Cloud Application Control: Redefining the Secure Web Gateway

www.censornet.com

Cloud Application Control: Redefining the Secure Web Gateway

Porn; love it or pretend it's something you once saw by accident at a friend's house, was at one stage both the undisputed king and at the same time, utter scourge of the Internet. On the one hand, it reigned through sheer size and dominance (no pun intended) and on the other, it vicariously gave birth to a whole security software industry, designed entirely to keep you, your children, work colleagues and Grandmother from seeing something that they shouldn't.

Web Security and Content filtering in its infancy was like a well-meaning overbearing parent. It's intentions and heart was in the right place but being told to wear a duffle coat and mittens on a nice sunny day on the off chance there may be a slight stiff breeze, is potentially overkill in anyone's book.

Today, we understand that cyber crime is at an all time high, not only in numbers but sophistication and in turn the security industry has developed multi-faceted layers to go toe-to toe with the bad guys. But if you go back to the origination of why web security and content filtering was first created, it all stems back to against web-based malware and controlling access to inappropriate content.

'If in doubt, block it' became the mantra of the corporate organisation and the Internet went from a liberating world of possibilities to a dangerous place where all sharp things were put out of our reach, the walls were padded, our hand was held and corks donned the end of our forks.

It isn't by any stretch a criticism; rather a fair and measured observational response to what was then unknown. At the time it was unquestionably the right thing to do until we figured out what was good and what was downright dangerous.

In the very beginning the Internet was relatively safe. Microsoft hadn't really upset anyone at that stage and the cyber criminal underworld had no reason to go hunting in cyber space. The worse possible outcome of a cyber attack was the unwelcome arrival of a Rick Astley screen saver that you couldn't remove or - if you were feeling especially gullible - a link with the promise of seeing Britney Spears naked doing something unspeakable to a snake. They were good times.

Fast-forward to today and the Internet is a modern day virtual deity in contrast, the nucleus to our daily lives but now we know the difference between good and bad from lessons mostly learned the hard way. The risk register has been re-

written, redefined and is borderline unrecognisable. We've also begun to trust websites in the same way as we once viewed the banks before they proved us horribly wrong, the evidence resides in our everyday activity.

On-line shopping is growing by roughly 20% year on year and if a small padlock appears in the URL bar, we'll happily hand over our credit and debit card details to well, almost anyone. The risk of explicit content has been marginalised and with good reason; from a cyber security perspective, you are statistically safer if you 'accidentally' visit a pornographic website than you are browsing a well- known high street online store. Much has changed.

Moreover, after years of 'talking about what the Cloud can potentially do', the rise of the Application has given it context and an actual definition in the real world that means something.

According to 'statisa.com', there are 1.3 million apps available across Android and Apple stores. That's just insane. Most companies are deploying cloud solutions, the expectation being that in 2018; some 59% of companies will be using SaaS (software as a service) in some capacity. Name your favourite large business software vendor and we'll show you evidence of their desire to lead with cloud-based solutions.

Here's a great example. Take the three largest software vendors (according to the annual Forbes 200 ranking) Microsoft, Oracle and SAP are positioning and marketing themselves as cloud companies. SAP is now even badging themselves as "The Cloud Company." When did that happen?

So where does this leave the traditional role of Web Security and Content Filtering? The truth is that it still has its part to play if it can adapt; but adapt it must and quickly and therein could lie the issue.

If you take a good, long, hard, undiluted look at the Web Security and Content Filtering market, it becomes abundantly clear very quickly that many of the products designed to protect us over a decade ago, haven't changed to address the rise of the Cloud Application; thus rendering their role, borderline redundant.

And this is why it has to change

The digital ecosystem offers opportunity to businesses of all sizes to reduce operating costs and optimise resource usage. Increasingly more organisations are delivering tangible value by encouraging mobile working practices, be it by simply providing mobile devices such as laptops, tablets and smart phones in a 'here is your device' (HYOD) agreement or by allowing their workforce to use their own devices i.e. bring your own device (BYOD) - click to read a white paper

The attraction of the latter is self-evident, it saves organisations money and it facilitates a blurring of the work-life boundaries. Mobile working naturally supports a "never off duty" culture. But whilst commercial opportunities arise from the rapid evolution of digital technology and software, so the question of security arises. A 2013 article in The Journal of Global Research in Computer Science provides an overarching review of the security issues around mobile devices.

Whereas once it was sufficient to protect desktop devices by applying URL filtering to discover swear words in town names, the world has moved on and traditional security practices no longer cut the mustard in today's modern day digital society.

