FuseMail®
Connect with Confidence

The importance of web security to modern-day SMEs

+44 (0) 800 093 2580 www.fusemail.com uksales@fusemail.com

Contents

Security through obscurity

...no longer applies.

No one is immune from online security threats anymore. Hackers and attackers are targeting everyone from the NHS to local charities to sole traders. Any click online could be your undoing, whether it is from an email, adware, spyware or an innocent looking link on a website.

Why has web security become so important?

This is nothing new; indeed web security and the need for web security have been around for a very long time. However, what has changed is that everyone is now more 'online' than ever before. Almost every organisation in the world uses online applications to run their business; from your CRM to your accounting system, you are online and you are visible. If you are visible, you are vulnerable.

In fact if you are simply online in any capacity, you are vulnerable.

All organisations have data or applications to plunder and hold to ransom. Be it your customer data, your email system or even your file networks, these are all critical to your everyday business workings. If you lost access to any of them through ransomware or malware, how would your business operations and reputation hold up? That question now applies to large global organisations as much as to a small local business.

This begs the question, could a hacker bring your business to its knees?

In order to answer this question, let us take a look at how to assess and address your vulnerabilities.

Assessing your vulnerabilities – the basics

Assessing where your major vulnerabilities lie is key to ensuring that you have your bases covered, so let's look at the best ways to protect your organisation from online threats through the lens of potential risks.

We would argue that outside of dedicated online security services the only way to safeguard your organisation is still through timely **system updates**, daily **network backups** and constant **employee education and vigilance**.

Outdated software and systems

Is your IT department aware of every piece of software on your company computers? The rise and rise of shadow IT would suggest they might not be. There are pieces of software on your employees' computers which have not seen an update in years and that is where you are vulnerable to attack. This area of IT is also known as Patch Management.

Look at 2017's wannacry attack, this huge security breach exploited out of date software on people's computers and spread like wildfire around the world, infecting everyone and causing chaos in hospitals, businesses and retail outlets.

No network backups

Not having them is not an option, but there are other, better ways to safeguard your company's network. Have you ever tried to restore an entire network from the back up, without becoming compromised all over again? Backups are there as a last resort – they are resource heavy. But again – you need them!

Lack of employee awareness and education

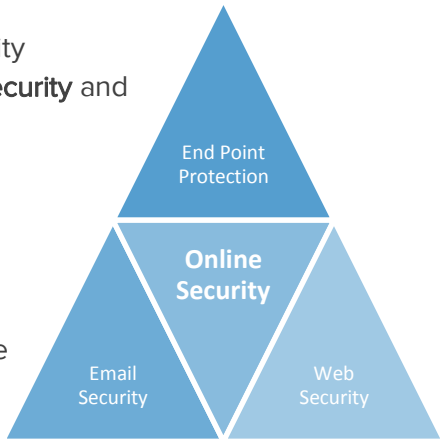
Your employees are your biggest asset. But when it comes to IT security, they are also your biggest risk. If you do not educate them about the threats, they will fall prey to them! However, no matter how good your employees are at spotting dodgy links, phishing emails and other potential threats, the day will come when someone clicks the link, downloads the attachment or gets phished. All it takes is one person and the whole system is compromised.

Let's say you have processes and budgets in place for ensuring your software is regularly updated; you take daily off-site backups of your network and you regularly educate your employees about the risks of being online - what options are now open to you to further ensure that your vulnerabilities are reduced once you have the basics covered?

We would now move you on to software or more commonly nowadays - cloud services. Let's look at your options here.

Specialist online security software and cloud services

Moving on to dedicated security services, the holy trinity of online security can be achieved through a combination of **end point protection**, **email security** and **web security**.



Endpoint protection and email security

These systems really are essential given today's online threats and, working hand in hand with the three areas previously mentioned, are the only sure-fire way to guarantee that you are comfortably covering all your bases. Most organisations have some form of endpoint protection (Antivirus) on their computers and all companies with email should (we hope!) have email security. When FuseMail talks to organisations about our world leading email security products we see generally good adoption of email security and endpoint protection in most sectors, but what about web security?

Web security

Adoption of web security services are seriously lagging behind, particularly in the SME marketplace.

