# TABLE OF CONTENTS

**Overview**  
3  
**Key survey findings**  
4  

## CLOUD ADOPTION TRENDS
- Cloud benefits  
  6  
- Cloud investments  
  7  
- Cloud adoption stages  
  8  
- Barriers to cloud adoption  
  9  
- Top cloud service delivery & providers  
  10  
- Most popular cloud workloads  
  11  
- Data stored in the cloud  
  12  
- Applications deployed in the cloud  
  13  
- Most popular cloud apps  
  14  

## CLOUD SECURITY CHALLENGES
- Cloud security concerns  
  16  
- Cloud security incidents  
  17  
- Security risks in the cloud vs. on-premise  
  18  
- Cloud apps vs. on-premise apps  
  19  
- Biggest security threats in public clouds  
  20  
- Cloud security concerns  
  21  
- Biggest cloud security headaches  
  22  
- Personal cloud storage policy  
  23  

## CLOUD SECURITY SOLUTIONS
- Paths to stronger security  
  25  
- Cloud confidence builders  
  26  
- Traditional security tools in the cloud  
  27  
- Most effective cloud security technologies  
  28  
- Most popular cloud security controls  
  29  
- Drivers of cloud-based security solutions  
  30  
- Barriers to cloud-based security solutions  
  31  
- Cloud application security  
  32  
- Access to cloud applications  
  33  
- Security impact on DevOps  
  34

- Methodology & Demographics  
  35  
- Sponsor  
  36
In this new report, you will learn how your peers are approaching cybersecurity in the era of cloud, including the latest trends and benchmarks to gauge how your own organization stacks up.

We hope you will enjoy this report.

Holger Schulze
KEY SURVEY FINDINGS

1. Security concerns top the list of barriers to cloud adoption led by general security concerns (53%, up from 45% in last year’s survey), legal and regulatory compliance concerns (42%, up from 29%), and data loss and leakage risks (40%). The rise in specific concerns about compliance and integration suggests that companies are moving from theoretical exploration of cloud models to actual implementation.

2. 53% of organizations see unauthorized access through misuse of employee credentials and improper access controls as the single biggest threat to cloud security. This is followed by hijacking of accounts (44%), and insecure interfaces / APIs (39%). One in three organizations say external sharing of sensitive information is the biggest security threat.

3. Verifying security policies (51%), visibility into infrastructure security (49%) and compliance (37%) were named as the top three cloud security challenges that cause the biggest headaches for IT security professionals.

4. Organizations moving to the cloud have a variety of choices available to strengthen cloud security. 61% of organizations plan to train and certify existing IT staff, 45% partner with a managed security services provider, and 42% deploy additional security software to protect data and applications in the cloud.

5. Encryption of data at rest (65%) and in motion on networks (57%) top the list of most effective security technologies to protect data in the cloud. This is followed by intrusion detection and prevention (IDP) with 48% and access control technologies such as Cloud Access Security Brokers (CASB) with 45%.
CLOUD ADOPTION TRENDS
After a few years of operating workloads in the cloud, organizations are confirming the benefits match the original promise of cloud computing. Availability (46%), cost reduction (41%) and flexible scalability (36%) top the list. Cloud is still falling short of expectations in the areas of regulatory compliance (13%) and the promise of reduced complexity (14%).

Q: What benefits have you realized from your cloud deployment?

Moved expenses from fixed CAPEX (purchase) to variable OPEX (rental/subscription) 32% | Accelerated deployment and provisioning 31% | Increased agility 28% | Improved performance 27% | Increased efficiency 26% | Increased geographic reach 24% | Increased employee productivity 23% | Improved security 19% | Accelerated time to market 18% | Align cost model with usage 18% | Not Sure/Other 25%
For over a third of organizations (38%), cloud investments represent up to 15% of overall IT infrastructure investment. Half of all organizations have over 15% of their IT invested in the cloud.

Q: Cloud infrastructure investments represent what percentage of your overall infrastructure footprint (in terms of servers/workloads/instances)?
79% of respondents are either in planning or trial stages, currently implementing or in active production cloud environments.

