion in 2014.¹ Gartner expects 60% of businesses to use office system capabilities from the cloud by 2020 (compared to 15% in 2015).²

Security remains a common reason for avoiding the use of public cloud services. The decision to host enterprise IT in the cloud raises a number of questions which executives should consider:

- How trustworthy is the cloud provider, and how secure are their solutions? Do they take responsibility for all aspects of security? Is this more, or less, secure than our existing approach?

- If we move to the cloud, how does our exposure to known threats change? And how might the ‘cloud threat landscape’ change in the future?

These are not simple questions to answer. The BAE Systems Threat Intel team tracks over 100 advanced cyber attack groups as well as numerous cybercriminal gangs and a range of general threats. Our experience has shown that attackers are highly adept at exploiting new opportunities for attacks to achieve their goals; if cloud uptake is as high as some analysts are predicting, it is likely that attackers will invest effort in developing capability against it.³

---

²gartner.com/newsroom/id/3119717
³Recent examples include cybercriminal and cyber-espionage campaigns against OSX, mobile platforms, etc.
In this report, we consider the three common ‘models’ of cloud computing; software, platform and infrastructure as a service, plus the addition of cloud collaboration and file hosting. See APPENDIX B for further details.

Our report is broken up into the following sections:

• An analysis of the threat to different cloud delivery models

• Key concerns that arise from transition to cloud, including changes in the cyber security market that are addressing these

• A set of predictions for how the threat landscape could evolve in an increasingly cloud-dependent world, including the adaptations that cyber-criminal, cyber-activist and cyber-espionage groups are likely to make

• An appendix (APPENDIX A) on novel attacks against cloud platforms that may be realised in future

Our experience has shown that attackers are highly adept at exploiting new opportunities for attacks to achieve their goals.
Threat Analysis

To analyse the threat to cloud delivery models, we have used a set of ‘attack types’ which cover the cyber threats that are relevant to cloud contexts. These have been drawn from ENISA’s 2015 Threat Landscape⁴ and Verizon’s 2015 Data Breach Report⁵, and are as follows:

- **Spearphishing** – attackers target individuals or organisations with carefully crafted emails that convince a victim to open an attachment or click a link
- **Watering Hole** – attackers compromise a website that is frequently visited by their targets, and use it to serve malware
- **Distributed Denial of Service (DDoS)** – Attackers use distributed resources and significant traffic volumes to flood a target service with illegitimate requests
- **Web App Attacks** – attacks against users of web applications or their backend applications (XSS, SQLi, etc.)
- **Insider Threat** – a trusted employee (of either the organisation or the cloud provider) either maliciously or accidentally abuses their position to damage the company, e.g. through information leakage
- **Crimeware** – the general threat posed by cyber-criminals in the form of spam, ransomware, exploit kits
- **Identity Theft** – attackers target employee personas and their credentials to gain access to systems
- **Database Access** – attackers target company data (sensitive information, personal data) for various purposes

The table on page 5 provides a high-level analysis of how the exposure to each threat changes for each cloud delivery model - compared to a baseline of traditional, on-premises IT. This analysis is coarse-grained; each box is given an up/down/same rating; in some cases, threats are not applicable to cloud delivery models and are given an N/A rating.