Users will find a way around everything

It's far too easy to openly scrutinise the user because we pretend they're 'somebody else'. They're not; they're you, they're us and the truth is, we're as guilty as they are because we're well, one of them.

Part of the reason the growth of cloud apps has posed such an open ended issue for the heritage of Web Security and Content Software is because broadly speaking, users will use

their judgement or lack thereof, tastes and preferences to use the tools they favour to get things done their way.

If you have legacy systems in house that are clunky and prevent your employees from getting their job done, they will, without fail find a way around them and guess what, the secure route is seldom the easiest one.

So, how do you manage risk and leverage value in an "everything-as-a-service world"? The risks themselves are becoming easier to define. Cloud applications in theory can be made secure at the point of access (see Amazon's AWS white paper) but that doesn't solve the issue at the point of use.

It has been proven that it's impossible to be 100% secure, so the importance of minimising the probability of either doing something daft or being cleverly socially engineered has to be top of every organisations agenda. Donald Rumsfeld said it best "there are also unknown unknowns -- the ones we don't know, we don't know". That quote is great but it's unlikely to help you if you end up having a tricky conversation with the Information Commissioners Office (ICO).

As a business, being able to define the boundaries of cloud and Internet access, application and data use, is key to delivering a more secure way of living with cloud services and working on the move. Embedding corporate applications into an employee's world requires a thorough understanding of how each employee may use their device or devices (the average number per person being three). With HYOD, the solutions can be as simple as locking down a device. By installing specific security protocols including encryption, local wipe, remote wipe and selective wipe functions, devices can be made very secure.

A lockdown policy can be as restrictive or as lax as a business's governance guidelines deems appropriate for any given role or job function. Not being able to download private apps or access restricted Internet sites makes the use of such devices rather constrained and the users less than happy.

It does however ensure that all users of those devices adhere to corporate intranet and computer use policies. On the one hand, you've managed to make data loss of sensitive information far less likely, on the other hand your users will soon find ways around your well-meaning policies. It simply negates the benefits of allowing employees to interleave their social and work lives.

The luxury we lost some time ago when aiming to secure our corporate world is that somewhere between the first iPhone and the Apple iWatch the users became savvy and smarter about technology than the poor IT departments looking to keep the lights on and protect them. Where there is a Wi-Fi, there's a way and there is nothing a determined user can't achieve without a search engine - In Google We Trust. And word spreads. Circumnavigating rules and restrictions isn't always intended to be reckless. On the contrary, it is seen as necessary to be productive.

You can of course fight it but you lose both ways, so embrace the fact that you need to secure the way that a user works in the real world, or it's probably time to get your flux capacitor back up and running and high-tail it back to a time when life was simpler and mobile phones weighed slightly less than a small horse.

There is a general acceptance beginning to evolve that an organisation must be able to monitor an individual's use of corporate assets at the most basic level, regardless of where they are and what device they are using. The selection process of cloud application control software should be done with this balancing act in mind or it is doomed to failure. There is a fine line between draconian control and acting as a benevolent dictator. There is a new wave of thought starting to evolve that as an organisation, it is incumbent upon them to find a way of delivering effective security whilst riding the digital innovation wave that leads to the land of productivity and happy people.

It was not that long ago, that misplaced disk drives or even complete laptops (left in trains or under pub tables) proved an embarrassment to some of the more sensitive civil service

departments. But that didn't prevent the rise in laptop usage as a way of providing remote and flexible working, it just got bigger, be it on trains, airplanes or at home. Sit on any form of public transport the world over and if you manage to make contact with another human being who isn't locked in a romantic gaze with an electronic device of some kind, then we have to safely assume your time machine was a complete success.

Providing employees with a sense of freedom is fundamental to maximising the value from the mobile and always-on culture in which we all live. Equally, the responsibility to keep the person and the corporate information safe is of integral importance.

The need to educate the user will never go away but asking them to refine their behaviours and diligence when they're busy and have a day job to do can't be viewed as a serious strategy.

We work and play invariably on the same devices and we are all users no matter how we define it; therefore how we protect our data needs to evolve to reflect and protect the way that we work in the real world.

Shadow Lands – The technological Bermuda Triangle

'Shadow IT' is easily dismissible as the buzzword to feed a new wave of excitable industry journalists but the cold hard truth is that it is alive, well and it has legs.

The consumerisation of information technology is creating a Shadow IT community and it is a planet where the CIO has little or no control; it's also on the rise. "Everything-as-a-service" presents the opportunity to buy localised, cloud apps that can complement or replace corporate on-premise systems software and most users will opt to use familiar apps and assume that their popularity or their brand makes them safe.

