Cloud Security: From Start Point to End Point

By Melinda Cross
If there’s any doubt the IT world is becoming cloudier, consider these facts:

- Spending on public and private cloud products grew 48.4 percent year over year in Q2 of 2018 to **$15.4 billion**.

- Cloud IT infrastructure spending in 2018 is projected to grow 31.1 percent year over year to **$62.2 billion**.

- Quarterly spending on public cloud IT infrastructure has grown 58.9 percent over the last three years.
Cloud computing offers organizations competitive advantages such as increased speed, agility, scale and collaboration. But what often happens in the rush to the cloud is lapse in security. “Legacy security tools can’t keep up with the rapid pace of adoption,” explained Jeannie Walker, security manager at White Hat Security.
In a 2018 Gartner survey of more than 100 senior executives, cloud security was ranked the No. 1 risk facing organizations. Gartner estimates that up to 95 percent of all data leaks in the cloud through 2020 will be due to incorrect configuration, account management or mistakes by IT departments, rather than the vulnerability of the cloud provider.

One important distinction to understand in cloud security is who owns responsibility at each point. Providers cover only the security of the cloud itself, not customer data or customer use of the infrastructure. Specific security responsibilities are divided between the cloud service provider and cloud customer in different cloud service deployment environments — infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).

The chart opposite indicates key responsibilities by cloud provider and customer, and shows that data and application security is always the primary responsibility of the enterprise customer.
## Cloud Security Shared Responsibilities by Deployment Environments

<table>
<thead>
<tr>
<th></th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Security</strong></td>
<td><img src="image1.jpg" alt="Image" /></td>
<td><img src="image2.jpg" alt="Image" /></td>
<td><img src="image3.jpg" alt="Image" /></td>
</tr>
<tr>
<td><strong>Application Security</strong></td>
<td><img src="image4.jpg" alt="Image" /></td>
<td><img src="image5.jpg" alt="Image" /></td>
<td><img src="image6.jpg" alt="Image" /></td>
</tr>
<tr>
<td><strong>Middleware Security</strong></td>
<td><img src="image7.jpg" alt="Image" /></td>
<td><img src="image8.jpg" alt="Image" /></td>
<td><img src="image9.jpg" alt="Image" /></td>
</tr>
<tr>
<td><strong>Host Security</strong></td>
<td><img src="image10.jpg" alt="Image" /></td>
<td><img src="image11.jpg" alt="Image" /></td>
<td><img src="image12.jpg" alt="Image" /></td>
</tr>
<tr>
<td><strong>Virtualization Security</strong></td>
<td><img src="image13.jpg" alt="Image" /></td>
<td><img src="image14.jpg" alt="Image" /></td>
<td><img src="image15.jpg" alt="Image" /></td>
</tr>
<tr>
<td><strong>Infrastructure Security</strong></td>
<td><img src="image16.jpg" alt="Image" /></td>
<td><img src="image17.jpg" alt="Image" /></td>
<td><img src="image18.jpg" alt="Image" /></td>
</tr>
</tbody>
</table>
Of 1,400 global IT decision-makers polled in 2018, 1 in 4 who use public clouds reported having data stolen and 1 in 5 have experienced an advanced attack against their infrastructure. Since cloud solutions help individual employees and departments solve critical business issues, the use of these systems and platforms without organizational approval — also known as shadow IT — poses additional risks to data security.

Forward-thinking IT departments are positioning themselves well ahead of these risks by deploying a range of security solutions from identity access management to gateway network firewalls to protect data and applications. Rising to the top of these solutions are DevSecOps, machine learning and endpoint security — all part of an increasingly sophisticated cloud security strategy.
CB PREDICTIVE SECURITY CLOUD
CONSOLIDATED ENDPOINT SECURITY SIMPLIFIED

The CB Predictive Security Cloud (PSC) is a single endpoint protection platform that consolidates security in the cloud, making it easy to prevent, investigate, remediate and hunt for threats.