Cloud computing can be classified by location and ownership of the cloud infrastructure:

**Private Cloud** - Cloud infrastructure and services are dedicated to a particular organization. Private clouds can reside on premise or be hosted by a third party.

**Public Cloud** - Cloud services and infrastructure are hosted by a third-party cloud provider and resources are shared among multiple cloud tenants / clients.

**Hybrid Cloud** - Cloud computing environment in which single applications are split across private and public cloud, often to dynamically accommodate spikes in server demand.

Q: What cloud service delivery model(s) is your organization using?
Cloud security concerns not only top the list of perceived barriers to cloud adoption, they are further increasing. General security concerns (with 53% up from 45% in last year’s survey), legal and regulatory compliance concerns (42% up from 29%), data loss & leakage risks (40% slightly down from 41%), integration with existing IT environments (35% up from 29%) and lack of expertise (26% up from 16%) top the list of barriers to cloud adoption. However, it is important to put this in context as the number of reported breaches in enterprise environments far exceed the reported exposure from cloud platforms.
The dominance of both cloud applications and cloud infrastructure requires that we think about securing these different entities as part of a holistic vision for securing application and infrastructure (both on premise and in the cloud). A majority of organizations (61%) uses SaaS models, followed by IaaS (53%) and PaaS (39%) as their cloud service delivery model.

Amazon AWS is the big fish in the cloud services pond, used by 45% of respondents. Microsoft Azure follows with 39%.

Q: What public cloud provider(s) do you currently use?

Q: What cloud service delivery model(s) is your organization using?
MOST POPULAR CLOUD WORKLOADS

Storage (52% up from 38% in last year’s survey), computing (51% up from 32%) and virtualization (44% up from 33%) top the list of most deployed workloads in the cloud.

Q: What services & workloads is your organization deploying in the cloud?

Productivity Applications (email, collaboration, instant messaging) 37%  |  Networking (virtual private cloud, DNS, etc)  35%  |
Database (relational, NoSQL, caching, etc.)  33%  |  Operating System 30%  |  IT Operations Applications (administration, backup, provisioning, monitoring, etc.) 25%  |  
Developer / Testing Applications 25%  |  Security (Identity management, access control, data protection, usage & resource monitoring, anti-virus, etc.) 25%  |  
Middleware 17%  |  Desktop virtualization  15%  |  Runtime  9%  |  Not sure/Other 17%  

Q: What services & workloads is your organization deploying in the cloud?
Email is the most common corporate information stored in the cloud (44%), followed by customer data such as names and contact information (31%), sales and marketing data (31%), and employee and payroll data (30%). Fewer organizations store intellectual property information (18%) or employee healthcare data (12%) in the cloud.

Q: What types of corporate information do you store in the cloud?

- Email: 44%
- Contracts, invoices, orders: 26%
- Customer data: 32%
- Sales & Marketing data: 31%
- Employee data: 30%
- Financial corporate data: 19%
- Intellectual property: 18%
- DevOps / development data: 16%
- Health information: 12%
- None: 11%
- Not sure/Other: 24%
The use of cloud applications is increasing as the number of organizations with 50% or more of applications deployed in the cloud (18%) has more than doubled since last year’s survey. It is apparent that the move toward cloud computing is inevitable. Organizations have no real competitive advantage by owning core IT infrastructure any more than owning power generation or water supply.
MOST POPULAR CLOUD APPS

Microsoft Office 365 is leading the way in existing cloud app deployments (41%) as well as planned future deployments (20%). Salesforce follows second and is already deployed in 27% of organizations and planned for future deployment in 7% of organizations. The migration to Office 365 is one of the biggest changes to enterprise IT in recent years. It represents yet another step in the migration of enterprises to a utility-based model for IT services delivery that started with Salesforce.com many years ago.

Q: What types of business applications is your organization deploying in the cloud?

Web-based applications and websites (47%), collaboration and communication tools (38%) and productivity tools (33%) are the most popular types of business applications deployed in the cloud.