---

⁵https://msisac.cisecurity.org/whitepaper/documents/1.pdf
<table>
<thead>
<tr>
<th>Cloud delivery model</th>
<th>Collaboration / File Hosting</th>
<th>Software As A Service (SaaS)</th>
<th>Platform As A Service (PaaS)</th>
<th>Infrastructure As A Service (IaaS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack type ↓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing</td>
<td>Up - Use of external services presents an increased social-engineering and delivery vector risk. i.e. attackers craft attacks to leverage the trust in external services</td>
<td>Down - attachments and links have a lower surface to exploit; malicious macros do not run in Office Online</td>
<td>N/A - email surface is not applicable in this context</td>
<td>Down - An IAAS end user can still be spearphished, but lateral movement and persistence become more difficult due to virtualization of IT</td>
</tr>
<tr>
<td>Watering Hole</td>
<td>Same - Creates extra surface for advertising malicious links, but creating these would likely require account compromise first</td>
<td>Same - browsing is the same</td>
<td>Same - Though if the cloud provider is compromised, an attacker can craft a highly targeted watering-hole (e.g. on the cloud hosted corporate intranet)</td>
<td>Down - An IAAS end user can still browse to a compromised site, but lateral movement and persistence become more difficult due to virtualization of IT</td>
</tr>
<tr>
<td>DDOS</td>
<td>Up - these services are exposed to the Internet and are therefore more vulnerable to DDoS. Aggregation of multiple targets onto a single provider also increases attack likelihood. DDoS protection and business continuity planning are key considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web App Attacks</td>
<td>Up - collaboration applications are potentially vulnerable to web attacks</td>
<td>Up - SaaS applications are potentially vulnerable to web attacks; scripting functionality (if present) may be exploitable</td>
<td>Up - from the perspective of both developers and end users. Attacks may require sandbox escape</td>
<td>Same - applications running on IaaS may still be vulnerable to SQLi, XSS, etc. – responsibility lies with customer</td>
</tr>
<tr>
<td>Insider Threat</td>
<td>Up - third-party administrators increase the baseline insider threat faced by organisational employees. Access control, logging, and monitoring are key considerations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crimeware</td>
<td>Up - Criminals may turn attention towards using cloud delivery techniques</td>
<td>Same - Ransomware and banking Trojans may still work against the endpoint; exploit kits may need to be modified. The provider may have measures in place to detect and block these attacks, but this cannot be guaranteed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Theft</td>
<td>Up - extra identities and credentials to manage. Single-sign on, 2-factor authentication, endpoint security and Virtual Private Networks are key considerations/mitigations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Access</td>
<td>Up - databases and information are by definition more exposed. Access control, Data Loss Prevention, jurisdictional issues are key considerations. Aggregation of information onto a (relatively) small number of providers means they become a more attractive target</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following observations emerge from this analysis.

- Cloud services are slightly less exposed (but by no means completely immune) to spearphishing and watering hole attack techniques, often used by high-end threat actors:
  
  - Exploits against MS Word and Adobe may not work in functionality-constrained and well patched SaaS environments. The threat from malicious macros (which are currently very popular) is also mitigated since Macros do not run in Office Online, and add-ins are not supported.\(^6\) However, as SaaS platforms become more popular, they may become enhanced with extra features based on code execution in the browser – this vector would make them more of a target.
  
  - In IaaS contexts, spearphishing and watering holes may still allow and attacker to gain a foothold on the victim’s machine. While the attacker may be able to get what they need from this position, it may be more difficult to move laterally within the victim’s estate from this point of presence owing to IaaS.

- The threat from DDoS, Web App Attacks, Insider Threat, Identity Theft and Database Access all go up across the spectrum of cloud services. This is due to increased dependency on resources that are exposed to – and accessible from – the Internet. A large number of security mechanisms could be deployed to protect against these threats (DLP, logging, access control, identity management, DDoS protection, etc.). However, the responsibility for security in cloud delivery models is somewhat blurred – as discussed further below.

Key Concerns

Who is responsible for cloud security?

Currently, cloud platform providers cannot be relied upon to provide and enforce all aspects of cyber security (and it is highly unlikely that this will ever be the case). Therefore, the responsibility for cloud security rests on both the provider and the customer: cloud computing should not be seen as a means to ‘outsource security’.

Interestingly, Gartner have predicted that by 2020, 95% of cloud security failures will be the customer’s fault.\(^7\) Although Gartner’s report does not state the types of failure that could contribute to this statistic, it is likely that they will fall into the following categories:

- Weak authentication – lack of two-factor authentication (2FA) poor password strength, password re-use
- Inappropriate controls on data – not implementing ‘need to know’, lack of encryption\(^8\)
- Lack of appropriate security functionality – e.g. no Data Loss Prevention or DDoS protection, which may not be part of a cloud provider’s offering (by default)

According to Gartner, only 3.8 percent of cloud IT spending is currently dedicated to security – compared to 11 percent of traditional IT spending.\(^9\) In other IT areas, high-profile attacks have been the catalyst for increased awareness of the threat that faces them (for example Stuxnet and SCADA/ICS). If a major attack were conducted by a nation-state against a large cloud provider such as Microsoft or Amazon, this could have huge knock-on effects on the cloud security market.

