portnox™

WHITE PAPER

Mythbusters: Debunking the Top 5 Cloud Security Myths

Putting the On-Premise vs. Cloud Security Debate to Rest

Whether you're a fan of digital transformation or not, there's no denying that the shift to the cloud is engulfing enterprise IT. According to Gartner, over the next five years, over $1 trillion in compounded IT spending will be directly or indirectly impacted by the cloud shift, making cloud security one of the most disruptive forces of IT spending since the early days of the digital age.

Despite industry recognition that the future of IT lies in the cloud, many businesses remain wary of the security implications of this shift. One BT Group[1] survey found that 49% of IT decision-makers are 'very or extremely anxious' about the implications of cloud security, and that overall, 76% of respondents' main concern with cloud solutions was their security. Those numbers do not bode well for the future of cloud security solutions, but there is good indication that cloud skeptics are losing steam.

Businesses are beginning to see significant returns on investment (ROIs) as a result of measures to take their network security to the cloud. This comes naturally when breaking with the traditional on-premise, appliance-based model that depends on costly hardware, software, and manual patch updates to keep networks secure. With cloud security solutions, IT teams' hands are freed to contribute more to their company's business proposition than just maintaining the status quo. That's because cloud security solutions are always patched, elastic, scalable and available at all times and locations – in case of the inevitable IT emergency.

That said, it's time to debunk some of the most common myths regarding cloud security before an outdated IT stack exposes your organization to emerging digital business risks.

"53% of organizations see unauthorized access through misuse of employee credentials and improper access controls as the single biggest threat to cloud security"

– Information Security Cloud Computing Survey, 2016 [2]

Myth #1 – The Cloud Isn't Secure

The top concern among C-Suites and IT teams is that cloud-based security solutions are more prone to threats than legacy, on-premise security solutions.

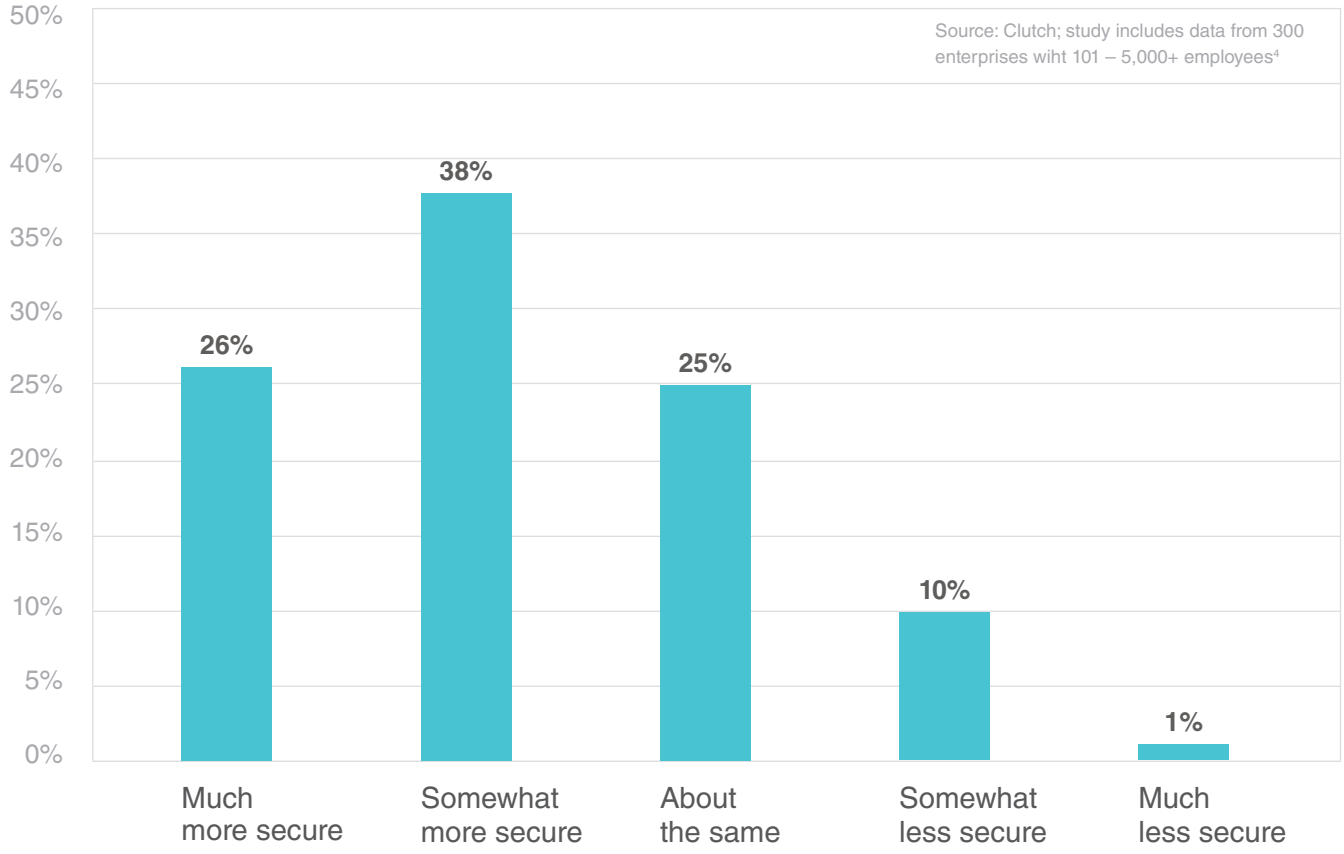
Debunked: On-premise security appliances require firmware upgrades to protect against known exploits, resulting in a constant need to keep the solutions up-to-date. In addition, configuration changes could expose the network to potential vulnerabilities, requiring tedious maintenance of management procedures and periodic penetration testing. However, cloud-based security solutions are constructed, from the outset, to evolve to address relevant threats in the current cyber security landscape. Indeed, security and gaining the trust of its various customers are key to the cloud-security solution provider's business proposition. That's why 64% of enterprises consider cloud infrastructure a more secure alternative to legacy systems[3].