THE POWER OF UNFILTERED DATA

CB DEFENSE
Next-Generation Antivirus + EDR

CB DEFENSE FOR VMWARE
Virtual Data Center Security

CB LIVEOPS
Real-Time Endpoint Query & Remediation

CB THREATSIGHT
Managed Threat Hunting & Triage

CB THREATHUNTER
Advanced Threat Hunting

SUPERIOR PROTECTION
Stop more attacks, take back control, and worry less

ACTIONABLE VISIBILITY
Cut down the guesswork and close security gaps fast

SIMPLIFIED OPERATIONS
Eliminate multi-vendor complexity and agent fatigue

UNIFIED DEFENSES
Strengthen your security posture

carbonblack.com
DevOps environments typically release frequently, incrementally and through an automated process. “In this fast-moving environment, security can often become an afterthought and vulnerabilities in code are overlooked,” Walker said. In the race to stay ahead of the competition, many enterprises view security as a roadblock to results. “With DevSecOps, security does not need to slow down the application development life cycle or create complex requirements. It can become a natural and streamlined part of the design and architecture of every application going into the cloud.”

The value proposition of DevSecOps is simple in that more security automation from the start reduces the chance of mistakes that can lead to downtime or attacks. DevSecOps also eliminates the need for security architects to configure security consoles manually. Gartner estimates that DevSecOps will be embedded into 80 percent of rapid development teams by 2021.

Checking for security flaws in parallel with software development has become a leading best practice in cloud security. DevSecOps uses a “shift left” approach in the software development life cycle (SDLC). This approach brings security closer to developers so they can scan their code as they write it, obtain fast and accurate feedback on any security flaws...
and adjust before any vulnerabilities are seen. When the application team integrates security into every aspect of the life cycle, the result is more secure applications and fewer vulnerabilities (see below).

The most effective application testing is DAST (Dynamic Application Security Testing), a black-box security methodology that tests an application from the outside by attacking it like a bad actor would, explained Walker. It continuously scans a website application as it evolves, providing automatic detection and assessment of code changes and creating alerts for any found vulnerabilities.

On the other end of the spectrum, SAST (Static Application Security Testing) examines the application from the inside out by looking into source code for potential security vulnerabilities. “While traditional static analysis solutions work, they are typically used at the end of the development process, which causes issues when trying to identify the point of entry of a breach,” Walker noted.

One of the measures of how well DevSecOps is working is the number of days it takes to fix a vulnerability. Walker said a customer using DevSecOps during development takes an average of 51 days to fix the issue, compared to 113 days using traditional static analysis. By combining development and security, DecSecOps shortens feedback loops, reduces incidents and creates a seamless security procedure.

This early detection that dynamic scanning provides also decreases the business cost of security defects. Finding an issue in the development phase costs roughly $80 per defect, compared to $7,600 during the production environment, according to the 2016 National Institute of Standards and Technology study from the Ponemon Institute.
Prediction Point: Artificial Intelligence and Machine Learning
Cybercriminals have managed to elude traditional security standards despite the prevention efforts of IT teams and enormous budgets of enterprises. Once a data breach occurred, significant investments of human and financial capital were needed to make improvements to security standards.

There’s been a growing movement from prevention to real-time threat detection using artificial intelligence (AI) and machine learning. An easy way to think of the difference between the two is that AI is the software, while machine learning is the algorithms that analyze the data (see graphic below). By getting ahead of cyberattacks with these automated discovery models, cloud service providers and enterprises can detect threats promptly by mining through large data sets.

At its Google Cloud Next conference in July 2018, Google announced it was using artificial intelligence and machine to block so-called “bad messages” and display a warning for suspicious messages. It’s expected that more information security teams within enterprises will leverage these predictive frameworks across public, private and hybrid cloud infrastructures.

