INTRODUCTION

Organizations continue to adopt cloud computing at a rapid pace to benefit from increased efficiency, better scalability, and faster deployments.

As more workloads are shifting to the cloud, cybersecurity professionals remain concerned about security of data, systems, and services in the cloud. To cope with new security challenges, security teams are forced to reassess their security posture and strategies as traditional security tools are often not suited for the challenges of dynamic, virtual and distributed cloud environments. This technology challenge is only exacerbated by the dramatic shortage of skilled cybersecurity professionals.

This report has been produced by the 400,000 member Information Security Community on LinkedIn in partnership with Cybersecurity Insiders to explore how organizations are responding to the security threats in the cloud, and what tools and best practices IT cybersecurity leaders are considering in their move to the cloud.

Many thanks to our sponsors for supporting this exciting research project: Alert Logic | AlienVault | Bitglass | Cavirin | CloudPassage | Dome9 Security | Edgile | Evident.io | GoAnywhere | HelpSystems | (ISC)² | Securonix | Sift Security

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Holger.Schulze@Cybersecurity-Insiders.com
Cloud security concerns – While adoption of cloud computing continues to surge, security concerns are showing no signs of abating. Reversing a multi-year downward trend, nine out of ten cybersecurity professionals confirm they are concerned about cloud security, up 11 percentage points from last year’s cloud security survey. The top three cloud security challenges include protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent).

Biggest threats to cloud security – Misconfiguration of cloud platforms jumped to the number one spot in this year’s survey as the single biggest threat to cloud security (62 percent). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

Cloud security headaches – As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top three security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent), compliance (38 percent), and setting consistent security policies across cloud and on-premises environments (35 percent).

Legacy security tools limited in the cloud – Only 16 percent of organizations report that the capabilities of traditional security tools are sufficient to manage security across the cloud, a 6 percentage point drop from our previous survey. Eighty-four percent say traditional security solutions either don’t work at all in cloud environments or have only limited functionality.

Paths to stronger cloud security – For the second year in a row, training and certification of current IT staff (57 percent) ranks as the most popular path to meet evolving security needs. Fifty percent of respondents use their cloud provider’s security tools and 35 percent deploy third-party security software to ensure the proper cloud security controls are implemented.

Cloud security budgets increase – Looking ahead, close to half of organizations (49 percent) expect cloud security budgets to go up, with a median budget increase of 28 percent.
# TABLE OF CONTENTS

- **CLOUD SECURITY CHALLENGES** 5
- **CLOUD SECURITY SOLUTIONS** 13
- **CLOUD ADOPTION TRENDS** 24
- **METHODOLOGY & DEMOGRAPHICS** 33
- **SPONSORS OVERVIEW** 34
- **CONTACT US** 37
CLOUD SECURITY CHALLENGES
While adoption for public cloud computing continues to surge, security concerns are showing no signs of abating. An overwhelming majority of cybersecurity professionals (91 percent) say they are extremely to moderately concerned about public cloud security, up 11 percentage points from last year.

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

Organizations are concerned about cloud security

- 91% Concerned
- 38% Very concerned
- 31% Moderately concerned
- 22% Extremely concerned
- 7% Slightly concerned
- 2% Not at all concerned
In the past 12 months, 18 percent of organizations have experienced a cloud security incident, a significant increase over the previous year. The rise in observed cloud security incidents further serves to support the increased security concerns related to adoption of cloud computing.

Did your organization experience a cloud related security incident in the last 12 months?

- **YES** 18%
- **NO** 64%
- **NOT SURE** 18%
While cloud providers offer many security measures, customer organizations are ultimately responsible for securing their own workloads in the cloud. The top three cloud security challenges highlighted by cybersecurity professionals in our survey are protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent) – all up compared to the previous year.

Concerns about accidental exposure have seen the biggest gain compared to last year, moving from the number 6 spot (26 percent in 2017) to number 4 (47 percent in 2018) on the list.

What are your biggest cloud security concerns?