[1] http://www.information-age.com/great-it-myth-cloud-really-less-secure-premise-123459135/

[2] https://pages.cloudpassage.com/rs/857-FXQ-213/images/cloud-security-survey-report-2016.pdf

[3] https://clutch.co/cloud/resources/security-trends-in-enterprise-cloud-computing

Compared to legacy systems, how would you rate the security of the cloud?



Myth #2 – The Cloud Is Still Too 'New' To Be Trusted

Cloud-based applications and services have been around for about a decade, while software and hardware-based solutions have a much longer history. So why trust the cloud?

Debunked: Maybe because an increasing number of both large and small to medium-sized enterprises across a variety of industries – government, healthcare, ecommerce etc. – are deploying cloud-based solutions for everything from human resource management to network security. According to IDG Research[5], "Cloud technology is becoming a staple to organization's infrastructure as 70% have at least one application in the cloud". Another survey from Clutch[6] found that **90% of businesses in the US use cloud infrastructure.**

In a 2017 survey[7] of more than 180 healthcare IT professionals, 61% said that they believed that their information was safest in the private cloud, compared to 11.5% on-premise in the case of an environmental disaster. In terms of cyber attacks, 58.5% favored the private cloud versus 32% who would stick with an on-premise solution.

Looking forward: 81% of respondents from the same survey stated that they plan to implement new or additional cloud services within the next three years.