---

\(^7\)http://www.gartner.com/newsroom/id/3143718
\(^8\)Documents need to be encrypted not only at rest, but ideally before they have been transmitted to cloud infrastructure. This is difficult to achieve when using SaaS or cloud collaboration, as the service needs to be able to view the data to be able to operate on it.
\(^9\)https://www.skyhighnetworks.com/cloud-security-blog/gartner-companies-spend-just-3-8-of-cloud-budgets-on-security/
**Changes in the market**

Recognising the potential security gap in cloud adoption, Gartner has proposed ‘Cloud Access Security Brokers’ (CASBs) as a technological solution for integrating security functions and enforcing policy across the customer and cloud domains. A number of companies have spun up in this area, including Adallom (who have since partnered with HP and been bought by Microsoft)\(^{10}\)\(^{11}\), and Zscaler. A key aspect of these solutions will be network and access monitoring.

It is also likely that cloud security risk assessments, compliance management and supplier reviews will become a big part of the ‘go-to-cloud’ decision process. Supplier trust is a key part of cloud computing, and is considered further below.

**Is the cloud provider trustworthy?**

Using a cloud provider for service provision, data storage, and compute power requires placement of a strong degree of trust in their operations. This raises a number of issues, which are discussed under the next 3 subheadings.

**Extra admins = extra insiders?**

As with traditional IT deployment, there is an ‘insider’ threat to cloud services from coerced, disgruntled or careless employees (potentially both current and former) that may leak an organisation’s data, which can be mitigated to some extent by access control and security vetting. However as illustrated in the diagram below, with cloud technology, there is also a possibility that a privileged employee at the cloud provider could leak an organisation’s data.\(^{12}\)

---

\(^{12}\)Encryption can be employed for data that does not need to be used within SaaS, but the applications that rely on reading and interacting with SaaS will not function effectively with encrypted data.
Security record

Although all providers will claim to have security at the forefront of their operations, this should be validated against their record and transparency in this space. Security researchers and motivated attackers have been able to find vulnerabilities in even the well-developed platforms. Some examples of cloud platform security issues are:

• A cross site scripting (XSS) attack was demonstrated in 2011 against Amazon Web Services

• Microsoft security issue in 2013 where SSL certificates were not renewed, bringing down their cloud storage services

• The cloud-based messaging platform Slack was hacked in February 2015, and attackers had access to central databases that contained usernames and encrypted passwords for their users for up to 4 days.

Terms of service and data handling

Terms and conditions for cloud-based systems are hugely important, and customers should be very wary of the potential implications of these.

Providers may state that:

• They may move data between sites (or countries) without letting their customers know – this could cause issues with data falling foul of the safe harbour decision which prohibits personal data being transferred to overseas jurisdictions with weaker privacy laws. It would be rare to see a contract for cloud computing where the customer is guaranteed that their data would not be transferred outside a specified country or region.

• They are not legally responsible for a data breach.

Cloud services require careful consideration from the perspective of global legislation on data protection. International Safe Harbour Privacy Principles enable US companies to comply with privacy laws that protect EU and Swiss Citizens. However, these safeguards can be over-ridden by the Patriot Act (renewed in 2015 as the ‘USA Freedom Act’), meaning that European data could be acquired and inspected by US law enforcement and intelligence agencies (any data hosted on servers owned by companies that have an office on US territory can in principle be seized). Political and legal agreements on these issues are still in flux: the EU/US framework with the US under the ‘Safe Harbour Privacy Principles’ was replaced by the ‘EU-US Privacy Shield’ in February 2016, but still faces uncertainty.
Changes in the market

There is demand from the market for compliance measures to enable organisations to place trust in cloud vendors. As such, there have been moves to standardise the information and assurance policies covering cloud providers.

SOC 2 Type II compliance is crucial for any cloud vendor working with larger, enterprise-level companies. It is conducted by an independent audit firm, and the audit is a rigorous review of a company’s backup and recovery systems. The SOC 2 Type II audit includes a full assessment of the five trust service principles (TSPs) namely Security, Availability, Processing Integrity, Confidentiality and Privacy.

