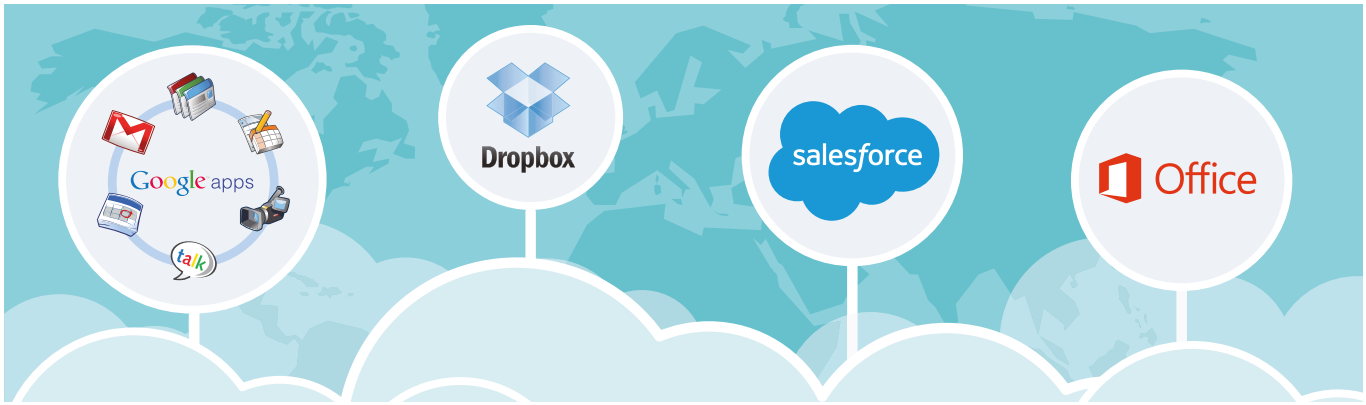
CENSORNET

WHY CLOUD APPLICATION SECURITY CONTROLLERS WILL RULE THE WORLD

Whitepaper

WHY CLOUD APPLICATION SECURITY CONTROLLERS WILL RULE THE WORLD

If we're being entirely honest, 'Cloud' and 'Security' are far from a natural marriage, in fact, on the surface, it's a partnership that shouldn't work. Cloud is seen as creative, open, progressive and inherently sociable. It's attractive to many and has a promising future to offer to any potential suitor. Its personal ad is therefore unlikely ever to read 'Seeks overly possessive, naturally paranoid control freak for companionship, windy walks and overbearing governance'.



Security bears the burden of a well-earned stereotype. Its job has been to historically govern and protect; to be dependable and predictable. Although its profile has soared since cyber attacks outstripped gun and drug crime combined, the perception of the role it has to play is still about as sexy as a comfy pair of slippers.

The shame is, when Cloud and Security are both at the top of their game, they have the opportunity to be the ultimate power couple but as things stand today, if that is to become a reality, much has to change.

The emergence of Cloud Application Security (CAS) is beginning to position Security in a new light, gives it a new wardrobe and puts it well and truly back in the game. In this whitepaper we discuss the change in the challenges that Cloud once presented, how the rise of the App has affected what we need to ask of Security and why the inclusion of CAS capability as part of the security functionality has the opportunity to make Security the hero it once was years ago when we first discovered it was no fun catching nasty viruses.

FIRSTLY, CLOUD ISN'T THE PROBLEM

The liberal way in which Cloud is used in the world has meant that it often finds itself on the front page of the newspapers for all the wrong reasons and usually hand in hand with a nasty salacious headline.

Before the Apple iCloud hack found itself in the public domain last year, you probably had no idea who Jennifer Lawrence was and why she seemed so averse to wearing clothes around mobile phones.

Poor iCloud, once trusted by millions; it was the ultimate virtual baby sitter for our personal imagery, a brand so loved that we forgive almost anything because it's both cool and pretty. Then one bad day at the office later and our hero joined the ranks of the compromised and was left looking at the carpet for answers.

Did people stop using it? Of course not but the exposure of its fallibility struck fear into the hearts of anyone that employs the camera function on their phone for anything other than taking pictures of their dinner. The news leaked, the public was enraged, villagers were angry and a scapegoat had to be identified. The Cloud was evil and it had to be stopped.