- Data loss/leakage: 67%
- Data privacy: 61%
- Confidentiality: 53%
- Accidental Exposure: 47%
- Legal and regulatory compliance: 46%
- Data sovereignty/control: 46%

Lack of forensic data 37% | Incident response 35% | Visibility & transparency 34% | Fraud (e.g., theft of SSN records) 27% | Liability 25% | Availability of services, systems and data 21% | Business continuity 18% | Disaster recovery 18% | Performance 16% | Other 7%
As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top two security control challenges SOCs are struggling with are visibility into infrastructure security (43 percent) and compliance (38 percent). Setting consistent security policies across cloud and on-premises environments (35 percent) is tied with security not keeping up with the pace of change in applications (35 percent).

What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

- **Visibility into infrastructure security**: 43%
- **Compliance**: 38%
- **Setting consistent security policies**: 35%
- **Security can't keep up with pace of change in applications**: 35%
- **Lack of integration with on-premises security technologies**: 34%
- **No automatic discovery/visibility/control to infrastructure security**: 33%
- **Can't identify misconfiguration quickly**: 31%
- **Complex cloud to cloud on-premises security rule matching**: 30%

Reporting security threats 27% | Remediating threats 23% | Automatically enforcing security across multiple datacenters 23% | Lack of feature parity with on-premises security solution 21% | No flexibility 8% | Not sure/other 16%
Misconfiguration of the cloud platform jumped to the number one spot in this year’s survey as the single biggest threat to cloud security (62 percent).

This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

What do you think are the biggest security threats in public clouds?

- **#1**: Misconfiguration of the cloud platform/wrong set-up (62%)
- **#2**: Unauthorized access (55%)
- **#3**: Insecure interfaces/APIs (50%)
- **#4**: Hijacking of accounts, services or traffic (47%)

- External sharing of data (39%)
- Foreign state sponsored cyberattacks (33%)
- Malicious insiders (30%)
- Malware/ransomware (26%)
- Denial of service attacks (22%)

Theft of service 12% | Lost mobile devices 7% | Not sure/other 7%
Organizations continue to believe public clouds are at higher risk of security breaches than traditional on-premises environments (49 percent), an 8 percent increase relative to last year’s 41 percent.

The respondents who believe that public clouds are less risky to security breaches decreased proportionally (at 17 percent, a 6 percent drop compared to last year’s 23 percent), further supporting the perception that the use of public clouds increases the probability of becoming a target for a cyberattack.

Compared to traditional IT environments, what would you say is the risk of security breaches in a public cloud environment?

- **49%** Higher risk of security breaches compared to on-premises
  - Significantly higher (20%)
  - Somewhat higher (29%)

- **17%** Lower risk of security breaches compared to on-premises
  - Significantly lower (1%)
  - Somewhat lower (16%)

- **20%** About the same

- **4%** Not sure
Perceptions of SaaS security remain relatively unchanged this year. A majority, 57 percent, believe that cloud apps are as secure or more secure than on-premises applications, down slightly from 58 percent in last year’s survey.

Are public cloud apps/SaaS (such as Salesforce and Office 365) more or less secure than on-premises applications?

- **Public cloud apps are more secure than our on-premises apps**: 20%
- **About the same**: 37%
- **Public cloud apps are less secure than our on-premises apps**: 25%
- **Not sure**: 18%
As more workloads move into the cloud, organizations are faced with unique security challenges that cloud adoption presents. Traditional network security tools made sense when an organization’s users and applications were hosted in a static centralized data center. Many of these legacy security tools/appliances are not designed for the dynamic, distributed virtual environment of the cloud.

Only 16 percent feel that traditional security tools are sufficient to manage security across the cloud, a six percent point drop from our previous survey. Eighty-four percent of respondents say traditional security solutions either don’t work at all in cloud environments or have only limited functionality, up six percent points from the previous year (78 percent).

How well do your traditional network security tools/appliances work in cloud environments?

- **60%** Limited functionality
- **24%** Our traditional network security tools don’t work in the cloud
- **16%** All capabilities work in the cloud
- **84%** claim traditional security solutions either don’t work at all or have limited functionality
Organizations recognize several key advantages of deploying cloud-based security solutions. As in previous years, respondents selected faster time to deployment (47 percent) along with cost savings (47 percent) at the number one factors for selecting cloud-based security solutions.

