KONC!SE SOLUT!ONS
THE CLOUD. SIMPLIFIED.

mimecast®

BETTER PROTECTION. LESS TOOLS.

7 BENEFITS OF SECURITY CONSOLIDATION.

OPINION PAPER: SECURITY

SO MANY THREATS, SO LITTLE TIME

Cyber security is a truly never-ending battle. As fast as IT teams work to protect themselves, cyber criminals devise new and increasingly sophisticated ways to exploit weaknesses they don't even know about yet.

CISOs globally are fighting to protect their organisations' Intellectual Property and their employees whilst managing IT teams with constrained budgets, limited time and stretched resources.

At a time when the skills shortage in the cyber security industry continues to grow, expert manpower to manage protection is proving hard to come by. According to the UK Government, 30% of businesses[1] have skills gaps in advanced areas such as pen-testing and security architecture, leaving less time to tackle the security jobs that are theoretically easier, but are every bit as pressing and potentially damaging.

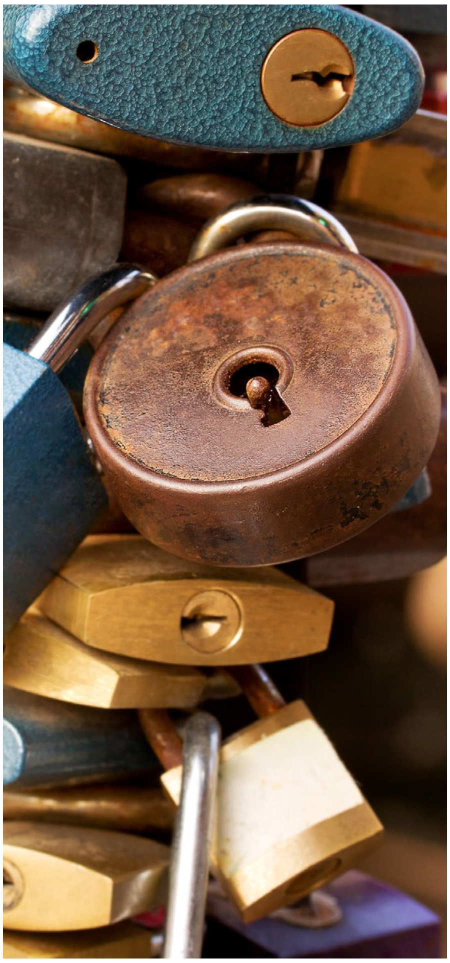
'BEST OF BREED' DOESN'T MEAN BEST SECURITY POSTURE

Security provisioning can feel like an exasperating cycle of knee-jerk reactions:

A new threat evolves. You've got to protect yourself. A host of new tools pop up to combat it. Endeavouring to offer the best defence, your team seeks out the 'best of breed' solution. Budget is found to deploy it. The next new threat evolves. You repeat the process.

While this secures you against each individual new threat, it doesn't necessarily mean that your overall security posture is getting any stronger. In fact, we've found that in many cases, more tools can lead to more problems, more notifications and leave ingress points vulnerable.
With so many tools shouting for your attention, it's easy to misread a tool, miss an important notification or fall for a false positive because of conflicting information across tools. Despite conventional wisdom, Koncise Solutions believe there's a strong case that a cleaner environment can be simpler, more secure and easier to manage.

THE AVERAGE ENTERPRISE BUSINESS HAS 75 SECURITY TOOLS DEPLOYED RIGHT NOW[2]



THE KEY IS KNOWING WHERE TO START

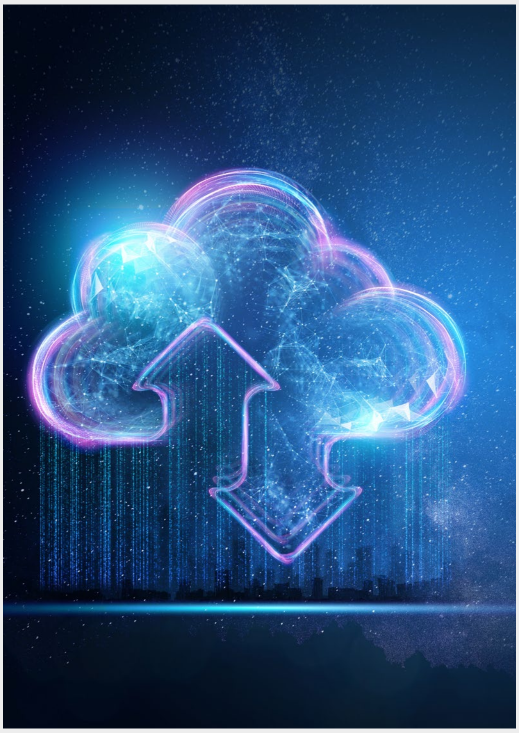
The Center for Internet Security (CIS) identify a list of 20 Critical Controls[3] that are fundamental to creating a secure IT architecture. Number 7 on that list is Email and Web Browser Protections. In context, these measures are the next step beyond basic protections like anti-virus. The reason? Because they are the two most attacked vectors you need to defend. Despite the massive array of measures to secure these fronts, 94% of malware is still delivered via email[4] and in 2019, web applications were involved in 43% of breaches[5].