Not the bad guys, no. Not the annoyingly clever criminals who had by-passed the seemingly airtight security; nope, this thing called the Cloud has ruined everything and it couldn't be trusted.

Now you could argue it's naïve to think that if you take a naked picture of yourself, your partner or an unsuspecting neighbour, that once you hit 'delete' it disappears into a cosmic bin for all eternity; like a magical deviant landfill.

On the other hand, you could say, what's the point in having a delete button in the first place if it doesn't permanently wipe the evidence off the face of the earth never to be seen again. If it doesn't totally destroy everything, then it may as well be called the 'I feel lucky button' on Google.

Either way, it sent out a message to the general public at large, even the world's biggest, coolest and most trusted brands may not be safe. Popularity and a cool logo doesn't equate to a secure service.

Now to the business world, this was far from news because the reticence to adopt certain elements of Cloud is a well-trodden path. We'd been to the Expo's when it was first mentioned, we watched as it was re-branded, re-diced and redefined as public, private, hybrid, on-premise, off-premise and simply App-tastic but none of them eradicated its abundant and exposed Achilles heel; security. Cloud in its infancy represented as much risk as it did opportunity and if we're honest we knew nothing before we began using it in the real world.

The whole iCloud episode, similar stories that preceded it and those that are yet to come should teach us at the very least, the blindingly obvious. The Cloud isn't the problem, frankly it's awesome but it does need to be protected in a manner conducive to the way that it is used.

IT'S TIME TO BURY THE VIRTUAL HATCHET

When Cloud was the new kid on the block, the risk of adoption was simply too variable and therefore untenable but that didn't really matter; it was gathering such momentum, the security market simply couldn't keep up, so the easiest option was to get the big red stamp out and mark it 'unsafe' and hope it would go away.

The problem was it didn't, it just got bigger.

The only thing growing at the same rate as the popularity of Cloud was the size of the problem that it represented to the average IT Security team. As far as the business was concerned, Cloud was a thing of beauty; it represented opportunity for consolidation, cost reduction, Apps that embodied productivity and the attractive option to 'outsource' the whole kit and caboodle to a specialist provider. The world was moving on.

The IT Security guys were less happy and at one stage would have wilfully shoved the whole offering where the sun doesn't shine (which ironically is also just behind a really big cloud).

At the time their resistance stemmed from good reason. Much time had been spent going to great lengths to secure the growing issue of cyber attacks and potential data loss.

They had developed a trusted contained model of computing which was built on centralised managed assets where they could largely put their hands around the data and implement controls and processes to protect it. Then along came Cloud, the unprecedented rise of the App, its relentlessly annoying overuse of the word 'agile' and all bets were off.

Our once lifeless static PC's were quickly replaced by mobile devices; personal and work lives set up shop on the very same piece of kit and the demise and conversely liberation of the work life blurry balance was born. Brilliant news for productivity but it left the traditional world of cyber security that could be measured, evaluated and monitored shaken to the core by the very users it sought to protect.

Security designed for a pre-cloud market ceased to be relevant and it probably didn't feel very fair after all that hard work. The truth is though, you could stamp your feet all you like and protrude your bottom lip so that it is visible only from space but one thing was for certain; change was coming.

THE FLAW AS THEY SAY, IS ALL YOURS

Once the control had been surgically removed from its internal security custodians, a gap in the cloud(s) began to emerge. With Security no longer contained on premise and the use of the Apps gaining traction, the burden of responsibility for data was up for debate.

This left many businesses with an interesting quandary; You can after all outsource many functions associated with technology but the responsibility of your data simply isn't one of them. Security was no longer a conversation centred only round technological advance; it was also becoming a procured contractual engagement and a legal minefield.

App providers today are a formidable disruptive force and demonstrably vary in their attitudes to Security from the well intending to the sales-hungry consumerised provider who on the surface appears entirely uninterested.

If we're to play devils advocate, it was always going to happen. Cloud Apps are generic by definition; they are created to service a mass market and the by-product is that security considerations are broad and lack granularity.