Amazon Web Services (AWS), Microsoft and Google have been audited for their SOC 2 Type II compliance; however, some other smaller cloud vendors have not completed the necessary auditing procedures. There is likely to be an increased focus on consultancy and compliance services that can provide assurance and help organisations choose appropriate cloud providers for their needs.

Implications of company data in the cloud - and user behaviour

For the cloud to be effective, businesses should be able to host a full array of information in the cloud – including personal information, commercially sensitive information, source code, etc. To safeguard against increased exposure to data leakage, companies should monitor corporate data that is shared and ensure that appropriate safeguards are put around sensitive data in the cloud (e.g. access control, identity management, DLP, logging).

Complications that may arise include the following:

- Some business contexts will require that offline working is possible (e.g. employees that travel regularly, without appropriate WiFi access). In these cases, it is likely that desktop applications will be used in tandem with SaaS – which creates an extra interface which could be exploited by attackers (e.g. targeting Office exploits, or intercepting data between desktop and cloud applications).

- Remote working could also cause issues if personal machines are used as endpoints – employees could potentially download company files or source code onto their personal machines and then expose accidentally or deliberately expose this information. In this case, the company will have no visibility over what has happened. Similarly, the ubiquity of HTTPS on free email providers (Gmail, Hotmail) means that even on enterprise IT, documents could be exfiltrated via these email services without DLP solutions picking them up.

Employees that may be frustrated at the lack of remote working support (or ignorant of the risks) and resort to the practice of ‘Bring Your Own Cloud’ (BYOC), where they use public or third-party cloud services to perform their jobs outside of company policy and process. This can be dangerous, allowing employees to disseminate documents over the internet with little corporate control.

Data Loss Prevention is a very different problem for cloud deployments - where data is already ‘outside the firewall’. IT security companies are beginning to move into this area – including established names (e.g. Symantec17) as well as start-ups (e.g. Elastica18, who were recently acquired by BlueCoat). Inspection of SSL flows between users and cloud services (particularly for Collaboration / File Hosting) will likely be of increasing importance to enterprises.

There is also an increasing market for solutions that can monitor the Internet (including the ‘dark web’) for material that relates to company interests. This is likely driven by the insecurity felt by CIO/CISOs that they cannot see where their data is and who is accessing it – and hence would like to understand if it pops up on other parts of the internet.

For the cloud to be effective, businesses should be able to host a full array of information in the cloud

18https://www.elastica.net/security-topics/cloud-dlp
Who’s accessing my cloud? Authentication measures, identity management and logging

Authentication

Cloud services may, depending on implementation, be accessible from any endpoint. With this in mind, the need for strong authentication becomes paramount.

Two-Factor Authentication (2FA) identifies users by ‘something they own’ in addition to their username and password. This second factor can either be a mobile phone (whose number is registered with the authentication server), or a hardware token (e.g. RSA token) that generates one-time codes periodically. Many cloud collaboration and File hosting services offer 2FA as an option, but these are rarely set by default. Some cloud collaboration services do not provide support for 2FA at all.

Where 2FA is not used, attackers can attempt ‘diagonal brute forcing’ of accounts on a target service using credentials that have been compromised in other breaches (e.g. eBay, LinkedIn, Gmail). This is shown in the diagram on page 12, and is an incredibly simple but effective attack that exploits the prevalence of password re-use. Cloud service providers should be able to detect and mitigate against brute-force attacks (e.g. through maximum re-tries, CAPTCHAs, alerting on abnormal levels of failed login attempts, etc.).

---

19 As soon as the user enters the one-time code into their keyboard, it becomes something that attackers can intercept. Cyber-criminals have invested in developing tools that can socially engineer their victims to intercept credentials in 2FA scenarios. However, 2FA remains far more secure than single-factor, and should be used where possible.

Single sign-on (SSO) is the process of authenticating to one system and using these credentials to login to other separate, but related, systems. This can be based on Windows Active Directory for a corporate domain, or OAuth methods, e.g. those using Facebook or Google Apps credentials to access other services). With a SSO framework for authenticating and authorising users, user management is simplified (e.g. for user creation and account deletion for leavers), and users have to remember less logins. However, SSO can be very difficult to set up and configure correctly.