Web security needs to become as important as email security and anti-virus, as all three work hand in hand to protect organisations against online threats.

Let's take a look at various web security threats.

Honing in on web security, you can look at why this is crucial to your organisation in one simple disaster scenario. Most of us would trust the BBC, but what if a site you trust became compromised?

Any link you clicked on the BBC site could try to download ransomware to your computer, infect your computer with a virus or start collecting information from your on-and-offline activities… down to recording what keys you are pressing to enter your personal or business online banking details.

Would your standard anti-virus or basic firewall block this type of attack? Probably not.

A decent cloud web security product will protect against common advanced threats like ransomware, spyware and other malware – not just on your network but on any network in the cloud through what we call **the cloud effect**. If someone in South Africa gets hit by a virus, the cloud effect means your network in Salford will then be protected from that virus – leveraging the scale of the product to provide a better service to customers across the globe. The web security service also knows to block known or suspicious websites such as phishing sites and of course, if it has some web filtering thrown in to the mix, it will save you thousands and potentially millions in lost productivity and legal suits.

To fully understand and appreciate the real need for web security, we are going to look at some of the more common threats online right now.

Web Security Threats

Malware

Definition: Software which is specifically designed to disrupt, damage, or gain unauthorised access to a computer system.

Malware is a blanket term, covering all kinds dangerous 'stuff' that can appear on your computer and network. We will go into more depth below on specific malware threats.

How do web security services help me here?

Cloud based web security systems work to stop the initial infection from any web based form (i.e. by preventing downloads).

On top of that, if the infection comes from another source for example an external USB drive, web security can stop the malware from calling home and sending data back to its master, or stop it connecting to the internet to download additional threats knows as payloads by identifying unusual behaviour on your system

Spyware

Definition: Software that enables an attacker to obtain covert information about a user's computer activities by transmitting data covertly from their hard drive.

Spyware is a scary piece of software; it can record keystrokes, on and offline activities and pick up a lot of information about you and your business in a very short period of time. It is essentially a little bit of code that stalks your every move. It then sends all that information back to someone who can use it to harm you or your company using all the information that has been collected.

How do web security services help me here?

Investing in a quality web security product can reduce your risk in this area significantly. It can prevent your machine becoming a member of any botnets* and it stops installed spyware from calling 'home' to deliver network or computer specific information. It can also prevent malicious redirects or cross site scripting (xss).

*Botnets: a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.

Ransomware

Definition: A type of malicious software designed to block access to a computer system (network drives, email systems – everything) until a sum of money is paid.

Ransomware is widespread and only going to get worse in the coming years. Ransomware locks everyone out of their file networks and applications (including their email!) and demands payment to release the lock.

Statistics show that many organisations pay out in order to get their systems back online. This is a dangerous precedent to set with hackers as they will attack you again and again.

How do web security services help me here?

Ransomware is another scary bit of software. It prevents you from accessing your files, emails, applications – everything that runs your business or organisation.

This is really where a decent web security system is worth its weight in gold. Invest in a system that has sandboxing as part of its offering and you will potentially see a ROI in just a few months. Sandboxing is a methodology where all downloads, especially office documents (the preferred delivery method of ransomware) can be analysed in depth in a secure location - off your network - to check for any embedded ransomware BEFORE it reaches your network.

Phishing

It is important to distinguish between the two types of phishing in online security - email phishing and phishing websites.

Email phishing - the fraudulent practice of sending emails supposedly from reputable companies in order to get people to reveal personal information, such as passwords and credit card numbers.

Phishing websites – websites which pretend to be a site they are not. This could be a website pretending to be your bank, so it can record your banking details.

How do web security services help me here?

Focussing on phishing websites for this section, you can look at web security from the point of view that it analyses websites on the fly. What it will be doing here is establishing whether the site is trustworthy, by assessing risk factors such as does it try to download anything to your computer and how long the website has been live; phishing websites are generally quite new and disappear quickly.

Social engineering / Spear phishing

Definition: The use of personal information garnered from direct contact or social media to specifically target someone in order to gain information or money from them.