As the understanding of Cloud has matured, progressive businesses have begun to intentionally adopt Enterprise Apps that suit the needs of their business but still rely on security products designed to protect a market from a different time with very different challenges. That's pretty bad news and it gets much, much worse.

Users (and when we say users, we don't mean the hapless lemmings portrayed in scare-mongering security marketing; we mean, even the well informed, good intentioned employees) will elect to use Apps that they personally favour, all in the valiant name of productivity.

It's a practice that has evolved from the BYOD culture and it looks like it's here to stay for the foreseeable future. Which means you either find a way to secure your users and enable them to work productively or face the fact that one day soon, you'll find yourself up a well known messy creak without a paddle.

Security has a new role to play and that is to simply adapt or cease to be relevant.

I'LL 'DROPBOX' YOU ...

The second an App becomes a verb it's time to become concerned, we learned that the hard way when 'Facebooking' shoe-horned its way into our lives and destroyed the English language.

Popularity of a brand has a way of making us feel assured. Worryingly, it seems to be that if an App is commonly used and known in the business world then it's assumed that somebody (probably a grown up with letters after their job title) has checked that it's safe to use.

Part of the reason the growth of Cloud Apps has posed such an open ended issue for traditional Web Security 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.

Here's a topical example, a well-intentioned busy user decides that they need to share data, let's say an export of 1500 customer records with a client for some legitimate business reason and there are many. Email isn't cutting it (and frankly often isn't all that secure anyway) so they connect to Dropbox, Box, WeTransfer (or any number of the file transfer providers) and up-load the file, safe in the knowledge they've done their job. What could possibly go wrong, everyone uses it; it'll be fine.

Then quicker than you can say 'Information Commissioners Officer', your sensitive data has been placed on a third party providers infrastructure protected only by an End User License Agreement (EULA) that the user agreed to. If you read the small print, you'll often find the words "we take no responsibility" in there for good measure.

Frequently these services have exceptionally poor security models favouring open sharing and can be almost impossible to revoke data once it has been uploaded. Vulnerabilities can also be a significant issue depending on their choice of software... which is also something that you can't control.

THE LONG ARM OF THE DIGITAL LAW

Data protection regulations started local but now they're mutating, have large teeth and have become well practised in dishing out fines with numbers that you'd have difficulty fitting onto a National Lottery Cheque.

The UK is already demonstrating its seriousness in prosecuting lapse attitudes to data loss but there are also new powers coming that will be consistent across Europe which drive mandatory breach disclosure and even bigger potential fines - up to 5% of global turnover or 100M euros (whichever is bigger).

A legal viewpoint: Now here's the thing, if one of your users elects to upload data to a cloud service, without any control over where it's going to finally end up and where it goes on the way there; you are running the risk of violating your country's laws on data export. You've got to be sure where your data is actually kept and processed. The cloud ecosystem does not recognise international legal borders or jurisdictions. Your user may not have done this knowingly but you'll still be liable. Their intention is irrelevant but your lack of control is.

Furthermore, different countries will handle/access your data, your intellectual property, your PII in different ways. The US Patriot Act has one type of reach in accessing your data, in the UK the Regulation of Investigatory Powers Act 2000 another. Choices have to be made about where your data goes and stays.

In short, this is already a legal minefield that continues to grow in size and danger exponentially. The yawning gap between the standard technical implementation of Cloud technology and the compliancy needs of the developing legal and business culture is dangerous. There are mitigating privacy enhancing technologies that can deal with such issues but many organisations have failed to recognise or implement them.*

* Dr Bandey, UK expert on International IP, IT, Cloud, Internet, Big Data and e-Safety Law

LET'S NOT PRETEND CLOUD SECURITY ISSUES ARE STILL UNKNOWN

Apps aren't a new piece of technology and we're well past the stage that we can say we're still figuring out the best way to secure them. We're not sucking and seeing; nor are we dancing around our handbags, kicking tyres or easing into what we should be doing; there are real ways to tackle known issues head on.

It is incumbent on every organisation to evaluate the use of services and insure they have effective controls to help their employees do the right thing; embrace cloud services but avoid exposing the company.