What are the main drivers for considering cloud-based security solutions?

- Faster time to deployment: 47%
- Cost savings: 47%
- Need for secure app access from any location: 37%
- Reduced effort around patches and upgrades of software: 33%
- Meet cloud compliance expectations: 33%
- Better visibility into user activity and system behavior: 30%
- Reduction of appliance footprint in branch offices: 26%
Despite the significant advantages offered by cloud-based security solutions, barriers to adoption still exist. When it comes to business transformation and cloud adoption, three important aspects must be aligned; people, process and technology.

Our survey reveals that the biggest challenge organizations are facing is not technology, it’s people and processes. Staff expertise and training (56 percent) ranked number one in the survey, followed by data privacy concerns (41 percent) and lack of integration with on-premises technology (37 percent).

**BARRIERS TO CLOUD-BASED SECURITY ADOPTION**

---

What are the main barriers to migrating to cloud-based security solutions?

- **56%** Staff expertise/training
- **41%** Data privacy
- **37%** Lack of integration with on-premises security technologies

**Other important barriers**:

- **34%** Regulatory compliance requirements
- **32%** Solution maturity
- **30%** Data residency
- **26%** Budget
- **22%** Integrity of cloud security platform (DDoS attack, breach)

Limited control over encryption keys 21% | Sunk cost into on-premises tools 19% | Scalability and performance 11% | Not sure/other 14%

---
In a data-driven economy, it is imperative that organizations protect and secure workloads in the cloud. As in previous years, data and network encryption technologies top the list as the most effective security technologies (data encryption at 64 percent and network encryption at 54 percent) followed by Security Information and Event Management (SIEM) (52 percent).

What security technologies and controls are most effective to protect data in the cloud?

- **Data encryption**: 64%
- **Network encryption**: 54% (VPN, packet encryption, transport encryption)
- **Security Information and Event Management (SIEM)**: 52%
- **Trained cloud security professionals**: 51%
- **Intrusion detection and prevention**: 50%
- **Vulnerability assessment**: 49%
- **Access control (e.g., CASB/Cloud Access Security Brokers)**: 49%
- **Log management and analytics**: 47%
- **Privileged Access Management (PAM)**: 47%
- **Data leakage prevention**: 46%

Additional technologies: Patch management 46% | Configuration management 46% | Single sign-on/user authentication 43% | Endpoint security controls 42% | Firewalls/NAC 41% | Network monitoring 39% | Anti-virus/anti-malware 37% | Application security scanners 32% | Secure managed file transfer 30% | Employee usage monitoring 30% | Mobile Device Management (MDM) 30% | Database scanning and monitoring 26% | Cloud asset discovery 23% | Cyber forensics 22% | Content filtering 22% | Not sure/other 20%
With use of the cloud increasing every year, more data is stored in cloud environments. For the second year in a row, cybersecurity professionals say access controls (65 percent) are the primary method to protect data in the cloud, followed by encryption (59 percent).

This year, the use of security services offered by the cloud provider (53 percent) jumped from fourth place to third, suggesting that organizations are looking toward their service providers to help provide additional data protection and risk mitigation as part of their services stack.

How do you protect data in the cloud?

- **65%** We use access controls
- **59%** We use encryption or tokenization
- **53%** We use security services offered by the cloud provider
- **46%** We connect to the cloud via protected networks

We deploy cloud security monitoring tools 41% | We deploy additional security services offered by third-party vendors 35% | We don’t protect data in the cloud 4% | Not sure/other 15%
As organizations adopt the cloud, many recognize the need to partner with security providers for robust protection capabilities not available in-house.

The top five attributes cybersecurity professionals look for in a cloud security provider include cloud native security tools (68 percent), cost effectiveness (64 percent), seamless integration with cloud platforms (57 percent), ease of deployment (53 percent) and demonstrated cloud knowledge (50 percent) — all are ranked by at least 50 percent of the survey participants, suggesting that SOCs are looking for a broad array of capabilities.

What do you look for in your cloud security provider?

