Malware in the Cloud

The risks and what you can do about them

> **88%** of companies have now adopted some form of cloud computing

The risks and what you can do about them

According to research conducted by the Cloud Industry Forum, 88% of companies have now adopted some form of cloud computing.

What's cloud computing? It's where you use software in your browser, rather than having to download it to your computer.

In lots of ways, the increase in use of cloud computing is a wonderful thing.

The many benefits of moving to the cloud have been well documented. From flexibility and convenience to reduced downtime and huge cost savings, it's easy to see why so many businesses have taken the plunge.

But as is often the way with the good stuff in life, there are downsides too. The explosive growth of cloud computing has opened the door to a host of cyber attackers, waiting in the wings to capitalise on the inexperience of business owners.

One of their favourite ways in is through malware; a malicious form of software with the power to spread through computer systems like a forest fire.

Although the threat of cyber-attacks has reached record levels, a staggeringly low number of cloud providers are offering full protection

This leaves countless UK businesses as sitting ducks, vulnerable to attack at any time despite investing in what they thought was a secure new system.

The really scary thing is that malware can go unnoticed for months. Gone are the days when a virus was obvious and caused computer screens to flash, wobble and fill with pop ups. Today's threats are far more insidious, sneaking in under the radar and causing untold damage that nobody knows about until it's too late.

Once this software infiltrates your system, trying to contain and destroy it is impossible on your own. And without strong protocols, a proactive approach and the right support in place, the threat gets closer every day.

You have to protect yourself

It's often hard to imagine how a computer virus spreads because to most (normal!) non-techy people it's a completely abstract concept. So, in order to really understand the threat, think of it like a physical disease. Even if you're fastidiously clean and eat a healthy diet, sitting in a room full of people with runny noses and hacking coughs puts you at risk of catching a cold too.

A sneeze can travel at up to 100 miles an hour and spread germs three metres away. Scientists taking samples from office items like doorknobs, keyboards, phones and desks found that between 40% and 60% of people who touched these items after someone with a cold caught the same virus. Within a matter of days that's almost an entire office full of sickly staff, resulting in at least a few of them taking sickies.

"Human" viruses spread fast and result in lost time and money. And it's exactly the same with your computer system.

Once hackers infect your system they can move to different hosts within the cloud, using a range of dirty tricks from phishing attacks and password pinching, to recording keyboard movements and good old fashioned brute force.

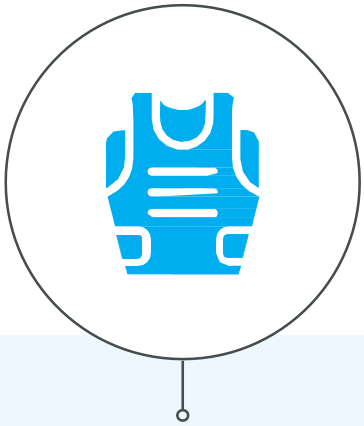
A recent report from Bitglass found an average of one in three SaaS (Software as a Service) apps contained malware. SaaS is just another term for cloud computing.

This wasn't from a small pool either – researchers scanned tens of millions of files before coming to this frightening conclusion.

Even more alarmingly, big name software including Microsoft OneDrive and Google Drive was rife with viruses. OneDrive showed a 55% infection rate with Google Drive at 43%. Dropbox and Box weren't much better, coming in at 33% each.

So, how do you enjoy the benefits of cloud computing without putting yourself and your company at risk?

Easy: With bullet proof security that's constantly protecting you in the background, so you don't have to think about it



That means constantly monitoring all devices, checking things are working smoothly round the clock and adding another layer of protection. So if a new sneaky virus does manage to break through the barriers you can keep it contained.

In human terms, that's like eating nothing but vitamin-rich food, smothering yourself in antibacterial gel, locking yourself in a sterile room and never making physical contact with anyone else.

In other words, impossible! If you want to conduct a normal life, anyway.

Until software suppliers release genuine solutions that are specific to malware in the cloud, the only approach you can take to security is a proactive one.

This is not the sort of situation where you can think "I'll just take my chances and hope nothing goes wrong" because if it does, the results can be catastrophic. You need to defend yourself from all sides and stay on the look out for trouble before it strikes.

The problem is, defending yourself against attack simply isn't something the average business can manage alone.

For any real chance of staying safe in the cloud you're going to need to work with a trusted third party who can take care of all the behind the scenes work and save the day if anything does go wrong.

That's easier said than done too – according to research from Palo Alto Networks only 15% of UK security professionals feel able to maintain the proper level of security across cloud based networks. Another 68% of cyber security experts working in large businesses said their organisations were unable to combat the risks. If these are the guys who are meant to be keeping computers safe, what hope is there for everyone else?