There is no sense that this will change any time soon, in fact the opposite is probably true because apps like Dropbox for example are simple, available and easy to use. If you can deploy an app in seconds to get the job done without the delay of following process or involving secure due diligence, then why not?

The issue is ease of use and a known brand is confused with tried and trusted. Applications intended for the Enterprise Market will almost certainly contain security consideration at a basic level but are often aimed more at making our lives easier and therefore naturally carry the risk of fallibility.

As more companies seek to embrace cloud applications to replace on-premise legacy systems, it's easy to miss the blindingly obvious. Apps are generic by definition; they are created to service a mass market and the security considerations are broad and lack granularity, therefore the natural by-product creates unnecessary risk.

If security and privacy requirements are to be meaningfully applied, the business needs greater visibility and control of enterprise data in the cloud that is accessed using both managed and unmanaged devices.
Shadows aren't by definition scary, particularly in the cold light of day.

Why Planning should always precede Application

The risks are less insurmountable when you break them down into bite-sized chunks and with decent planning the unprecedented rise of cloud applications doesn't require taming, it's a wave that can be ridden safely.

As we move beyond the basic capabilities of Web Security and Content Filtering and take into account the applications that we use, it's important to scope what the risks are and what policies are in place to protect the organisation data and the user.

- What are the liabilities of the company and what are the liabilities of the employee?
- Can the policy be legally enforced?
- Are there guidelines in place for File Sharing?
- Is there a list of accepted or banned known apps?
- If data is lost will the employer and/or employee be liable for a fine or disciplined and how will the rules around that be defined e.g. what defines culpability on the employer or employee's part?
- How will the standing orders of the Data Protection Act be enforced?
- What will an employee have to agree to i.e. installing of monitoring software, security protocols etc. on their personal devices?
- Are there any restrictions on private apps on private or corporate devices?
- How is access to data to be managed?
- How is corporate data protected from access via personal devices?

Protection also doesn't mean prohibiting the user but the ability to identify, capture and manage any unusual activity that may compromise the organisation through use of a personal device. There is a fine line between an invasion of privacy and an airtight solution that protects the integrity of company data.

Why 'Cloud Application Control' rocks

"By 2016, 25% of enterprises will secure access to cloud-based services using a CASB (or CAC) platform, up from less than 1% in 2012, reducing the cost of securing access by 30%" - Gartner – The Importance of Cloud Access Security Brokers (CASB).

Gartner 's prediction is well founded. They believe that cloud access security brokers would be the top security technology during 2014/15. Minimising corporate exposure whilst maintaining control was at the heart of their opining.

Their recommendations make interesting reading and they urge the market to consider the following areas of technology and design when evolving an approach to Cloud Application Control (CAC):

- Start with getting visibility into the use of cloud applications and the potential risk they represent.
- Rather than requiring the purchase of yet another security gateway device, query existing SWG and identity federation gateway providers to determine whether they offer the needed CAC capabilities.
- Evaluate broader cloud access security brokers or cloud application control providers that will also provide some basic security capabilities (such as identity services) as this market matures.
- As an alternative to on-premises appliances, consider CAC/CASB solutions that are capable of delivering the same type of security and policy enforcement without requiring all traffic to be routed through on-premises appliances.
- Understand the limitations of how the CAC/CASB inserts itself into the data path — for example, forward proxy, reverse proxy, SAML redirection, client-side agent and so on. There are pros and cons with each of these techniques

In a nutshell, the more capable an organisation is able to extend its security protocols hand in hand with its employees, the more likely it will be to respond to market, technological and social changes for that matter.

Just as social media has helped re-create and extend how we interact with each other, we should allow the rise of the cloud application to revolutionise how employees do their jobs but to make that work, protection has to evolve beyond the web gateway and into the realm of CAC.

Web security and content filtering has traditionally been built around the assumption that organisational perimeters are fixed and the boundaries understood but in a 'Everything as a service' market, that is no longer an applicable set of rules. There is an abstraction of the historical security models taking place that requires the orchestration of smarter

solutions. It isn't that the way which we protect the web gateway is wrong but it must be extended and adapted to follow the behaviour of the user.

Everybody walk the dinosaur

The web security market has undoubtedly flourished as Cyber Crime has become increasingly sophisticated and in theory we should be building upon our learning's from the last decade. The concern however is that many of the trusted vendors, known brands who are charged with the responsibility of keeping us safe from the bad guys have barely changed or improved in recent years.

Just because it sounds insulting, doesn't make it any less true.