94% OF MALWARE IS STILL DELIVERED VIA EMAIL[4]

Accordingly, securing email and web should be considered fundamental protection for every organisation. Inadequate protection will leave you hugely vulnerable.

However, your users are the gatekeepers to these domains, and 'human error' is often the difference-maker for a successful exploit. As attacks become smarter and leverage social engineering, they also become more difficult to spot. Even the most conscientious of employees can slip up. One wrong link clicked, or one dodgy attachment downloaded can lead to financial, reputational or operational catastrophe.

With email, web and human error being so closely interlinked, a united approach to defending them can result in increased security coverage, rather than less, frequently saving budget for use on other projects or to further enhance protection.



WHAT ABOUT GOING SINGLE VENDOR?

Traditionally, going single vendor has been perceived as making a compromise on certain security measures. IT teams naturally want the best they can afford and philosophically believe choosing a combination of leaders is the right way forward. While this can be true, as already discussed, it comes at a price.

Perhaps controversially, we believe that with security technology now being so advanced, the trade-offs in capability are minimal and are outweighed significantly by the benefits.

To make this approach work, vendor selection is critical to maximise protection, simplify operations and properly consolidate cost.

If you pick your single vendor carefully, these are the benefits you stand to gain:

7 WAYS GOING SINGLE VENDOR CAN BOOST YOUR DEFENCES:

REASON 01

MANAGEABILITY

Bringing email, web and security training under one roof can help to claw back some highly coveted management time, as your IT team has fewer inter-application integrations to handle. With defences seamlessly knitted together, their interdependencies are automatically configured for success, with little intervention needed from your team. With one vendor spanning all three areas, you can gain greater control over a wider portion of your security posture in one swoop.

It's impossible for IT teams to skill-up comprehensively on the ins and outs of every single one of their tools, so teams frequently specialise in a core few, and just maintain a working knowledge of the majority. With just one vendor's controls and processes to learn, IT teams can gain a deeper understanding of their solution and therefore get the most value out of it. As we've already mentioned, finding and recruiting skilled people is tough enough at the moment, so cutting back on your vendors also simplifies the list of skills required from any new recruits.

Less vendors also means less relationships to manage. Email and web security require such comprehensive coverage, and protecting your people is so vital, that having just one vendor to liaise with means your IT team can spend less time managing maintenance tasks such as license renewals, and more time securing your network.

REASON 02

COST CONSOLIDATION

By consolidating your security vendors for these key areas into one single provider, you'll not only consolidate your costs, but also simplify the lives of the finance department – both in terms of front-end procurement and back-end reporting. With one single vendor, accounts and IT teams will have increased visibility into how much money is being spent on key pillars of security.

Going single vendor achieves comparable levels of protection to your existing combination of solutions, sometimes even more, whilst liberating budget to be better spent elsewhere. Whether that's investment in extending your protection even further, or on better security training for your employees, that's a big plus in our book.

REASON 03

DECREASED MEAN-TIME-TO-REMEDIATE (MTTR)

In a perfect world, security incidents would never occur, but if that were the case then you wouldn't be reading this, right? In the event that something does go wrong, a timely response can be make or break and certainly dictates the potential fallout.

Identifying incidents becomes a much more straight-forward process when you're operating fewer monitoring tools. When an event occurs, it's likely that several security tools will alert you to danger as it starts to affect them. The result of this is likely to be a barrage of noisy notifications which collectively make it tougher to navigate to the root of the problem. Having one version of the truth makes the path to resolution both clearer and quicker. With one vendor protecting your major security bases, you also can gain clearer insight into how an incident is impacting your entire security posture, rather than a collection of narrow views from point solutions.

The same goes for when you need support. With a single vendor approach, you have just one number to ring for all the help that you need, rather than being bounced from vendor to vendor to identify the cause without really knowing whose support you need most.

REASON 04

BETTER CONFIGURED TOOLS

With every new threat comes pressure to respond rapidly and protect your assets accordingly. In the rush to roll-out new ‘best of breed’ tools, configuration tweaks that help them integrate fully with the rest of your estate are often missed. With fewer tools to deploy, and therefore more time on your hands, solution configurations can be better managed to maximise the value you get from your investments. By thoroughly configuring a smaller number of tools for success, you can reduce the volume of workflows occurring and their complexity, which improves alert accuracy and safeguards the time of stretched IT teams.

