✓ Symantec™

You need to convince the business to invest in more robust security for Office 365.

Now What?

IT leaders know the importance of security in the cloud era, but some stakeholders may be less aware, and might assume that when adopting Microsoft Office 365, it's already secure enough.

But the truth is, Office 365 (O365) is a broad and diverse platform that can present a complex security risk, spanning everything from account takeovers, to malware infections and data loss. It's also a safe bet that Office 365 is not the only cloud service your business is using. In short, you need a more comprehensive approach.

Use this 6-point business case builder to demonstrate why Symantec CloudSOC (CASB) and Email Security.cloud are the best investment of your security budget to provide protection for not just Office 365 but your wider cloud environment.

1 Show how your key data is already residing in the cloud

2 Show how sophisticated threats are increasing the impact of a breach

3 Show why you need visibility across all your cloud applications

4 Articulate the benefit of securing all your SaaS apps

5 Demonstrate the need for third-party security on O365

6 Prove why Symantec is a better investment for your security budget

1 Show how your key data is already residing in Office 365

The average organisation uses about 40x more cloud apps (sanctioned and unsanctioned) than CIOs believe,[1] and the amount and types of data stored in those apps, such as Office 365, lacks visibility and control. So it's a safe bet that no matter how many security controls you have in place, your sensitive data is already in Office 365 – leaving it vulnerable to compromise.

Consider running an Office 365 Data Risk Assessment to help support your case. It's free, and you will receive:

- An inventory of all the sensitive content that has been uploaded and stored in Office 365
- A summary of risky exposures, such as sensitive content being shared outside the organisation
- Identification of inbound risky content shared with employees, such as malware
- Identification of your riskiest users

Key takeaway

Our data is already travelling in and out of Office 365, whether we can see it or not. We need superior technology that we can trust to keep our organisation's cloud environment protected against the threats it can be exposed to.

2 Show how sophisticated threats are increasing the impact of a breach

Email continues to be the top attack vector for malicious attacks and data breaches, with 66% of malware coming from email attachments[2]. But these cyber-attacks are getting more intelligent and harder to detect. And email isn't the only means of entry.

However cyber criminals gain access to your systems, security breaches aren't merely inconvenient, they're time consuming, stressful and damaging to a business's reputation. They're costly too, with any downtime having a huge impact on the bottom line. The fact is, it's not a case of 'if' you're targeted; it's a case of 'when'.

Here are a few facts and figures to support this:

- 43% of all breaches involved social tactics[2]
- In 2019, half of malware campaigns will use encryption to conceal themselves[3]
- 71% of organised cyber-criminal groups used spear phishing to steal data[4]
- 2017 saw a 46% increase in new ransomware variants[4]
- There was also a 92% increase in new downloader variants[4]

1 2018 Shadow Data Report, Symantec, 2018
2 A Guide to Protecting Microsoft Office 365 from Security Threats, ESG Research (August 2018)
3 https://business.financialpost.com/technology/cio/ciscos-network-intuitive-effort-to-bring-intelligence-machine-learning-to-networking
4 A Guide to Protecting Microsoft Office 365 from Security Threats, ESG Research (2018)

Key takeaway

The figures speak for themselves. If we're not protecting ourselves with the best technology, we risk significant losses of time, money and stress when our security is inevitably compromised.

3 Show why you need visibility across all your cloud applications

The cloud introduces new risks and compliance issues for organisations already dealing with the traditional threat landscape. It renders traditional network perimeter obsolete, and opens new doors to data loss and cyberattacks.

And when users go rogue and use shadow IT to handle business data, this risk increases exponentially. The problem is, IT has no way to identify, classify and control sensitive, compliance-related and confidential data that could be exposed in the cloud.

Symantec CloudSOC delivers powerful capabilities for cloud application security, monitoring and controlling access, discovery of shadow IT, real-time detection of intrusions and threats, helping to protect against data loss and compliance violations, and investigation of historical account activity for post-incident analysis.

Key takeaway

Our security is still at risk from shadow IT and other cloud apps. With Symantec CloudSOC we get visibility and analysis, not just for Office 365, but our entire ecosystem of cloud apps and services, whether they're sanctioned or unsanctioned.

4 Articulate the benefit of securing all your SaaS apps

The benefits of Office 365 are undeniable, with a feature-rich, powerful set of collaboration and productivity tools. Beyond the Microsoft environment though, 74% of organisations are using other software-as-a-service in some capacity.[5] With such a fragmented infrastructure, with many layers of built-in security and overlapping bolt-on toolsets, it's hard for IT to maintain a single view for visibility and policy controls across the entire suite of SaaS apps and services.

With Symantec you can:

- Help protect against new and emerging multi-vector attacks (web, email, endpoint, and collaboration apps)
- Help protect SaaS applications, including O365 and other business SaaS apps, while discovering and (where necessary) restricting use of shadow cloud applications
- Identify and control account takeover or malicious actions through user behaviour analytics
- Gain control of content: tracking, access, email, sharing across all business applications
- Keep key information under corporate control for consistency and visibility

Key takeaway

Adoption of Office 365 gives us a powerful opportunity to replicate our cloud strategy and security posture across multiple clouds, and all the business applications we need to support and protect.

5 Demonstrate the need for third-party security on O365

In the rush to migrate to Office 365, many organisations don't spend enough time considering the implications on their security, focusing instead on the powerful productivity gains and cost savings. There's no denying that Office 365 is a powerful platform, but Microsoft is not a security expert, and with so many tools and apps in the O365 suite, delivering and maintaining all of them is Microsoft's primary objective.

Key takeaway

Effective enterprise-grade security isn't included in basic Office 365 packages, so we're going to need to invest in additional security regardless. It makes more sense to invest in a market-leading security system that can secure the entire enterprise, rather than protect just a single cloud platform.

6 Prove why Symantec is a better investment for your security budget

- The Symantec CloudSOC CASB offering has been named a Leader in the most recent Forrester Wave Report[6] and Gartner Magic Quadrant for Cloud Access Security Broker (CASB)[7]

- Radicati has also named Symantec at a Top Player in its Market Quadrant for Secure Email Gateway in 2018, and also in its Market Quadrant for Advanced Persistent Threat Protection[8]

- These solutions combine to deliver superior protection with powerful capabilities, and the option to integrate with other Leader's quadrant protections like DLP, SWG and endpoint protection, to create a fully Integrated Cyber Defense Platform

Key takeaway

The analysts have done the hard work for us, and their data clearly shows even if we buy the additional security that Microsoft offers to secure the Office 365 environment, we still wouldn't get the level of protection we'd get from a specialist third party security partner like Symantec.

Next steps

Want to talk to an Office 365 expert to help fine-tune your business case?
Request a callback now and one of our team will get straight back to you.

Request a callback

6 The Forrester Wave: Cloud Security Gateways, Q1, 2019
7 Magic Quadrant for Cloud Access Security Brokers, Gartner, 2018
8 Radicati Market Quadrant – Advanced Persistent Threat Protection 2018

✓ Symantec