Targets of this type of attack are often senior managers or finance people who have access to the company's bank accounts.

How do web security services help me here?

Social engineering attacks are more of an email security threat, however web security can help here too. If an email contains links to bad websites or harmful attachments, then working in partnership with your email security service, web security adds another layer of protection.

Zero day/zero hour attacks

Definition: Attacks that target - in the majority - publicly known but still unpatched vulnerabilities in your operating systems and applications.

How do web security services help me here?

This is another area where web security and another security option work hand in hand. In this case it is web security working with your end point protection. Both work in a similar way to protect against this type of threat, whereby they have the flexibility to roll out patches to known security issues on standard software. The software vendor can often take up to a week to roll out a security update whereas the power of the cloud allows cloud web security providers to roll out a fix in hours or even minutes.

Another area where cloud web security comes in useful in this type of scenario is the ability to detect the breach in the first instance. Once a breach is detected in the cloud, it is blocked for all cloud users.

Accidental or non-malicious business threats:

The web security threats discussed up until this point are all deliberate attacks on your organisation's network. But what about accidental threats?

Data Loss

Information is often transmitted freely by email within an organisation and stored in archives. But what if sensitive information is sent outside your organisation? If a customer emails you their credit card information should you be able or allowed to forward that email to a colleague. Should your employees be able to send sensitive customer data to their personal email addresses?

How do web security services help me here?

Web security services have the capability to protect your organisation's data leakage points e.g. web mail (yahoo, gmail etc) and social networking sites. Any kind of data leakage points can be analysed for set phrases and keywords associated with confidential information to protect your intellectual property and sensitive customer data. Examples of this are files that contain words such as 'confidential', 'private' or strings of information such as credit card numbers and bank numbers, customer data with email strings etc. can all be prevented from being emailed via popular web mail sites.

Shadow IT

Shadow IT is a relatively new term but creeping into the vernacular as more and more organisations start to understand its potential as a security risk. It is defined as a system or application that has not been installed nor is it maintained by your IT department. Examples of this are file sharing systems or video conferencing systems or games which have not been sanctioned for use within your organisation but which your users have put on their computers for convenience or fun. The risk here is that this software will become out of date, or will hold sensitive business information, or will be the cause of big productivity losses. In the case of sensitive business information being stored on unsanctioned and potentially out of date software or cloud services, the issue is that your organisation is no longer in control of the data and the applications that have been installed may even be forgotten about by the users meaning your network and data is no longer secure.

How do web security services help me here?

Cloud web security services can help here in a few ways. First of all they are constantly scanning traffic on your networks and therefore can identify malicious destination traffic or specific traffic types such as "Command & Control" botnet servers. This means the cloud web security product can see if a computer on your network has become victim "a slave" to a botnet, due to an out of date application.

Cloud web security services can also be used to restrict your user access to common cloud applications like Dropbox, or gaming software, meaning less productivity losses and preventing data loss.

Productivity losses

We have up until now, discussed threats in terms of damage and risk to your networks and IT systems. However in terms of what can be monitored by cloud web security services, productivity monitoring and controlling what your employees and colleagues can do and see online are key considerations for investment. Web security software is so much more granular than firewalls and can allow you to adjust policies for departments, people and location. Being able to monitor what people are doing online, when they are doing it and for how long can help move your organisation to productivity highs.

How do web security services help me here?

We touched on this above around the idea of restricting access to gaming applications but it can be applied to social media sites, recreational sites and so on. This filtering element of web security is a big one where employee productivity is concerned. You can also use the reporting element of the service to highlight repeat offenders and caution people on correct use of company time and equipment.

A real-life example of the benefits of web security

Let's take a look at one of our active web security clients. This customer has 1,000 seats on our WebCritical platform. Below is an anonymised breakdown of their account statistics over a one month period.