This doesn't begin and end with popular unregulated apps, this extends to services that have been transformed into business facing apps to keep the wheels turning, such as CRM systems, Enterprise Social Media, File Sharing or even Virtual Infrastructure given the increasing IaaS and PaaS trend.

Ignore them at your peril because these platforms although marketed as business ready tools are assumed to have robust security from the get go. Unfortunately adoption of these services very often (though not always - some providers do a better job than the average business) degrades security or at least makes the issue uncertain.

The developing trend of Shadow IT and the evolution of the savvy user outgrowing the IT department means Cloud services can in principle be implemented without intervention with one swipe of a credit card and you're away.

That's part of the reason the App market is thriving at the rate that it is because it's simple and easy to use, the fulfilment if you will of the carrot dangled for many years by the technology evangelists.

In many ways the Cloud presents the opportunity for higher quality secure services. A large CRM specialist is likely to be able to invest significantly more in technology and skilled people to protect their infrastructure than the average business but that shouldn't stop us from addressing the obvious.

Large Cloud services or popular Apps also make large, sexy and interesting targets where extremely large volumes of valuable data could be obtained or misplaced- far more than the average business.

These are risks that we all know about Cloud that haven't been meaningfully addressed to take into account the growth of Shadow IT and the sporadic use of Apps on personal mobile devices used in a business context.

The answer however isn't to slam the brakes on because if we do, we prove that we have learned nothing. The answer lies in the ability to sensibly manage, analyse and control access to Cloud Applications, apply risk mitigation through policy and help employees avoid circumventing necessary business controls to get the job done.

WHAT 'CLOUD APPLICATION SECURITY' BRINGS TO THE TABLE

If we're to learn anything from the dynamic popularity of the App world, it is that innovation and forward motion inspires, captures imagination and makes all things possible. That requires a departure from conventional thinking for the Security market but it's also a long overdue kick up the butt for those that seek to prohibit progress.

The trick is to lead, to anticipate what success looks like and not chase the problem with solutions long after the brown stuff has left the donkey. The role of CAS doesn't just fix an issue, at its absolute core it enables and protects.

By 2020, 85% of large enterprises will be using CASB/CAS, which is up from less than 5% today (Gartner, Market Guide for CASB)

Gartner 's prediction is well founded and talks openly about the need for Security to extend beyond the web gateway and address the gap that resides between traditional web filtering and the need to secure the way in which we use Apps in today's market.

They believe the continued & growing significance of SaaS, combined with persistent concerns about security, privacy & compliance, continues to increase the urgency for control & visibility of cloud services.

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 Security:

- Start with getting visibility into the use of cloud-based services and the potential risk they represent.
- Rather than requiring the purchase of yet another security gateway device, query existing SWG and identityfederation gateway providers to determine whether they offer the needed CASB capabilities.
- Evaluate broader cloud services brokerage 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 CASB solutions that are capable of delivering the same type of policy enforcement without requiring all traffic to be routed through an on-premises appliances.

NO MORE SCARY STORIES PLEASE, WE'VE HEARD THEM ALL

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 CAS.

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.

YOU CAN'T PROTECT YESTERDAY

As CAS evolves you can sense the growing nervousness among the traditional Web Security vendors and with good reason. Many of the world's biggest most trusted brands, particularly in the Web Security and Content Filtering world have barely changed or improved their market offering in recent years.

The issue is that many of them designed their software prior to the explosion of the App and their products and approach has been on the ropes for some time now. Unfortunately for them, the rise of the CAS or CASB market is beginning to shine a bright unflinching light on where those gaps lie to the extent that having the word 'security' in their title is even starting to look a little bit awkward.

We also need to be mindful however of the bandwagon entering from stage left. Since Gartner weighed into the debate, there has been a clear emergence of CAS/CASB entering into the market, all heralding the badge of a specialist. That's good; it solves a genuine gap in the market however they need to stand up to the same scrutiny that the established players face.

If they can prove they have experience in leading Web Security and Content Filtering capability and can demonstrate they can bridge the gap to effectively deliver CAS as part of the web security functionality in a meaningful, measurable way, then they're a keeper and you should offer them the posh biscuits when they arrive.