Many of the traditional web security software vendors designed their software pre the digital explosion. Because of the velocity in changes to technology, it is simply not sufficient to deploy sentinel software i.e. guarding the gateway to the internet of all things. Security needs to be aggressively offensive to defend both the corporate body and the employee. All high-risk threats have to be dealt with extreme prejudice.

Security architects require an umbrella that spans the corporate entity and its remote employees. But it needs to be an umbrella that is made of titanium, folds down to the size of a matchbox and automatically deploys at a demi bar increase in barometric pressure. Add to all this, the ability to manage user roles, redact sensitive data if required, analyse, report and generally shine a light on who is, or is not complying in order to generally help sniff out possible nefarious behaviour.

It's no surprise that there has been an emergence of Cloud Application Control Providers or Cloud Access Security Brokers of late, technologies positioned to plug the gap of the vicarious user that is hell bent on productivity at all costs.

Change is afoot, for those who seek it.

Conclusion

The importance of bridging the gap between Web Security and Cloud Application Control

We've identified that in the 15 years since web security and content filtering was first created, the landscape in contrast is unrecognisable. Salesforce was in its infancy, YouTube didn't exist, so if you wanted to watch videos of cats doing the funniest things, then therapy was your only real outlet. The term 'Facebooking' was a made-up verb waiting to irrevocably destroy the English language and you could happily turn on your computer safe in the knowledge that nobody would be sending you pictures of what they were about to eat. They were indeed simpler times.

Today, it seems you're sandwiched between security vendors that offer traditional web security and content filtering products designed to protect a very different market to the one we know is flourishing in activity, yet steeped in unknown risk. There is also an emergence of new cloud application control providers, purely aimed at the cloud application market with no tenure or history in the learning's that have came from coping with the complexities of the web in the last decade. Very few vendors give the visibility, analysis and control that are needed to have any meaningful impact in the current digital world.

There has been a void in the market for some time that bridges that gap between traditional web security and content filtering and the next generation of CAC. To protect doesn't mean to prohibit and there are ways to allow users to flourish but still keep them safe.

It does require a shift in conventional web security thinking though but that's what is needed when you are looking to protect an extraordinary market.

Modern cloud application control should truly 'follow the user'. It should enable the discovery of all cloud apps and services, analyse the risk and be able to audit and log all usage, maximising visibility for everyone's benefit beyond simply reporting after the event.

There is a clear need to have a service that runs in the cloud responsible for aspects like authentication, policy enforcement and reporting, but also a component that is installed either locally on the network (as a virtual software appliance) or on

the endpoint (as native client software), or it could be a hybrid combination of both.

Having on-network or on-device control is critical but more often than not is absent with a pure cloud service. Ideally you also need a lightweight protocol that works without the need to 'proxy' the web content to centralised servers. If you try to use a new security product that increases latency, you won't be winning any popularity contests any day soon. Speed however, doesn't need to come at the cost at the integrity of protection, it still has to do the job and do it well.

We've established in this paper that keeping away 'all things naughty' has been marginalised by the rise of bigger and nastier threats and the age of 'Allow or Block' is far behind us. By simply blocking, the risk is run that a company misses out on all the productivity gains the app related world delivers but lurking behind that same inviting door could be the very thing that loses your data or has a profoundly negative effect on the organisation.

CAC clearly has the opportunity to revolutionise the web security and cloud market but it needs to go beyond the new shiny marketing strapline and live up to its hype. It must demonstrate the capability of an enterprise secure web gateway but deliver real time discovery and analysis of cloud applications by enabling true visibility and demonstrate authentic control.

As Web Security and CAC evolve, the focus will inevitably shift to better, smarter ways to monitor suspicious behaviour, control functionality and encrypt information within a public or private cloud application; it will have the ability to ring fence sensitive data and greatly minimise the probability of it landing up in the wrong hands.

Web security products that act as a forensics tool after the event, to put it politely have little or limited value and there are plenty of them.

Simply put, we need to take all of the learning's and value we have gleaned from understanding trends and behaviour from traditional Web Security and Content Filtering, then extend that capability to redefine the role of CAC to realise its full potential. If we successfully bridge that gap, CAC ceases to be just a promising possibility and becomes a meaningful deliverable in any organisation.

Company Head Office
Network House . 6th Floor . Suite 6.01
Basing View . Basingstoke . RG21 4HG . UK

Research & Development Centre
Bristol & Bath Science Park . Dirac Crescent
Emersons Green . Bristol . BS16 7FR . UK

Contact UK
t: +44 (0) 845 230 9590
f: +44 (0) 845 230 9591

Contact USA
t: (408) 290-6688
f: (408) 351-4294

Visit us online at www.censornet.com