Application development / testing 26% | Sales & Marketing 25% | HR 25% | Business intelligence / analytics 24% | Disaster recovery / storage / archiving 24% | Content management 22% | Finance & accounting 19% | Supply chain management 11% | Not sure/Other 20%
Cloud security concerns are on the rise. An overwhelming majority of 91% of organizations are very or moderately concerned about public cloud security. Today, perceived security risks are the single biggest factor holding back faster adoption of cloud computing. And yet, adoption of cloud computing is on the rise. The overwhelming benefits of cloud computing should drive organizations and security teams to find a way to “get cloud done”. This is a prime example to where security can have a profound impact on enabling business transformation.

Q: Please rate your level of overall security concern related to adopting public cloud computing

- 44% Very concerned
- 47% Moderately concerned
- 4% Not sure
- 5% Not at all concerned

91% organizations have security concerns
A majority of respondents say they did not experience a cloud-related security incident. 36% can’t disclose or aren’t sure about security incidents, indicating a lack of visibility into cloud security.

Q: Did your organization experience a cloud-related security incident in the last 12 months?
We continue to see evidence that the perception of cloud security is slowly improving relative to traditional enterprise IT environments. The share of organizations that see a higher risk of security breaches in the cloud compared to traditional IT environments is shrinking to 21% compared to last year’s 28%.

Q: Compared to your traditional IT environment, would you say the number of security breaches you experienced in a public cloud is?

- **22%** Lower risk of security breaches compared to on-premise
  - Significantly lower (7%)
  - Somewhat lower (15%)
- **30%** About the same
- **21%** Higher risk of security breaches compared to on-premise
  - Significantly higher (5%)
  - Somewhat higher (16%)
- **0%** unchanged from last year
- **7%** p.p. from last year
Perceptions of SaaS security are slowly improving, thanks to continued investments in security controls and customer education. For the first time since we asked this survey question, a majority of over 52% believe that cloud apps are as secure or more secure than on-premises applications, up from only 40% in last year’s survey. The math is simple: Large cloud providers can outspend any enterprise in securing their infrastructure and apply expertise and manpower that is better utilized in protecting a shared infrastructure. The results are superior in terms of availability, performance and security of cloud environments.

Q: Do you believe public cloud apps/SaaS like Salesforce and Office 365 are more or less secure than your internally hosted applications?

- Public cloud apps are more secure than internal apps: 17%
- Public cloud apps are about as secure as internal apps: 35%
- Public cloud apps are less secure than internal apps: 33%
- Not sure: 15%

52% Believe that cloud apps are as secure or more secure than on-premises applications
Unauthorized access through misuse of employee credentials and improper access controls is the single biggest threat (53%) to cloud security. This is followed by hijacking of accounts (44%) and insecure interfaces/APIs (39%). 33% of organizations say external sharing of sensitive information is the biggest security threat. Identity management and access control is an emerging and increasing threat concern for enterprises scaling and on-boarding to the cloud. The good news is that all these risks can be addressed by using security controls including multi-factor authentication, Identity and Access Management (IAM), Cloud Access Security Brokers (CASB), IP range restrictions and access auditing.

---

**BIGGEST SECURITY THREATS IN PUBLIC CLOUDS**

Q: What do you consider the biggest security threats in public clouds?

1. Unauthorized access - 53%
2. Hijacking of accounts - 44%
3. Insecure interfaces/APIs - 39%
4. External sharing of data - 33%

Additional threats include:
- Posting of confidential proprietary data by employees 33%
- Malicious insiders 32%
- Denial of service attacks 31%
- Foreign state sponsored cyber attacks 30%
- Malware injection 25%
- Abuse of cloud services 24%
- Shared memory attacks 18%
- Lateral movement of threats (east-west traffic) 16%
- Theft of service 15%
- Lost mobile devices 12%
- Natural disasters 5%
- Not sure/Other 9%

Q: What do you consider the biggest security threats in public clouds?
Data loss, leakage and privacy continue to top the list of cloud related security concerns, virtually unchanged from last year’s survey findings. Concerns about legal and regulatory compliance have seen the biggest gain, moving from the number 7 spot (24%) to number 4 (39%) on the list, in line with the observed rise of compliance concerns as a key barrier to cloud adoption.

Q: What are your biggest cloud security concerns?