- Security tools are cloud native (are agile, can be deployed with automation, support scalability, etc.)
- Cost effectiveness
- Integrates seamlessly with cloud platforms
- Ease of deployment
- Demonstrates cloud knowledge

Not sure/other 11%
For the second year in a row, training and certifying current IT staff (57 percent) ranked number one by organizations to assure that their evolving security needs are met. Fifty percent of respondents use their cloud provider’s security tools and 35 percent deploy third-party security software to ensure the proper security controls are implemented across on-premises and the cloud.

When moving to the cloud, how do you handle your changing security needs?

- **57%** Train and/or certify current IT staff
- **50%** Use cloud provider security tools (e.g., GuardDuty in AWS)
- **35%** Deploy security software from independent software vendor(s)
- **30%** Partner with a Managed Security Services Provider (MSSP)
- **28%** Hire staff dedicated to cloud security
- **1%** Look at security-as-a-service providers to outsource 24x7 monitoring

Not sure/other 19%
We asked organizations which actions cloud providers could take to improve their confidence in moving to the cloud. They identified five key confidence boosters to help alleviate their security concerns. Encrypting data-at-rest (49 percent) was the number one issue to address, followed by APIs for reporting, auditing and alerting on security events (46 percent), and setting and enforcing security policies across clouds (45 percent).

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

- Encryption of data-at-rest: 49%
- APIs for reporting, auditing and alerting on security events: 46%
- Setting and enforcing security policies across clouds: 45%
- Automating compliance: 39%
- Creating data boundaries: 39%
- Isolation/protection of virtual machines: 33%
- Limiting unmanaged device access: 31%
- Leveraging data leakage prevention tools: 29%
- Protecting workloads: 19%

Not sure/other 15%
Organizations realize that security training, certification and awareness is a key cornerstone in the defense against security breaches. Training and expertise remains the highest concern among IT professionals as the biggest barrier to better security management, a majority (67 percent) consider training and certification valuable to their employees in reducing risk and helping protect the organization from both internal and external cyber threats.

Security training is an important component of an organization’s security posture. A well planned security training program will ensure there is a continual focus on IT security, helping employees identify what data is protected, assessing risk, mitigating procedures, compliance requirements, and how often the program will be revised and refreshed.

A majority, 59 percent, see their security training program as very or somewhat effective.

What percentage of your employees would benefit from security training and/or certification for their job?

Consider training and certification valuable to their employees in reducing risk and helping protect the organization

67%

How effective is your current security training program?

Very effective

Very ineffective

Somewhat ineffective

Neither effective nor ineffective

Not sure

59%

See their security training program as very or somewhat effective.

46%

Somewhat effective

14%

13%

13%

8%

6%
The survey reveals that organizations are recognizing the growing significance of cloud security threats and are investing resources accordingly. Looking ahead, close to half of organizations (49 percent) expect budget increases. Twenty-four percent expect their IT budgets to remain flat, while only 6 percent foresee their cloud security funding to shrink.

When asked about the degree of their security budget increases, cybersecurity professionals anticipate their program funding would increase by 28 percent, on average.
CLOUD ADOPTION TRENDS
SaaS remains the most deployed cloud model (52 percent) as software stacks are maturing, followed by IaaS (36 percent) and PaaS (28 percent), both showing strong adoption by organizations. To a lesser extent, newer deployment models such as BPaaS (11 percent) and FaaS (10 percent) have lower rates of production deployments.

What is your organization’s adoption of cloud computing?