CONCLUSION – WHY CAS/CASB PROVIDERS WILL RULE THE WORLD

Once upon a time, not that long ago, we sought to protect the Internet and Cloud was the beast that was yet to be tamed but times have undoubtedly changed. One-dimensional security lacks the flexibility demanded by the market it seeks to serve. Today, it has a new directive, to liberate and enable users to do their jobs safe in the knowledge that they're protected but not prohibited.

As organisations begin to ask the questions that CAS can answer, you're likely see a natural attrition of the well-known Web Security and Content Filtering vendors. Many of their products were designed to service and protect the digital world from web-borne malware some 15 years ago and the market has become wise to the repackaging of the same solutions brandishing a rehashed strapline and positioned as something new, again.

An organisation seeking a CAS vendor will soon realise that specialism is scarce. There is an emergence of new providers, purely aimed at the CAS market, but the issue is they seldom have the tenure or history that stem from the learning's gleaned from the complexities of the Web Security and Content Filtering progression.

Vendors that 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 will be a formidable force by anyone's measure. We know this because we've done our homework.

CAS at the top of its game should truly 'follow the user' and their behaviour. It should encourage the use of Cloud Apps and services while keeping company assets safe. It should have the depth to be able to analyse the risk, audit and log all usage, maximising visibility at the time that an issue occurs, not act as a forensics tool, that points out the obvious long after it's all gone horribly wrong.

The market has been calling for a service that runs in the Cloud responsible for aspects like authentication, policy enforcement and reporting. Add into that 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 and you have a heavyweight contender with a lightweight footprint which is long overdue.

It's also been proven that if you try to use a new security product so prohibitive that it increases latency, prepare yourself to be about as popular as Jeremy Clarkson at a BBC diplomacy briefing. A lightweight protocol that works without the need to 'proxy' the web content to centralised servers will equal happy secure users.

As an industry we're in the privileged position of redefining our place digital history; our role isn't to block or deny but to enable and protect. Hiding behind the clichéd stance that Cloud Security contains too many unknown risks smacks as a weak transparent excuse for products that haven't evolved to address and protect the exponential rise of the app.

By denying users the option to use the Apps that encourage them to be productive, we fail to recognise the huge leaps we have made as an industry in keeping the Internet a safe place to be. The Cloud isn't the enemy; it never has been.

CAS has the opportunity to bring forward an era of specialism within the Web Security market that both organisations trust and users frankly don't notice. Productive and easy to use Apps have gone from strength to strength and the reasons are simple. Their ancestors were big and clumsy and they have evolved by departing from conventional thinking by producing extraordinary solutions.

Much can be learned from what users love about Cloud Apps. They're cool, easy to use, encourage productivity and they make all that use them happy and in control. These aren't characteristics normally associated with protection and that's probably why Cloud and Security never looked like a natural match; that is until now.

Web Security has lost its slippers but incorporating CAS capability as part of the web security functionality will help organisations realise all that it can bring. Vendors providing CAS functionality will one day rule the world; not by taming the Cloud App market but by embracing and securely enabling all that has made it successful.

That's probably all that the Cloud wanted from a partner in the first place and let's face it, more diverse marriages have gone the distance.

CENSORNET | POWERFUL, ENTERPRISE-CLASS CLOUD SECURITY FOR YOUR ORGANISATION

UNIFIED SECURITY SERVICE (USS)

360° Protection for your IT Systems

CensorNet USS provides visibility across vital security points within the business and maximum insight and control through one viewpoint.

CLOUD APPLICATION SECURITY (CAS OR CASB)

CensorNet's Cloud Application Security helps businesses gain visibility inside all cloud applications see uploads, usage, and suspicious activity and set appropriate controls.