**Benefits of AI and Machine Learning for Cloud Security Are Many:**

- **Artificial Intelligence**
  
  Software that can solve problems by itself

- **Machine Learning**
  
  Algorithms that learn from data

- AI is a system that has the capability to learn and adapt to the change in its environment. It uses predictive analysis to pre-model results to get ahead of attacks.

- Current machine learning technologies can detect unusual threat events using high volumes of data. The more data processed by machine learning, the more patterns are detected to help AI give indications of cyberthreats whenever there is a slight change in pattern flow.

- Machine learning rapidly processes real-time data and relates them across time and geography to help enterprises get ahead of security events often by days.

- Events are often detected and blocked within hours, shutting down the flow into the network and preventing data leakage.

- By delegating the first level of security analysis to automation, security teams can better prioritize workload and focus on more critical threat.
End Point: Where Most Attacks Start

In recent years, endpoint security has moved to the top of the priority list for organizations, and the reason is clear: Industry research by International Data Corporation (IDC) shows that 70 percent of successful breaches enter through an endpoint such as a laptop, tablet or phone. A mobile workforce has proven to be the weakest security link and an easy target for attackers.

“A mobile workforce and the cloud have dramatically changed the security landscape,” explained Rick McElroy, security strategist for Carbon Black. “The decentralization of end users who work from anywhere and everywhere means that critical business applications and resources are more vulnerable than ever.”

As IT resources shift to a cloud-first strategy and mobile devices become the primary hardware for employees, endpoint security is now one of the hottest issues for security teams.

A 2017 survey of 665 IT and security leaders by the Ponemon Institute revealed that organizations are grappling with securing their endpoints and pay big time for a successful attack — $5 million, on average. The research also showed that:

- **7 OUT OF 10** report their endpoint security risk has significantly increased over the last 12 months.
- **FILELESS ATTACKS** are on the rise—up to 77 percent of attacks use fileless techniques.
- **FILELESS ATTACKS** are 10 times more likely to succeed than file-based attacks.
- **RANSOMWARE** is still a major threat, with 54 percent of organizations experiencing this type of attack.
- **3 OUT OF 4** organizations report managing endpoint risk is complex and difficult.

McElroy explained that the decision to focus more IT resources on endpoint security varies between enterprises depending on what kind of data the business handles and where that data is located. He offered some considerations for designing and monitoring an endpoint security strategy:

- A company’s **COMPLIANCE REQUIREMENTS**, if it’s a highly regulated industry.
- How **MOBILE** its workforce is.
- The value and amount of **DATA AVAILABLE VIA MOBILE DEVICES**.
- **PAST INCIDENT DATA**, including how data flows, the number of attacks mitigated each month and the need for manual intervention.

Despite the fact that many IT security teams are in the process of getting up to speed on endpoint security, McElroy said the good news about endpoint security is that it adds a new layer of protection without requiring a wholesale change in an existing security practice.
Inside a Docker Cryptojacking Exploit

WATCH NOW
The introduction of the European Union’s General Data Protection Regulation (GDPR) adds another issue into the cloud security mix, as organizations now are required to ensure that their data practices fully comply.

Based on a survey of 177 global IT organizations by Commvault, only 12 percent understand how GDPR will affect their cloud services. These results indicate that enterprises with a cloud-first strategy could be highly vulnerable to this regulation.

CONCLUSION

Despite the challenges for CIOs and IT security teams to keep up with the ever-changing cloud environment, the solutions described above can help ensure enterprises will soar with cloud possibilities without being dragged down by any damaging winds of security vulnerabilities.

Melinda Cross is a content developer and brand storyteller who believes words have the power to influence action for organizations. She partners with leaders in finance, risk management, technology, and e-commerce to convey their thinking with compelling data and stories.
Applications are the business in this digital age. Securing the applications that drive your business is essential to providing safe digital experiences to your entire business ecosystem.

The WhiteHat Application Security Platform is a cloud service that allows organizations to bridge the gap between security and development to deliver secure applications at the speed of business.