<table>
<thead>
<tr>
<th>Cloud Model</th>
<th>Deployed/in production</th>
<th>Currently implementing</th>
<th>Trial/pilot in progress</th>
<th>Planning to deploy</th>
<th>No plans to deploy</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS (Software as a Service)</td>
<td>52%</td>
<td>16%</td>
<td>9%</td>
<td>10%</td>
<td>13%</td>
</tr>
<tr>
<td>IaaS (Infrastructure as a Service)</td>
<td>36%</td>
<td>18%</td>
<td>17%</td>
<td>15%</td>
<td>14%</td>
</tr>
<tr>
<td>PaaS (Platform as a Service)</td>
<td>28%</td>
<td>19%</td>
<td>14%</td>
<td>18%</td>
<td>21%</td>
</tr>
<tr>
<td>BPaaS (Business Process as a Service)</td>
<td>11%</td>
<td>9%</td>
<td>9%</td>
<td>18%</td>
<td>53%</td>
</tr>
<tr>
<td>FaaS (Function as a Service)</td>
<td>10%</td>
<td>8%</td>
<td>10%</td>
<td>16%</td>
<td>56%</td>
</tr>
</tbody>
</table>
Over the past few years, public cloud providers have continued to mature and expand their service offerings. The two biggest cloud providers continue to compete for the lead in our survey: Amazon Web Services (72 percent) and Microsoft Azure (71 percent). Interestingly, Rackspace Cloud (67 percent) displaced Google Cloud Platform (54 percent) among our survey participants to claim third place this year.

What cloud IaaS provider(s) do you currently use or plan to use in the future?
Forty percent of organizations say their primary cloud deployment strategy is a hybrid cloud, optimizing their investment by integrating multiple cloud providers to work together as a single seamless environment. The remaining respondents equally said their cloud deployment of choice was either a single cloud (30 percent) or a non-integrated, multi-cloud solution (30 percent).

The growing trend is organizations are leveraging more than one cloud provider for a multitude of reasons, ranging from high availability (HA), disaster recovery (DR) and multi-vendor sourcing strategy to name a few.

What is your primary cloud deployment strategy?

- **30%** Single Cloud
- **30%** Multi-Cloud (e.g. multiple providers without integration)
- **40%** Hybrid (e.g. integration between multiple providers, managed as a single cloud)
As organizations become more comfortable using cloud services, more are considering cloud for broader categories of services beyond email and sales force automation. These include mission-critical and production-grade applications.

The top three cloud services and workloads that organizations are deploying are productivity applications (48 percent), computing (46 percent) and storage (44 percent).

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

- **Productivity applications**
  (email, collaboration, instant messaging, etc.)
  - 48%

- **Storage**
  (object storage, archive, backup, etc.)
  - 44%

- **Business applications**
  (CRM, marketing automation, ERP, BI, project management, etc.)
  - 39%

- **Computing**
  (servers, containers, etc.)
  - 46%

- **Security**
  (Identity management, access control, data protection, threat detection, usage & resource monitoring, anti-virus, etc.)
  - 40%

- **Database** (relational, NoSQL, caching, etc.)
  - 37%

- **Virtualization**
  - 37%

- **Developer/Testing Applications**
  - 37%

- **Networking** (virtual private cloud, DNS, etc.)
  - 34%

- **IT Operations Applications** (administration, backup, provisioning monitoring, etc.)
  - 31%

- **Operating System**
  - 29%

- **Middleware**
  - 17%

- **Runtime**
  - 10%

- **Not sure/other**
  - 22%
Software as a Service (SaaS) has become the de facto delivery model for organizations to consume many core business applications, replacing traditional on-premises applications. These business applications include email, collaboration, customer relationship management, human resources, marketing automation, business intelligence, storage and many more.

In this year’s survey, a majority of respondents deploy Microsoft’s productivity suite, Office 365 (71 percent), followed by Microsoft’s online email service, Microsoft Exchange (33 percent). Rounding out the top five most popular SaaS apps are Salesforce (33 percent), ServiceNow (28 percent) and Dropbox (24 percent).

Which of the following cloud SaaS services are currently deployed in your organization?

- Microsoft Office 365: 71%
- Microsoft Exchange: 33%
- Salesforce: 33%
- ServiceNow: 28%
- Dropbox: 24%
- Google Apps: 22%
- Box: 15%
- Workday: 13%
- SAP HANA: 7%
- SAP SuccessFactors: 5%
- SAP Hybris: 2%
- Not sure/other: 19%
It’s no surprise that for a third year in a row, email is the most common information stored in the cloud (57 percent), a 13 point increase over last year’s survey. Notably, a reversal in trend this year, an increasing number of organizations indicate they are storing more of their intellectual property information in the cloud.

This re-enforces our findings that organizations are more comfortable with investing and moving their business-critical applications and data to the cloud. Sales and marketing data (37 percent) jumped from fourth place to second place this year, and tied for third place are DevOps and customer data at 35 percent.