Most enterprise oriented cloud platforms support SSO with Active Directory via SAML, from collaboration tools (e.g. DropBox), through to IaaS market leaders (Amazon Web Services – where a number of third-party SAML 2.0 identity providers can be used to support SSO for administrator web console access).21

Identity Management has become a major issue within cyber security with the ever-increasing number of logins and online services that users have to remember. SSO (discussed above under the heading of Authentication) is one mechanism to manage this, but other services are becoming available that can provide increased flexibility.

One of the simplest and most popular ‘password managers’ is LastPass; it has been stated that 91% of organisations have LastPass users.22 While LastPass’ cryptographic protection of user password databases is very strong, it has been targeted twice (2011, 2015), with the latter attack leading to theft of customer email addresses, password reminder questions, server per-user salts (randomly generated additional data inputs), and hashed master passwords (although cracking these hashes would be incredibly difficult).

Many providers are recognising the need for identity management that can be deployed against cloud IT in combination with on-premises integration (e.g. for Active Directory / LDAP) – so-called ‘Identity-as-a-Service’ (IDaaS) solutions (which are themselves cloud-based). Centrify23 and IBM24 are two such examples. ForgeRock provide a number of products in this area, and extend their identity management to cover devices as well as people.25

24http://www-03.ibm.com/security/services/cloud-identity-service/
25https://www.forgerock.com/platform/
Logging

Logging is hugely important in IT security and underpins attack detection and incident response. With transition to the cloud, the availability of logs on events such as unauthorised access, failed logons and system events as well as alerting on suspicious behaviour on the network become even more important, and these tools will not necessarily be implemented (adequately) by the cloud provider.

Security vendors are now able to provide authorised analysts with an ability to access this information and distil intelligence from it, by ingesting information, storing it and analysing it within a single, common workplace.

Large cloud platforms are likely to provide some level of logging – for example Microsoft Azure (PaaS/IaaS), whose logs can provide coverage of “Policy violations, Internal and external threats, Regulatory compliance and Network, host, and user activity anomalies”. However, there is a growing market for standalone products and services that can be used to cover cloud-enabled IT estates – for example Alert Logic’s Log Manager.

Availability considerations

Cloud adoption brings with it increased dependency on the Internet, and also exposes essential services to the Internet. As a result, cloud services are inherently susceptible to DDoS attacks, as the diagram below shows. Large providers offer advice and technical options for mitigating this threat (for example, AWS recommend using Amazon Virtual Private Cloud (VPC) to protect non-public instances from the internet, as well as offering load balancing solutions). Amazon ECS and Microsoft Azure both commit to an SLA of 99.95% for virtual machines in a single region / availability zone, and do not offer ‘DDoS Protection’ themselves.

26http://download.microsoft.com/download/b/6/c/b6c0a98b-d34a-417c-826e-3ea28c9f9dd/azuresecurityandauditlogmanagement_11132014.pdf
29https://aws.amazon.com/ec2/sla/
30https://azure.microsoft.com/en-gb/support/legal/sla/virtual-machines/v1_0/
DDoS attacks have recently been very popular with cyber-criminal and activist groups, particularly in the form of ‘DDoS for Ransom’, e.g. attacks conducted by Armada Collective and DD4BC. There is a growing market for DDoS Protection services, and these are being made available for cloud deployments – e.g. Incapsula’s DDoS protection for AWS. For PaaS, Gov.UK suggests making application architecture as provider-independent as possible, to ensure that there if outages occur (or suppliers discontinue service for whatever reason) that there is no single point of failure.

Predicted changes in the threat landscape

While cloud uptake is relatively low, attackers do not need to concentrate their efforts on these platforms. The level of disclosed vulnerabilities and breaches in cloud platforms is currently low, but vulnerability research and attacks against cloud platforms are likely to correlate closely with their uptake, which is predicted to soar in the next 5 years. Attacker success will depend on security spending, and, on a case-by-case basis, the level of consideration that is given to the problems posed by hosting data, applications and computing power in the cloud.