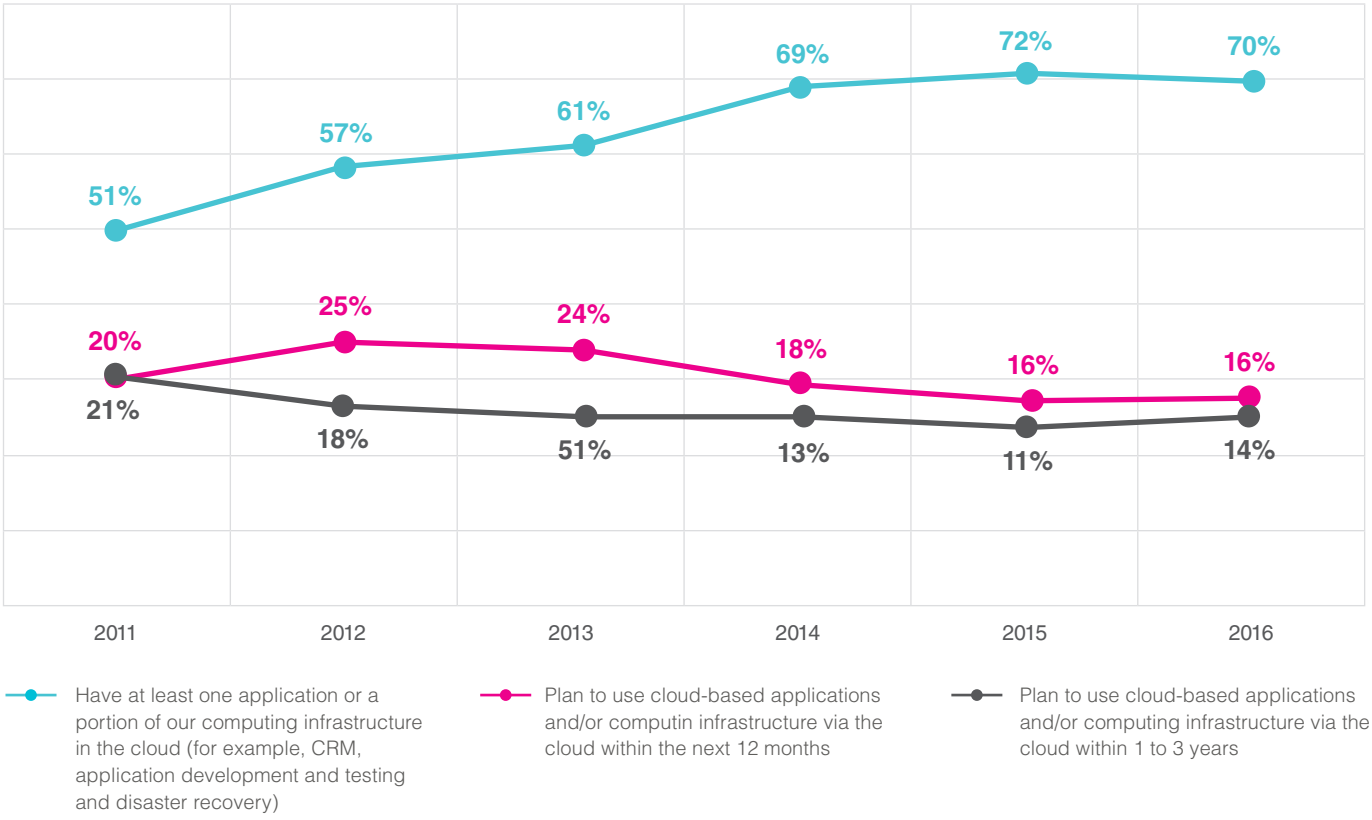
[4] https://clutch.co/cloud/resources/security-trends-in-enterprise-cloud-computing

[5] https://www.idgenterprise.com/resource/research/2016-idg-enterprise-cloud-computing-survey/

[6] https://clutch.co/cloud/resources/security-trends-in-enterprise-cloud-computing

[7] https://www.channele2e.com/business/vertical-markets/evolve-ip-survey-healthcare-data-safer-in-cloud-than-on-premises/

Use of Cloud Technology Continues Expanding



Reference: "2016 IDG Enterprise Cloud Computing Survey" [8]

Myth #3 – The Cloud Is Great for Productivity Apps, But Not for Securing the Network

It would be ubiquitous to repeat that cloud apps are now an integral part of enterprises of all sizes, but that's not necessarily true of network security. There is big difference between putting administrative and sales information on the cloud, and allowing network and endpoint access to be controlled from the cloud.

Debunked: Network access control (NAC) is a growing concern for CIO/CISOs and IT teams in large to SMEs due to rising pressure to gain control over digital business risks amid rapidly emerging cybersecurity threats. However, the stigma of the cloud being less secure isn't necessarily true. In fact, Gartner reports[9] that by 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

[8] https://www.idgenterprise.com/resource/research/2016-idg-enterprise-cloud-computing-survey/

[9] https://www.gartner.com/login/loginInitAction.do?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252Fcode%252F296799

Myth #4 – Cloud Solutions Require Re-Educating IT Teams

Because IT teams are used to employing software or hardware-based legacy security solutions, training them to deploy a security-as-a-service (SaaS) solution would require significant time and resources. In addition, it takes up just as much time and resources to deploy various cloud security solutions as it does to deploy existing on-premise solutions, so why take the leap?

Debunked: Cloud solutions inherently cut time and costs associated with security management in IT teams, freeing them up to carry out more productive and profitable action items. Cloud-based security solutions are a great opportunity for organizations to hold back on capital expenditure in exchange for essential operational expenditure – investing in the right security tools for their business rather than additional manpower to maintain it.