What types of corporate information do you store in the cloud?
How does the reality of cloud computing hold up against the promise of reduced cost, increased agility, accelerated time-to-market or improved uptime?

Sixty-six percent of the IT professionals surveyed said their cloud investments are meeting or exceeding expectations. Notably, about one out of five respondents (21 percent) were unsure if the cloud had delivered on the promised benefits to the organization.

How has cloud computing delivered on the promised benefits for your organization?

- 66% think their cloud investments are meeting or exceeding expectations
- 54% As expected
- 12% Better than expected
- 21% Not sure
- 13% Worse than expected
It’s important to recognize that with all of the benefits, cloud is not without its challenges. Lack of qualified staff or expertise tops the list as the primary barrier to cloud adoption (42 percent), moving up one spot from second place last year. Tied for second place this year are general security risks and integration with existing IT environments at 39 percent.

The survey highlights a number of technical and organizational barriers that continue to hinder cloud adoption, as cloud technologies continue to mature, many of these barriers will be easier to overcome for organizations.

What are the biggest barriers holding back cloud adoption in your organization?

- Data security, loss & leakage risks: 38%
- Legal & regulatory compliance: 34%
- Loss of control: 27%
- Internal resistance and inertia: 24%
- Fear of vendor lock-in: 22%
- Lack of staff resources or expertise: 42%
- General security risks: 39%
- Integration with existing IT environment: 39%
- Lack of maturity of cloud service models: 21%
- Complexity managing cloud deployment: 20%
- Lack of transparency and visibility: 19%
- Lack of management buy-in: 17%
- Lack of budget: 15%
- Cost/lack of ROI: 14%
- Billing & tracking issues: 12%
- Performance of apps in the cloud: 11%
- Dissatisfaction with cloud service offerings/performance/pricing: 10%
- Lack of customizability: 10%
- Lack of support by cloud provider: 7%
- Availability: 4%
- Not sure/other: 15%
The 2018 Cloud Security Report is based on the results of a comprehensive online survey of over 570 cybersecurity and IT professionals to gain deeper insight into the state of cloud adoption and security challenges, trends and best practices. The respondents range from security analysts and IT managers to CISOs, reflecting a representative cross section of organizations of varying sizes across different industries.

**METHODOLOGY & DEMOGRAPHICS**

**JOB LEVEL**

- Specialist: 20%
- Manager/Supervisor: 20%
- Consultant: 16%
- Director: 10%
- CTO, CIO, CISO, CMO, CFO, COO: 10%
- Owner/CEO/President: 5%
- Vice President: 3%
- Project Manager: 3%
- Owner/CEO/President: 13%

**DEPARTMENT**

- IT Security: 57%
- IT Operations: 13%
- Engineering: 7%
- Operations: 4%
- Product Management: 4%
- Compliance: 3%
- Other: 12%

**COMPANY SIZE**

- Less than 10: 8%
- 10-99: 12%
- 100-499: 11%
- 500-999: 8%
- 1,000-4,999: 16%
- 5,000-9,999: 11%
- 10,000 or more: 34%

**INDUSTRY**

- Technology, Software & Internet: 19%
- Government: 17%
- Financial Services: 15%
- Professional Services: 10%
- Healthcare, Pharmaceuticals & Biotech: 9%
- Education & Research: 7%
- Manufacturing: 5%
- Other: 18%
SPONSORS OVERVIEW

**Alert Logic** | [www.alertlogic.com](http://www.alertlogic.com)

Alert Logic® Security-as-a-Service solution delivers deep security insight and continuous protection for cloud, hybrid and on-premises data centers. Providing application, system and network protection from the cloud. The Alert Logic solution analyzes over 400 million events and identifies over 50,000 security incidents monthly for over 3,800 customers.

**AlienVault** | [www.alienvault.com](http://www.alienvault.com)

AlienVault has simplified the way organizations detect and respond to today’s ever evolving threat landscape. Our unique and award winning approach combines our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault’s Open Threat Exchange, making effective and affordable threat detection attainable for resource constrained IT teams.