49% Data loss/leakage
46% Data privacy
42% Confidentiality
39% Legal and regulatory compliance

- Data sovereignty/control 34%
- Accidental exposure of credentials 26%
- Lack of forensic data 26%
- Incident & problem management 25%
- Visibility & transparency 19%
- Availability of services, systems and data 17%
- Liability 17%
- Disaster recovery 13%
- Performance 13%
- Business continuity 13%
- Fraud (e.g. account hijacking) 12%
- Not sure/Other 5%
- None 1%
Verifying security policies (51%), visibility into infrastructure security (49%) and compliance (37%) were named as the top three cloud security challenges that cause the biggest headaches for IT security professionals. Because the cloud is a new environment, that is often incompatible with existing security technologies, there is a need for a new holistic security model to cover both on-premise and cloud environments. The holy grail is a unified security policy that can be applied across the infrastructure regardless of the underlying assets.

Q: What are your biggest cloud security headaches?

51% Verifying security policies
49% Visibility to infrastructure security
37% Compliance

No automatic discovery / visibility / control to infrastructure security 32% | Reporting security threats and solutions 31% | Remediation threats 29% |
Security can’t keep up with pace of changes to new / existing applications 27% | Can’t identify misconfigurations quickly 26% |
Complex cloud to cloud / cloud to on prem security rule matching 21% | Unknown / hidden open IP port 20% |
Automatically enforcing of security across multiple datacenters 18% | IaaS / PaaS security rules limit / cap 15% |
Lack of integration with on-premise security technologies 12% | Too much time and resource management overhead 11% |
Lack of feature parity with on-premise security solution 9% | No flexibility 7% | Native to cloud application or cloud infrastructure 5% | None 4% |
Not sure/Other 15%
Employee access to private cloud storage is one of the biggest risk factors regarding data leakage and theft - and organizations are responding accordingly. 42% of organizations do not allow employees to access private cloud storage services from the company’s network – 36% do allow access. This is a notable reversal of last year’s survey findings where only 36% of organizations did not allow access to cloud storage services. Identifying the use of unauthorized cloud services (“Shadow IT”) remains a major visibility challenge.

Q: Are employees allowed to access personal cloud storage services (those registered to a personal email address) from the company’s network?
Organizations moving to the cloud are faced with new security challenges that cannot be addressed with traditional security approaches. Secure clouds cannot exist without the right cloud security expertise. 61% of organizations plan to train and certify existing IT staff in cloud security to ensure the proper cloud security controls are being implemented both internally and with third party cloud service providers. Organizations realize that their IT teams need to stay current on evolving cloud technologies, threats and mitigation strategies. In addition, 45% of organizations plan to partner with a managed security services provider and 42% deploy additional security software to protect data and applications in the cloud.

Q: When moving to the cloud, how do you plan to handle your security needs?

- Train and certify existing IT staff: 61%
- Partner with a managed services provider who will provide the resources: 45%
- Use security software from independent software vendor(s): 42%
- Add security staff dedicated to cloud security issues: 23%
- Hire Professionals: 23%
- Look at different security-as-a-service providers to outsource - 24x7 monitoring: 17%
- Not sure/Other: 19%
Setting and enforcing security policies across cloud environments is by far the most requested capability to increase confidence in public clouds.

56% Setting and enforcing security policies across clouds

39% Ability to create data boundaries
38% APIs for reporting, auditing and alerting on security events
37% Effective mapping of security controls for internally-hosted applications to the cloud infrastructure
34% Isolation/protection of virtual machines
33% Ability to compare security levels across cloud providers

Q: Which of the following would most increase your confidence in adopting public clouds?

- Improved Security compared to self-managed deployment 30%
- Organization certification 29%
- High-integrity infrastructure 27%
- Regulatory oversight 25%
- Protecting workloads 15%
- Not sure/Other 13%
Most traditional security tools have not been designed for cloud environments and the unique challenges cloud adoption presents. The survey results confirm that traditional tools work somewhat or not at all for over half of cybersecurity professionals (59%). Only 14% feel that traditional security tools are sufficient to manage security across the cloud. The gap, say those surveyed, is primarily in both verifying security policies and visibility into infrastructure security. This is a great example of the dissolving perimeter. Together with mobility, the need to secure access from anywhere (mobile users, branch locations) to anywhere (physical datacenter, cloud datacenter and public cloud apps) breaks the traditional network topology and perimeter defense. The resulting proliferation in point security solutions is putting additional pressure on short handed security teams, as experienced security staff is still scarce.