Overall their network was protected from *6,152,280 potentially harmful activities*. 5,391 of these were threats and 6,146,889 were policy violations*. We detected and blocked *4,482 instances of malicious content* that could have infected the network and we *blocked 3 attempts by botnets* to "call home" and potentially steal data. **All this in just ONE MONTH!**

Take a look at the table below, it outlines the URL classes from within the organisation's risk categories and shows how many of each class were blocked or allowed. WebCritical allows administrators to then drill down to the specific data sets to see who is accessing these blocked sites in order to highlight lost productivity and/or threat areas for senior management to review:

URL Classes	Blocked / Allowed
Business Use	Blocked 3.8 M / Allowed 77.5 M
Productivity Loss	Blocked 101.3 K / Allowed 8.6 M
Bandwidth Loss	Blocked 38.5 K / Allowed 6 M
General Surfing	Blocked 2.2 M / Allowed 3 M
Legal Liability	Blocked 208 / Allowed 243.1 K
Adv. Security Risk	Blocked 5.4 K / Allowed 422
Privacy Risk	Blocked 739 / Allowed 0

The table below shows the number of times attempts were made to access blocked content. Administrators can then analyse the data to find repeat offenders.

No. of blocks	Categories
83	Anonymizer
62	Computer Hacking
49	Pornographer
10	Copyright Infringement
4	Nudity

WebCritical also allows you to analyse areas marked as liability exposure and use that information to find new areas to block or to highlight areas of large productivity loss. This is another area where you can drill down into the data to identify which users in your organisation are accessing this content and report areas of inappropriate work-time activity.

No. of visits registered	Categories
234,932	Gambling
3,910	Lingerie/Bikini
1,659	Questionable
867	Adult Themes
792	Copyright Infringement

*Within the WebCritical portal you can set up a series of policies specific to your organisation. These can be around department or individual access to websites, the type of threats you want to block, whether or not you allow certain activities to be carried out on certain sites and times employees can access certain sites etc.

A 2018-style security breach

What will a 2018-style security breach look like? The risks are no longer as simple as potentially losing access to your network. The introduction of regulations and legislation like GDPR mean that security breaches are now more costly than ever before. You *must* report them and as it currently stands breaches *will* be penalised. In all of these scenarios reputation management also comes into play, particularly where you are dealing with customer data and your ability to protect it.

So a 2018 style security breach means:

- loss of customer data
- compromised financial systems
- loss of access to critical business applications
- damaged reputations
- potentially huge fines

The more you digitise, the more pathways there are into your business operations and the more you open yourself to risk. However if your organisation does not embrace digital, you risk lower productivity and efficiency, and higher costs. The less you digitise the less you are capable of doing as an organisation from a productivity and resource point of view. It's a catch 22.

However, as we discussed there are ways to reduce your risk across the board.

Let's look at the checklist on the next page and go through some of the more common security threats and what you can do today to reduce your risk in each area.

Your Checklist

Time to take stock. How does your network security measure up?

Risk area	What have I done?	What can be done?
Systems updates and upgrades		For all known applications installed on your network and machines, have you applied all the updates recommended by the vendor? For everything else, do you regularly take stock of what is on your colleagues' machines and if everything is up to date? Do you have a formal patch management protocol?
Backups		This one is simple. Do you take regular, secure backups of your network? To go a step further, do you regularly educate colleagues on the importance of using company drives rather than their computers' hard drives or external drives such as USB sticks? Have you ever tested your ability to successfully restore from a backup?
Employee awareness		Do you make your colleagues aware of modern cyber threats? Do you hold regular training sessions within your organisation to ensure people understand how to avoid common pitfalls? Do your senior managers know how to spot a phishing or spear phishing attack? (If not, download our guide here.)
Spyware		Do you have a strong web security product which can prevent the download of malicious software? Does your web or endpoint security product scan for unusual behaviour on your network and computers?

Risk area	What have I done?	What can be done?
Ransomware		Do you have a strong web security product which can prevent the download of malicious software? Do you employ sandboxing for downloaded documents? Does your web or endpoint security product scan for unusual behaviour on your network and computers to identify any problems? Do you have network backups which you can use to roll back to a safe point? Do you have DR solutions in place including email continuity? This would allow you to access your email even in the event of a ransomware attack.
Phishing (Websites)		Do you have a strong web security product which can analyse how safe a site is and block those that are deemed unsafe?
Spear phishing		Do you ensure that anyone who has access to business critical information is aware of the ways in which they could be compromised? Do you hold regular training sessions with senior managers and finance staff to ensure they know how they could be tricked into revealing confidential business information? You can download and use our handy guide to help you here.
Zero day attacks		Do you have a robust endpoint security system? Do you have a web security service in place? Are you applying all patches as and when they come into play?