WEB SECURITY

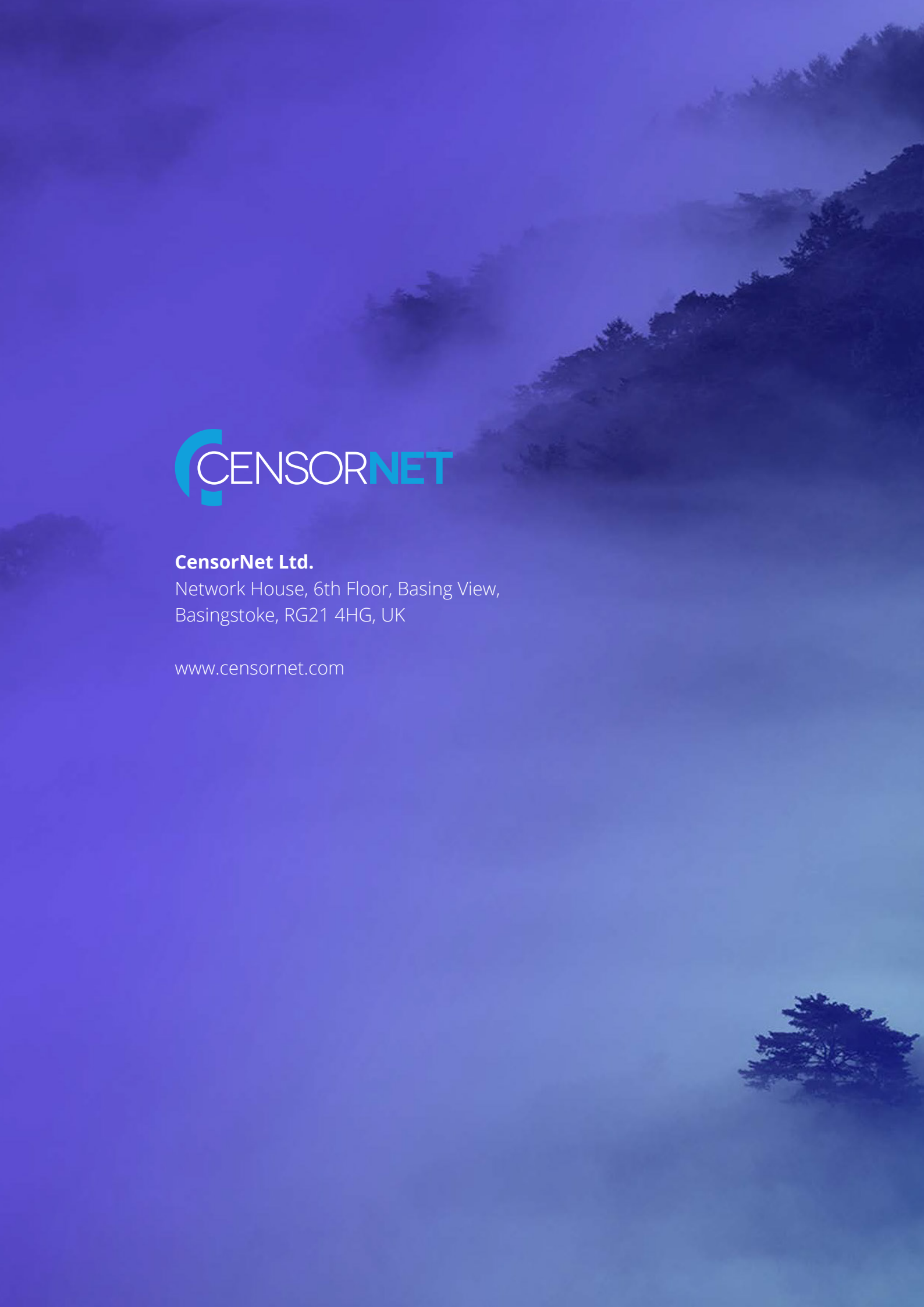
CensorNet's Web Security provides complete security policy protection seamlessly for the entire workforce inclusive of any device.

EMAIL SECURITY

CensorNet Email Security is a cloud based email security and backup service that scans both inbound and outbound email for viruses, phishing threats, content violations and spam.

MULTI-FACTOR AUTHENTICATION

CensorNet's Multi-Fator Authentication is adaptive and user-centric authentication using contextual intelligence to ensure highly secure user authentication.



CensorNet Ltd.
Network House, 6th Floor, Basing View,
Basingstoke, RG21 4HG, UK

www.censornet.com