When you're shopping around for an IT support company, also known as a Managed Service Provider, you need to be confident that they've got your back. They'll need to be all your favourite action heroes rolled into one; a gun-slinging, zombie killing, alien fighting mercenary who'll stop at nothing to keep your computer system safe.

Ok, so maybe you can't expect Vin Diesel to turn up the next time you log an IT issue, but you can still check out their credentials and not settle for anything less than someone who's really got your back.

They'll need impressive SLA stats and be able to demonstrate that they take a proactive approach to malware in the cloud, **including:**

Zero-day threat protection

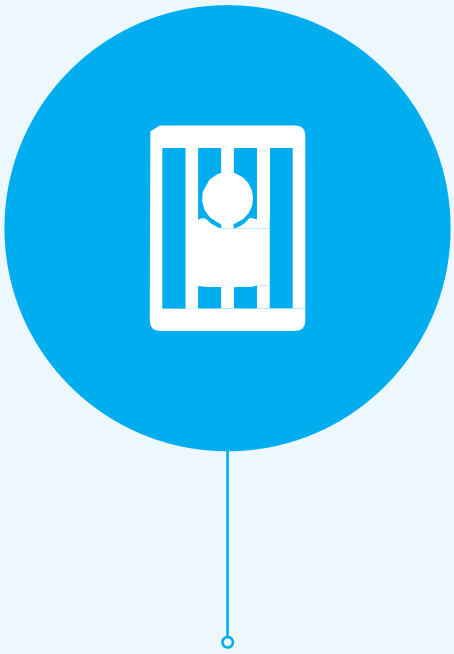
A zero-day vulnerability is a flaw in software or hardware that's hard to spot but can quickly wreak havoc. Once the flaw is exploited, hackers are able to infect systems with viruses before the developer gets chance to create a patch or fix it. Robust zero-day threat protection uses static analysis to identify potential threats based on behaviour, stopping them in their tracks.

Endpoint protection

An end point is tech speak for a device, such as a laptop, desktop computer or a phone. It's essential that all endpoints in your organisation are protected, but most cloud platforms don't offer high quality security solutions for devices like laptops, phones and servers. The best options stop malware before they can get to endpoints and work seamlessly across all applications.

BYOD (Bring Your Own Device)

A lot of organisations fall down due to lax Bring Your Own Device policies. The ability for staff to access their work documents on their own mobiles, wherever they are, is brilliant for productivity and cost savings, but you need to know that they're handled properly 24/7. Any cyber security expert worth their salt will be able to advise you on policy and deployment, and keep those devices safe even when they're not under your roof.



Confinement

With new threats popping up every day, even the best in the business won't be able to give you a 100% guarantee that a clever hacker won't be able to find a sneaky new way to break down your barriers. What they can do is keep any viruses confined so they don't spread throughout your system. Fast action is critical in maintaining the integrity of your data, so you'll want to enlist a team that offers this additional layer of protection.

This is your safest option

Staying secure in the cloud requires a holistic approach to your business processes, from software to devices to apps. Thousands of people innocently download applications that they assume will be safe because they're in the iTunes or Android app store, but don't be fooled.

Malicious hackers will happily exploit people's trust in apps, seeing it as the perfect opportunity to spread their viruses. The truth is, you've got just as much chance of encountering malware from an app as you have from any other online service, so vigilance is key.

That leads nicely on to the next point: education. The most important thing you can do is get your employees up to speed, because the one thing hackers count on above all else is their naivety. Employees are the number one cause of data breaches in SMEs, accounting for millions of pounds worth of losses.

It's not their fault. Hackers are smart and know exactly how to lure people in with convincing looking emails and websites. But when staff are properly informed about what to look out for and given incentives to raise anything that looks suspicious, organisations can keep even the most ruthless attackers locked out.

Cloud computing is brilliant. It's revolutionised the way people not only do business but live their lives. So much so that it's hard to image how we ever managed without it. It's given businesses the freedom to grow without having to invest a fortune; improves efficiency and productivity like nothing else; and offers capabilities that simply wouldn't have been possible to deliver through in-house tech.

The problem isn't with cloud computing, it's with how organisations approach it. Just like anything else you value, it's important to take appropriate measures to keep your computer systems safe.

Avoiding malware in the cloud requires a multi-layered approach that includes people and technology. It requires constant vigilance and the ability to fight off potential attackers before they get the chance to cause havoc. You can't be expected to do all that on your own, so it makes sense to find someone who can.

IT Support (UK) Ltd

Email: info@itsupport.uk.com

Phone: 01689 422522 (Kent & SE) or 0208 123 0007 (London)

Contact us today to ensure your business gets all the good stuff the cloud can offer, and none of the bad.