That's added to the easy and instant deployment of cloud-based solutions that includes, among other features, the ability to automate a number of security actions such as system updates, patching, and more. Automation minimizes the digital business risks associated with network security management by understanding how the network is supposed to function and what its security requirements are, then carrying out these requirements instantly and without question. According to a 2016 survey[10] among 2,200 members of the "Information Security Community" on LinkedIn, cloud-based security solutions have 45% popularity as the most effective security technology to protect access to the cloud network, namely because of its powerful automation abilities.

The same survey found that the lowest barriers to entry for cloud-based solutions are Integration with existing IT environments, at 35%, and Lack of expertise at 26%. In addition, only 6% of respondents stated that they were wary of cloud solutions due to Lack of support by cloud provider.

Myth #5 – Cloud Solutions Can't Help With Compliance

Cloud solutions are constantly changing – one minute they are a "must have" security tool, and the next they are an imminent source of risk to company information. How can you trust cloud security solutions to adhere to increasingly stringent information security compliance protocols?

Debunked: Compliance is one of the biggest reasons for what is known as the "IT Headache" because it's necessary to keeping the enterprise network up-and-running. However, cloud-based security solutions are one of the "cures" for this headache because they take the job of enforcing compliance out of the hands of the IT team and put it in the cloud security solution's lap. If it's making sure rogue devices are blocked from the network or ensuring that all endpoints have necessary patch updates, cloud-based security solutions allow for continuous and real-time auditing, monitoring and control of all of the operational aspects of IT infrastructure. By adopting a cloud-based security solution to enforce compliance, CISOs/CSOs are not only making IT teams happy, but are minimizing critical digital business risks.

With on-premise, server-based applications, companies are 100% responsible for making sure that they fulfill regulatory compliance requirements. With increasing regulations such as SOX, PCI-DSS and GDPR, IT teams often have more compliance initiatives to keep track of than they have staff.

That's where cloud-based solutions can have added value by segmenting compliance reporting sections to make reporting and monitoring easier: data privacy, information security, government regulations, etc.

[10] https://pages.cloudpassage.com/rs/857-FXQ-213/images/cloud-security-survey-report-2016.pdf

Conclusion – Security-as-a-Service Solutions are the Future

According to Gartner, "By 2020, a corporate 'no-cloud' policy will be as rare as a 'no-Internet' policy is today". While in many cases, hype can have dangerous potential, in the case of cloud security solutions, it's a win-win situation: a win for digital transformation/innovation and a win for CISOs/CSOs eager to control and minimize their digital business risk.

Maximize Cloud Benefits with CLEAR - Security-as-a-Service

This might not be the usual Security-as-a-Service (SaaS) you're used to hearing about in the cloud computing context, but it's just as important (if not more). As this white paper has attempted to show, cloud security is the next great frontier for the growing, dynamic and innovative enterprise. When businesses control network access from the cloud, they control their exposure to emerging digital business risks, closely tied with innovative progress. Portnox CLEAR, a breakthrough Security-as-a-Service Network Access Control (NAC) solution, gives CISOs and IT teams the visibility, control and management capabilities they need to keep their company technologically agile and secure while embracing the processes of digital transformation.

Portnox CLEAR: The first cloud-based Security-as-a-Service solution for Network Access Control, CLEAR provides visibility, control and risk management capabilities for all devices and users on wired, wireless and virtual networks, to effectively confront digital business risks and emerging cybersecurity threats.

Try it Now!

About Portnox

Portnox secures connected organizations' corporate networks utilizing its next-generation network access control and management solutions. Portnox's solutions manage any Internet of Things (IoT), BYOD, mobile or company devices accessing the network, even in remote locations.

Founded in 2007, Portnox provides its global customers with a complete view of device and network visibility, reducing security risks and improving network control. Portnox offers two solutions – CORE for On-Premise NAC and CLEAR for cloud-based NAC – allowing companies to grow, optimize, and evolve their infrastructure while maintaining the upmost security and compliance. The company was recognized by Gartner as a pure-play security vendor of network access control solutions and is a recipient of the 2016 Global Frost & Sullivan Award for Competitive Strategy Innovation and Leadership, among other Security Industry Awards. Portnox has offices in the U.S. and in Europe.

Contact Us

Americas: usinfo@portnox.com | 1.855.476.7866
Europe: dotell@portnox.com | (44) 1273.256325

www.portnox.com

portnox™