Q: How well do your traditional network security tools / appliances work in public cloud environments?
Virtually unchanged from last year’s cloud security survey, encryption of data at rest (65%) and in motion on networks (57%) tops the list of most effective security controls to protect data in the cloud. This is followed by intrusion detection and prevention (IDP) with 48% and access control technologies such as Cloud Access Security Brokers (CASB) and Identity and Access Management (IAM) with 45%.

65%  Data encryption
57%  Network encryption
48%  Intrusion detection & prevention

Trained cloud security professionals 45%  |  Access control (e.g. CASB / Cloud Access Security Brokers) 45%  |  Log management and analytics 43%  |  Firewalls / NAC 40%  |  Data leakage prevention 40%  |  Endpoint security controls 40%  |  Patch management 38%  |  Network monitoring 37%  |  Single sign-on / user authentication 35%  |  Anti-virus / Anti-malware 35%  |  Employee usage monitoring 29%  |  Mobile device management (MDM) 25%  |  Database scanning and monitoring 24%  |  Content filtering 24%  |  Security Information and Event Management (SIEM) 22%  |  Cyber forensics 21%  |  Not sure/Other 12%

Q: What security technologies and controls are most effective to protect data in the cloud?
The most prevalent cloud security controls include multi-factor authentication in nearly half of organizations. One in four organizations deploy additional security mechanisms.

- **45%** use multi-factor authentication for access control.
- **43%** use encryption or tokenization to protect data in the cloud.
- **41%** use intrusion detection & prevention.
- **40%** use security services offered by the cloud provider.

Organizations deploy additional security mechanisms:

- We deploy additional security services offered by third party vendors 25%
- We don’t protect data in the cloud 5%
- Not sure/Other 21%

Q: How do you protect data in the cloud?
Faster time to deployment (47%), reduced software maintenance efforts (40%) and direct web access from any location (35%) are the dominant drivers for cloud-based security solutions.

Placing security in the cloud provides significant ROI benefits for businesses. It breaks the traditional “appliance model” of security: Instead of physical constraints, patch and upgrade cycles, and need for a local IT support, the cloud enables a security model that is up to date, always patched, elastic and scalable, and available everywhere.

Q: What are the main drivers for considering Cloud-based Security Solutions?
On the flipside, data privacy (56%), compliance (43%) and platform integrity (39%) are the main barriers to cloud-based security solutions.

These concerns apply to cloud in general. Using regional cloud instances to comply with data localization requirements, minimizing personal data storage, and demonstrating tight security controls around the platform should make cloud-based security the default security delivery model. This way, cloud computing can offer a compelling alternative to on-premise security in the face of emerging threats, shrinking budgets and scarce expertise.
A majority of organizations are taking proactive measures to protect their business applications. We dug deeper to find out how companies were protecting their applications. The most popular application security measures are penetration testing (59%) followed by web application firewalls (54%) and developer education (47%).

Q: What Application Security measures are you taking in order to protect your business applications?
The vast majority of organizations surveyed (55%) use Active Directory on premise as the authoritative directory to identify, authenticate and authorize access to cloud applications. Consequently, access to cloud based applications for a majority of organizations depends heavily on proper security controls around on-premise Active Directory infrastructure. The cloud enablement of Active Directory is a key enabler for moving to cloud-based security infrastructure.

Q: What is the authoritative directory you use for identity data and authentication, and authorization of access for your cloud based applications?

<table>
<thead>
<tr>
<th>Directory Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>On premise Active Directory (synchronization)</td>
<td>28%</td>
</tr>
<tr>
<td>On premise Active Directory (federation)</td>
<td>27%</td>
</tr>
<tr>
<td>On premise LDAP Directory (Non Microsoft)</td>
<td>8%</td>
</tr>
<tr>
<td>Cloud based Directory only - AzureAD</td>
<td>4%</td>
</tr>
<tr>
<td>Cloud based Directory only - Amazon Simple AD</td>
<td>3%</td>
</tr>
<tr>
<td>None</td>
<td>7%</td>
</tr>
</tbody>
</table>

Not sure/Other: 23%
46% of respondents state that security slows down continuous development methods like DevOps, another 15 percent noted that security is ignored completely in their DevOps process.

