Google Cloud

Cloud & On-Prem:
Security by the Numbers

Enterprise cloud adoption continues to accelerate, which means that more and more companies are storing information offsite or in the cloud. IT leaders are increasingly focused on data security, because as data volumes grow, so do threats—as well as significant opportunities.

Estimated worldwide spending on public cloud services in 2019

$141 billion

It was $70 billion in 2009—and the growth isn't just monetary. Companies are storing more of their data in the public cloud than ever before. The move to the cloud has in turn led to a surge in cloud security innovation and, as developers flock to secure the virtual world, on-prem data centers run the risk of being left behind.[1]

The estimated increase in annual data generation from 2009 to 2020

4300%

Outsourcing the majority of your organization's data management to the cloud will allow you to dedicate more resources to providing the IT services that your business needs to grow into the future.[2]

The proportion of information security professionals concerned about the weaponization of IoT devices for DDoS attacks

78%

The Internet of Things (IoT) represents both an opportunity and a threat for businesses. The rise of connected devices means richer customer insights—but it can also mean increased vulnerability. Using a public cloud provider with built-in security measures can mitigate these risks by helping to ensure that your data is securely stored and monitored at scale.[3]

The percentage of IT leaders who believe a serious data breach will hit their organization within 12 months

65%

Data breaches are a reality of modern global computing. How does your data center's security compare to other public cloud providers, and how quickly can you address the vulnerability that enabled the breach? Public cloud providers that rely on a secure and reliable data infrastructure as a primary product offering dedicate significant resources and talent to predicting, minimizing, and combating attacks.[4]

Breaches that begin with spear phishing

91%

Perhaps your data center is secure, but how secure are your people? Phishing emails can dupe even the most diligent employee, and IT teams can take time to catch on. Spear phishing, which focuses on a particular organization, group or person, can pose a particular risk—but choosing a larger public cloud provider with high standards for security can help mitigate the risk of phishing attacks.[5]

The year-on-year increase in frequency of DDoS attacks

200%

Dedicated Denial of Service (DDoS) attacks flood the target system with traffic from multiple locations, sometimes working in tandem with a Trojan virus. This flood makes it difficult to differentiate attack signals from legitimate user traffic and almost impossible to stop by typical IP blocking. Larger public clouds can scale during an attack and keep businesses online. They can also allocate resources to work to predict when DDoS attacks might occur. There's a community of public cloud providers, researchers and other cloud workers that share important security findings freely to ensure that the cloud systems are as secure as possible.[6]

The average time for financial corporations to detect a data breach in 2015

98 days

Some industries took much, much longer. Depending on the size of your organization and the sensitivity of your data, any breach could deal a catastrophic blow to your organization's reputation and bottom line. Public cloud providers offer a stable and scalable security infrastructure.[7]

IT professionals surveyed in 2016 who were confident that cloud had equal or greater security than internal IT systems

64.9%

Storing data securely is a cloud provider's bread and butter, and security breaches are simply unacceptable. Google Cloud leverages purpose-built hardware, dedicated privacy and security teams, multi-layered physical site security, a variety of redundant systems and a global network to help safeguard our customers' data.[8]

Number of security engineers Google employed in 2016

650+

Their job is to maintain Google's defense systems, develop security review processes, build security infrastructure and implement our security policies. Some are also thought leaders in data center construction, security and privacy, and have literally written the book on these topics.[9]

The number of unfilled cloud security jobs in 2019

1.5 million

As cloud security becomes increasingly important, cybersecurity expertise is in ever higher demand. According to Cybersecurity Ventures, there will be 6 million global job openings for cybersecurity professionals by 2019, with 1.5 million of those unfilled. To get ahead of this trend, choose a cloud partner with a strong security track record, like Google Cloud.[10]

Find out what Google Cloud can do for your organization >

Footnotes

[1] IDC, 2016, 'Worldwide Semiannual Public Cloud Services Spending Guide'
[2] CSC, 2012, 'Big Data Universe Beginning to Explode'
[3] Tripwire, 2016, 'Tripwire Black Hat 2016 Survey: IoT Risks and Cyber War'
[4] Okta, 2016, 'Okta EMEA Report: Secure Business Agility', pg 2
[5] Trend Micro, 2017, 'Spear-Phishing Email: Most Favored APT Attack Bait', pg 3
[6] I Am Wire, 2016, 'Top 7 Cyber-Security Predictions for 2017 and Beyond'
[7] LBM & Tech Beacon, 2016, 'Cybersecurity Trend Report'
[8] Cloud Security Alliance, 2015, 'The Cloud Balancing Act for IT: Between Promise and Peril', pg 3
[9] Google Cloud
[10] Cybersecurity Ventures, 2016, 'Cybersecurity Jobs Report'

Google Cloud