**Bitglass** | [www.bitglass.com](http://www.bitglass.com)

Bitglass’ Cloud Access Security Broker (CASB) solution provides enterprises with end-to-end data protection from the cloud to the device. It deploys in minutes and works across apps like Office 365, Salesforce, and AWS. Bitglass also protects data on mobile devices without the hassles of MDM.

**Cavirin** | [www.cavirin.com](http://www.cavirin.com)

Cavirin provides risk, cybersecurity and compliance management for the enterprise hybrid cloud through automated discovery, security posture assessment, predictive analytics, and intelligent remediation guidance.

**CloudPassage** | [www.cloudpassage.com](http://www.cloudpassage.com)

CloudPassage Halo is the only workload security automation platform that offers on-demand delivery of security controls across data centers, private/public clouds, virtual machines and containers – at speed and scale.
SPONSORS OVERVIEW

**Dome9 Security** | **dome9.com**

Dome9, the public cloud security company, delivers peace of mind to enterprises through security and compliance automation as they scale in any cloud. With Dome9, organizations gain full visibility and control of their security posture, allowing them to minimize their attack surface and protect against vulnerabilities, identity theft, and data loss in the cloud. Dome9's agentless SaaS solution provides operational efficiency for faster time-to-protection. Enterprises choose Dome9 as their key partner to provide the active protection necessary throughout their cloud journey.

---

**Edgile** | **Edgile.com**

Edgile is the trusted cyber risk and compliance partner to the world’s leading organizations, providing consulting, managed services, and harmonized regulatory content. Our strategy-first model optimizes IAM, GRC, and cybersecurity both on-premises and in the cloud. By transforming risk into opportunity, we secure the modern enterprise through solutions that increase business agility and create a competitive advantage for our clients.

---

**Evident.io** | **www.evident.io**

Evident.io was founded to fill the need for security and compliance for public clouds. The Evident Security Platform (ESP) helps organizations gain visibility and automate policy enforcement across all their cloud infrastructure.

---

**GoAnywhere** | **www.goanywhere.com**

GoAnywhere Managed File Transfer is enterprise-level software for automating and securing your file transfers through a single interface. GoAnywhere's security and auditing features help you achieve compliance, increase security, and streamline processes.
SPONSORS OVERVIEW

HelpSystems | www.helpsystems.com

HelpSystems helps you protect business-critical data with a suite of integrated and automated security solutions for defense in depth, comprehensive visibility, and streamlined reporting across your on-prem and cloud environments.

(ISC)² | www.isc2.org/ccsp

(ISC)² is the largest not-for-profit membership body of certified cyber, information, software and infrastructure security professionals worldwide, with over 130,000 members. (ISC)²’s flagship certification is the CISSP®. In 2015, (ISC)² and the Cloud Security Alliance (CSA) partnered to launch the Certified Cloud Security Professional (CCSP®) credential for security professionals whose day-to-day responsibilities involve procuring, securing and managing cloud environments or purchased cloud services. (ISC)² offers education programs and services based on its CBK®.

Securonix | www.securonix.com

Securonix radically transforms enterprise security with actionable intelligence. Our purpose-built security analytics platforms mine, enrich, analyze, score and visualize data into actionable intelligence on the highest risk threats to organizations. Using signature-less anomaly detection techniques, Securonix detects data security, insider threat and fraud attacks automatically and accurately.

Sift Security | www.siftsecurity.com

Sift Security CloudHunter, automates the detection of misconfigurations and active threats across an organization’s public, private, and hybrid cloud infrastructure. CloudHunter correlates all your cloud data and provides unified visibility across multiple cloud service providers, actionable alerts, and enables rapid response, dramatically reducing the time and skill needed to investigate and respond to security events.
Want to see your brand featured in the next cybersecurity report? Contact Crowd Research Partners for more information.

| email | info@crowdresearchpartners.com |

Fact-based content
Sales-ready leads
Brand awareness

Visit Crowd Research Partners for more details

Produced by:

Crowd Research Partners
Cybersecurity INSIDERS
LinkedIn Group Partner Information Security

All Rights Reserved. Copyright 2018 Crowd Research Partners.