Risk area	What have I done?	What can be done?
Data loss		Does your business have restrictions in place with regards to who has access to what data? Do you have a web security system in place that can identify and stop sensitive data from leaving the organisation through external means? Does your email security system have policies in place which scan for things like credit card information and customer data being sent externally by email?
Shadow IT		Do you have admin locks on individual machines meaning only IT can put applications on PCs? Do you do regular scans of colleagues' machines?
Productivity losses		Do you have web usage policies? Do you have a filtering system which can allow people access to what they need by department or role and restrict access in the same way? Do/can you report on internet usage? Do you restrict access to certain types of content?

Online Security Threats Matrix

Our handy online security threat matrix* below can help you identify key threats and highlights the relevant security product needed to combat them.

	Email Security	Endpoint Protection	Web Security	Web Filtering
Threat				
Malware	x	x	x	
Spyware	x	x	x	
Ransomware	x	x	x	
Viruses	x	x	x	
Phishing (email and web)	x			x
Spoofing	x			x
Social engineering	x			
Zero day exploits	x	x	x	
Productivity losses				x
Legal liability	x			x
Human error	x	x	x	x
Data loss	x		x	
Shadow IT	x	x	x	x
Reputation	x			x

*please note this matrix is not an exhaustive list of threats and solutions and should be used as a starting point only.

FuseMail Web Security – WebCritical, Powered by Zscaler

FuseMail's WebCritical offers a uniquely stable and powerful web security option to the SME market. The product forms part of the world's largest security cloud and is employed by leading global enterprises. We have now made it more affordable then ever for the SME market through our new package options. Pick and choose from a range of possibilities to ensure you have all your bases covered.

Use the table on the next page to choose the package and add-ons that would best suit your needs or work with our web security experts to find the solution for you. Take a look below at the benefits of choosing WebCritical for your web security.

Key product benefits

- Build your own product bundles to suit your needs
- Protect your organisation from web-based threats
- Take control of internet browsing
- Enforce web usage policies to all users regardless of their location or device
- Improve operational resilience with multi-site and roaming user support
- 24/7/365 UK-based product support

Benefit from the world's largest cloud footprint

WebCritical has the largest cloud footprint in the world. We can demonstrate this by looking at our worldwide datacentres. This means you get the benefit of cloud-learning on a massive scale. Once a threat is blocked for one of our customers, it is blocked for all of them.

WebCritical – Web Security Packages and Bundles

FuseMail's WebCritical internet security bundles get a revamp with more flexible, cost-effective packages and a choice of add-ons. WebCritical offers faster, easy to scale, cloud internet security for users in the office and on the road across devices. Choose the package below that best suits your needs and then select from a range of add-ons to boost your internet security.