59% of respondents indicated that agility and accelerated deployments are among the cloud adoption benefits, yet security slows down DevOps. Utilization of “built for the cloud” security products provides security governance directly integrated into the DevOps process and is key to fully realizing the benefits of the cloud.
The Cloud Security Spotlight Report is based on the results of a comprehensive survey of 2,200 professionals across a broad cross-section of organizations about their adoption of cloud computing and security related concerns and practices.

The 2,200 respondents range from technical executives to managers and practitioners, and they represent organizations of varying sizes across many industries. Their answers provide a comprehensive perspective on the state of cloud security today.

**CAREER LEVEL**

<table>
<thead>
<tr>
<th>Career Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specialist</td>
<td>25%</td>
</tr>
<tr>
<td>Manager / Supervisor</td>
<td>19%</td>
</tr>
<tr>
<td>Consultant</td>
<td>17%</td>
</tr>
<tr>
<td>Director</td>
<td>14%</td>
</tr>
<tr>
<td>Owner / CEO / President</td>
<td>7%</td>
</tr>
<tr>
<td>CTO, CIO, CISCO, CMO, CFO, COO</td>
<td>6%</td>
</tr>
<tr>
<td>Vice President</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>8%</td>
</tr>
</tbody>
</table>

**DEPARTMENT**

<table>
<thead>
<tr>
<th>Department</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security</td>
<td>52%</td>
</tr>
<tr>
<td>IT Operations</td>
<td>20%</td>
</tr>
<tr>
<td>Engineering</td>
<td>9%</td>
</tr>
<tr>
<td>Operations</td>
<td>6%</td>
</tr>
<tr>
<td>Compliance</td>
<td>4%</td>
</tr>
<tr>
<td>Sales</td>
<td>3%</td>
</tr>
<tr>
<td>Product Management</td>
<td>2%</td>
</tr>
<tr>
<td>Marketing</td>
<td>2%</td>
</tr>
<tr>
<td>Finance</td>
<td>2%</td>
</tr>
<tr>
<td>Legal</td>
<td>2%</td>
</tr>
<tr>
<td>HR</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

**COMPANY SIZE**

<table>
<thead>
<tr>
<th>Company Size</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fewer than 10</td>
<td>11%</td>
</tr>
<tr>
<td>10-99</td>
<td>13%</td>
</tr>
<tr>
<td>100-999</td>
<td>19%</td>
</tr>
<tr>
<td>1,000-4,000</td>
<td>16%</td>
</tr>
<tr>
<td>5,000 – 10,000</td>
<td>9%</td>
</tr>
<tr>
<td>Over 10,000</td>
<td>32%</td>
</tr>
</tbody>
</table>

**INDUSTRY**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology, Software &amp; Internet</td>
<td>20%</td>
</tr>
<tr>
<td>Government</td>
<td>18%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>12%</td>
</tr>
<tr>
<td>Professional Services</td>
<td>8%</td>
</tr>
<tr>
<td>Healthcare, Pharmaceuticals, &amp; Biotech</td>
<td>8%</td>
</tr>
<tr>
<td>Education &amp; Research</td>
<td>6%</td>
</tr>
<tr>
<td>Computers &amp; Electronics</td>
<td>5%</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>5%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>3%</td>
</tr>
<tr>
<td>Energy &amp; Utilities</td>
<td>3%</td>
</tr>
<tr>
<td>Retail</td>
<td>3%</td>
</tr>
<tr>
<td>Non-Profit</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>
CloudPassage

CloudPassage® Halo® is the world’s leading agile security platform that provides instant visibility and continuous protection for servers in any combination of data centers, private clouds and public clouds. The Halo platform is delivered as a service, so it deploys in minutes and scales on-demand. Halo uses minimal system resources; so layered security can be deployed where it counts, right at every workload – servers, instances and containers. Leading enterprises like Citrix, Salesforce.com and Adobe use CloudPassage today to enhance their security and compliance posture, while at the same time enabling business agility.