We expect to see the following changes in the threat landscape:

- Attackers will target companies of interest via their cloud services, in line with where there is opportunity for making money (cyber-criminal) or obtaining sensitive data (cyber-espionage). Attackers will use social engineering and other means to target credentials for cloud logins of interest. This could be against both end-users and Cloud providers themselves.

- Nation-state actors will invest more heavily in reconnaissance against cloud providers and in developing capability against cloud platforms, including attacks against hypervisors, etc. Market dominance of relatively few cloud providers may lead to increased motivation to attack those platforms – and to exploit multiple target customers of interest in one-off attacks. According to recent research, Amazon, Microsoft, Google, and IBM hold 54% of the cloud market and are growing faster than their competition. The extra risk to business of being ‘collateral damage’ of an attack on a common provider can be mitigated to some extent by using ‘private cloud’ (i.e. dedicated infrastructure for your company), but this comes at extra cost.

- The increased dependency on the Internet will lead to increased DDoS attacks (largely from criminal and activist groups). Recent attacks against root DNS servers in Turkey caused intermittent outage to all .tr domains; geopolitical tension could drive similar attacks against other countries, which would have severe implications for businesses that are entirely cloud dependent.

- Attackers will increasingly exploit cloud services to enable their attacks. Over recent years, we have seen cloud hosting being used as a vector for infiltration, covert communications and exfiltration; research has also shown that attackers are renting AWS instances to conduct SQLi attacks.

---

Attacker success will depend on security spending, and, on a case-by-case basis

---

31https://www.incapsula.com/ddos-protection-for-aws.html
32https://gds.blog.gov.uk/2015/09/08/building-a-platform-to-host-digital-services/
33http://www.informationweek.com/cloud/amazon-microsoft-ibm-google-capture-cloud-market/d/d-id/1321484
34http://www.dailydot.com/politics/turkey-ddos-attack-tk-universities/
Summary

Cloud platforms have the potential to be hugely widespread and important. Their ease-of-use and low entrance threshold should ensure that enterprises can use technology that is based off-premises, lowering their IT overheads in doing so. While it is clear that the cloud is neither ‘inherently insecure’ nor ‘completely secure’, there is no simple answer to whether cloud is more or less secure than on-premises. Some risks decrease, some increase, and what is important is that the risks which increase are identified and mitigated early in the cloud adoption life-cycle.

The market for cloud security products and services will have to meet the needs of customers with a huge array of use cases to allow transition the cloud to proceed without creation of major weaknesses that attackers will be looking to exploit.
Appendix A – Current research; future attacks?

This appendix covers ‘cloud-specific’ security research and vulnerability disclosure. It is likely that attackers will look to develop capability in these areas as cloud adoption continues.

PaaS: Sandbox Escape - Access to other applications

In December 2014 it was announced that there were multiple vulnerabilities in how Google implemented its security for sandboxing individual applications on its Google App Engine service, allowing sandbox escape. This could mean that data from other applications installed on the same infrastructure could be accessed. A similar attack was shown against Oracle Java Cloud Service. These vulnerabilities were responsibly disclosed to both Google and Oracle allowing them to address the faults and patch the issues.

IaaS: Side-channel attacks - obtaining encryption keys

Amazon EC2 instances, Google Compute Engine, RackSpace and Linode all provide encryption options for data at rest, meaning that if the physical storage medium is lost or stolen then the data should be relatively secure. However, the encryption key will be stored in the volatile memory (RAM) of the virtual instances; it is possible that this key could be extracted by malicious software with the appropriate privileges on the virtual machines, or by extracting the virtual memory from the hypervisor.

Security research has demonstrated that RSA private keys can be retrieved from Amazon EC2 instances which have been hosted on the same hardware. However, this research relied on access to a VM running on the same physical hardware as the target, and required that the target was running a particular version of the popular open source software package Libgcrypt. Amazon has since stated that the research does not demonstrate real-world vulnerability in Amazon EC2.

IaaS: Virtual Machine Escape - Attacks against the hypervisor

A virtual machine escape is the capability of breaking out of a virtual machine onto the hypervisor that it is running on. From this hypervisor, it would be possible to access data from other virtual machines on the same system. This has been demonstrated most recently by the proof of concept code called Venom, which allowed code execution on the hypervisor/host. This is not the first time that virtual machine servers have been shown to be vulnerable to this type of attack; although Venom is arguably the most serious vulnerability of this type discovered, 6 others have been disclosed, the earliest of which dates back to 2007.