	Professional	Professional+	Business	Transformation
CLOUD SECURITY PLATFORM				
Data Centres Global access, high availability, with latency SLAs	✔	✔	✔	✔
Traffic Forwarding GRE tunnel, IPsec, proxy chaining, PAC file, or Mobile App	✔	✔	✔	✔
Authentication SAML, secure LDAP, Kerberos, hosted	✔	✔	✔	✔
Real-Time Cloud Security Updates Receive full cloud threat sharing (cloud effect), daily security updates (over 120,000/day) and 60+ security feeds	✔	✔	✔	✔
SSL Inspection Full inline threat inspection of all SSL traffic with SLA. Granular policy control forcontent exclusion	Add-on	✔	✔	✔
Nanolog Streaming Service Transmit logs from all users and locations to an on-premise SIEM in real time	Add-on	Add-on	✔	✔
CLOUD SECURITY SERVICES				
URL and Content Filtering Granular policy by user, group, location, time, and quota; dynamic content classification for unknown URLs and Safe Search	✔	✔	✔	✔
File Type Control True file type control by user, location, and destination	✔	✔	✔	✔
Inline Antivirus & Antispyware Signature based antimalware and full inbound/outbound file inspection	✔	✔	✔	✔
Reputation-Based Threat Protection Stop known botnets, command-and-control communications, and phishing	✔	✔	✔	✔
Standard Cloud Firewall Granular outbound rules by IP address, port, and protocol (5-tuple rules)	✔	✔	✔	✔
Advanced Cloud Firewall Full outbound next-gen cloud firewall with application and user awareness and location control; full logging and reporting	Add-on	Add-on	Add-on	✔
Bandwidth Control Ensure business apps like Office 365 are prioritized over recreational traffic	Add-on	Add-on	✔	✔
Standard Cloud Sandbox Zero-day protection for .exe and .dll files from unknown and suspicious sites	✔	✔	✔	✔
Advanced Cloud Sandbox Zero-day protection for all file types from all sites; ability to hold file delivery until confirmed sandbox clean; advanced reporting			Add-on	✔
Advanced Threat Protection PageRisk and content analysis of malware, callbacks, cross-site scripting, cookie stealing, and anonymizers	Add-on	✔	✔	✔
Cloud Application Visibility & Control Discover, monitor, and control access to web applications	Add-on	Add-on	✔	✔
Mobile Application Reporting & Control Visibility, granular policy control, and threat protection for devices on the corporate network			✔	✔
Web Access Control Ensure outdated versions of browsers and plugins are compliant	Add-on	Add-on	✔	✔
Data Loss Prevention Inline scanning to prevent confidential data leaving the organization	Add-on	Add-on	Add-on	Add-on

Enterprise License
An Enterprise License Agreement bundle, which includes all available add-on services, premium support and deployment advisory services, is available for customers with 10,000+ seats

Your Cloud Web Security Options

Cost

Security is not an area where you should cut costs. You need to ensure that your security budget is where it *needs to be* in terms of reducing the risk to where your senior management *think it should be*. Do you carry out regular risk reviews in line with expectations and budgets and report back up the chain?

The questions you need to pose to your management team are simple.

- How much money and time are we losing trying to fix problems associated with potential or real security breaches?

And ...

- How much are we losing in lost productivity because we have no ability to sensibly filter and monitor web usage?

Services

Although we have focussed primarily on web security in this document, it is critical that if you do want to reduce your risks as much as possible, you look at all areas available to you including web security, email security and endpoint protection.

Service providers

FuseMail is a leading cloud security service provider covering all three major cloud security areas – email, web and endpoint.

We help organisations big and small cover their bases and benefit from the cloud security effect without blowing their budget. We also offer industry leading support from the UK 24/7/365 as standard, across our service portfolio.

Get in touch to discover our industry leading services

Call +44 (0) 800 093 2580

Email uksales@fusemail.com

Visit www.fusemail.com/en-gb/

Take Action NOW

Book your demonstration

Sign up for your free trial

About FuseMail®

FuseMail® enables businesses around the world to communicate with confidence every day. Our cloud based services provide simple, secure, and scalable solutions for email security, spam/virus filtering, archiving, encryption, web security and email hosting. With award-winning local support and an international suite of products and features, FuseMail® is a world leader in email and web security.

WebCritical web security

WebCritical cloud-based web security gives you control over what employees do online and protects your organisation from web-based threats. Read more online.

SecureSMART email security

SecureSMART's multi-layered security keeps you safe from known and emerging email-based threats, using a combination of custom filters and industry-leading anti-virus, anti-spam and anti-phishing engines. Read more online.

ClickSMART URL protection

ClickSMART provides another level of protection against phishing and ransomware attacks by preventing email recipients from clicking on dangerous URLs. It rewrites web links in emails, enabling them to be rescanned at the time of the click. Read more online.

ContinuitySMART email continuity

Adding ContinuitySMART to your SecureSMART package upgrades SecureSMART to SecureSMART Suite. This upgrade brings with it always-on email continuity and 90 days of email replay. Read more online.

ExchangeSMART Hosted Exchange

ExchangeSMART is FuseMail's Hosted Microsoft Exchange solution that provides you with all the features and collaboration options of an in-house installation of Microsoft Exchange, but without the prohibitive costs and time-consuming administration. Read more online.