To enable this attack, the attacker must have an initial point of presence on one VM on the ‘target’ hypervisor. To obtain this, the attacker could:

- Compromise one of the VMs being run on the target hypervisor (e.g. by account compromise)
- Register legitimate VPS(s) through the cloud provider that may be run on the target hypervisor

---

39http://www.theregister.co.uk/2015/10/02/amazon_boards_windows_against_leet_keystealing_neighbours/
40http://venom.crowdstrike.com/
41http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1744
42http://venom.crowdstrike.com/
43In practice, the latter may be very difficult to exploit. Amazon has not released a definite figure for the number of servers it has available in its data centres worldwide, but a conservative estimate from 2014 put the total number of worldwide servers at 1.4 million – see http://www.enterprisetech.com/2014/11/14/rare-peek-massive-scale-aws/. It is relatively easy to work out the location of an Amazon EC2 instance, but each location has a minimum of one data centre, (i.e. a minimum of 50,000 servers). It would be very difficult for an attacker to guarantee that they had access to the same physical server on which the target was operating; one approach may be to automate the thousands of creation of new instances, performing ‘reconnaissance’ each time – though this may be impractical and expensive.
Virtual machine escape would be very difficult to achieve, and is within reach of only the most capable threat actors (sophisticated nation-state groups). It would likely rely on discovery of 0-day exploit(s) in the virtualisation platform, as well as an initial step which is likely to require social engineering of the target organisation or the cloud provider. However, once achieved, it would be very difficult to defend against. As malware could exist on the virtualisation platform it would be practically invisible to the underlying virtual machine. It could also survive the reinstallation of the virtual machine infecting each one on first boot.

By exploiting vulnerability in the virtualization platform, it may be possible to download all of the files from the hypervisor, including not only the data at rest, but in theory, the data from RAM used to encrypt the data on the hard disk, as illustrated in the diagram below.

**Attackers** will look to develop capability in these areas as **cloud** adoption continues.
## Appendix B – Common models of cloud computing

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud collaboration and file hosting</strong></td>
<td>Websites and portals that allow users to collaborate and share documents over the Internet.</td>
<td>Atlassian Cloud, DropBox, OneDrive</td>
</tr>
<tr>
<td><strong>Software as a Service (SaaS)</strong></td>
<td>Software that is located on an externally hosted server. SaaS is usually accessed via a web browser, although pre-built applications for mobile systems are also common. SaaS applications replace common desktop applications, e.g. word processing / spreadsheets / email within a web browser.</td>
<td>Office 365, Google Apps, Salesforce</td>
</tr>
<tr>
<td><strong>Platform as a Service (PaaS)</strong></td>
<td>Provides a platform which facilitates development and deployment of applications. The ‘platform’ can include APIs, operating systems, database interaction, etc.</td>
<td>Google App Engine, Amazon Web Services Elastic Beanstalk; Salesforce Heroku</td>
</tr>
<tr>
<td><strong>Infrastructure as a service (IaaS)</strong></td>
<td>Outsourcing of in-house servers to external providers. Distinct servers can offered (web, email, file, distinct applications etc.) but the typical model is for virtualisation of multiple machines on one physical ‘hypervisor’. If deployed appropriately and at scale, this creates significant cost savings. The company’s data is stored on infrastructure managed by the cloud provider, who is also responsible for compute power.</td>
<td>Amazon EC2, Google Compute Engine, MS Azure, RackSpace</td>
</tr>
</tbody>
</table>
We are BAE Systems

At BAE Systems, we provide some of the world’s most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, defend people and national security, and keep critical information and infrastructure secure.

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

BAE Systems, Surrey Research Park, Guildford
Surrey, GU2 7RQ, UK
E: learn@baesystems.com   | W: baesystems.com/businessdefence

LinkedIn: linkedin.com/company/baesystemsai
Twitter: twitter.com/baesystems’ai

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +61 9240 4600

BAE Systems
Arjaan Office Tower
Suite 905
PO Box 500523
Dubai, U.A.E
T: +971 (0) 4 556 4700

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000