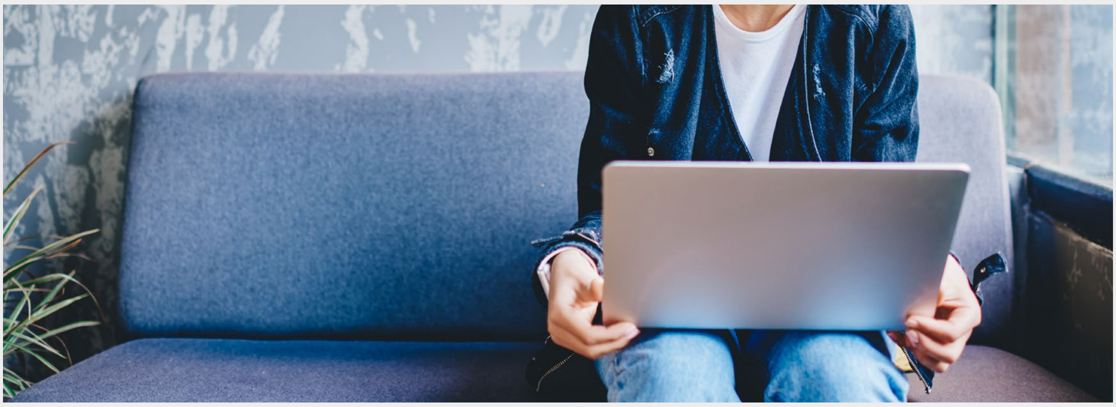
A single vendor approach also allows more time to learn the intricacies of a tool and check that you aren’t paying for functions you don’t need. ‘Silver bullet’ tools regularly hold additional functions outside of their primary role that go untapped because they duplicate the roles of existing tools or are just too complex to realise the benefit from. That seems like an avoidable waste of money to us. Reducing the number of tools in your stack ensures that each one is optimised and unlocks trapped cash that you can reinvest in more comprehensive coverage or other more pressing projects.

REASON 05

BETTER, MORE SECURE REMOTE WORKING

It’s safe to say that most businesses’ foreseeable futures will include remote working in some capacity. As many organisations have regrettably discovered, dispersed workforces create increased susceptibility to threats. Hackers are well aware of the abundance of opportunities for manipulation and are ramping up their efforts in response. Both email and web are inundated by more attacks than ever before, demanding increased employee vigilance at the exact moment they’re distracted the most. In a remote working environment (especially for those not used to it) employee concentration levels inevitably take a hit from interruptions by kids, pets and the Amazon delivery driver. And yet, one momentary lapse in concentration can lead to a dodgy domain being visited or important credentials being shared.

Heightened threat levels demand businesses have more checks in place, but more checks doesn’t have to mean more tools. With the right combination of technology, networks are better equipped to tackle the increased dangers that come from having dispersed workforces. Having a single vendor for three of the most exploited breach points means that you can confidently secure your users as they work from home.



REASON 06

REDUCED ATTACK SURFACE

Ok, this is a big one, so we're going to say it loud and clear: the fewer ingress points you have, the easier it is to defend your network, and the harder it is for hackers to penetrate it. In our experience, the irony is that the more protection tools you have, the more chance there will be that a door is left ajar to those who want to do you harm. The very tools that are there to protect you can become a weakness, offering a false sense of security.

Equally, reducing the number of tools in your architecture will make your life much easier in a crisis scenario. If your defences are breached, then the more complex your architecture is, the harder it will be to obtain a trustworthy analysis of the attack and stall its effects on your wider network. Not only do IT teams have less places to look, but breaches have less places to hide.

REASON 07

SPEEDIER UPDATES

With one simple update to apply across your most important security endpoints, there's an awful lot less finetuning to be done, reducing the roll-out time dramatically. When new updates and features are released, you'll feel the benefit much quicker if they easily integrate with your existing solutions.

Patch day can be a trepidatious one as you try to work out what the effects will be on your wider environment. With one vendor, the potential ripple effect of security patches is far more contained, as you know that your three most important tools will go unaffected. With more time freed up to iron out issues with other tools, the whole patching process can be made quicker and more secure.

ALL THIS, WITH LESS MANPOWER

It’s no secret that security eats up a good portion of IT teams’ budgets, and so does employing the right people to handle it. At the bare minimum, security professionals need to coax all their best of breed solutions into doing the right thing, interpret the data output, and monitor their ongoing performance. It takes a phenomenal amount of manpower just to manage them all.

Or does it?

What if the vendor chosen across your three most likely ingress points was a leader in its own right? Remember, we’re not trying to find best of breed in every nuance of protection, just these most important attack planes.

Koncise Solutions’ belief is that Mimecast’s world-class security solutions and widely-respected heritage in the market allow you to confidently consolidate your security vendors. You can lean on premium protection whilst offloading a bunch of the tough stuff thanks to technology that’s built to work together. With less manpower headaches to make security work, you can reallocate your resources elsewhere, allowing you to truly do more with less.

THE MIMECAST APPROACH TO SECURITY

Mimecast has a wide range of tools that work together to protect your data and defend the areas of your network that demand the most comprehensive protection:

EMAIL

- Detect and stop phishing attempts from entering your perimeter.
- Analyse and sandbox suspicious attachments and links.
- Prevent your email domain being spoofed to send out nasties to internal and external contacts.
- Set overarching security policies that enable your users to share information securely.

WEB

- Monitor and block user access to malicious sites and cloud apps that could cause harm in your network.
- Protect your employees and devices when they're on your network, and importantly when they aren't.
- Prevent ransomware attacks from taking hold by blocking outbound connections to command and control servers.

HUMAN ERROR

- Equip your employees with all the skills they need to spot security threats.
- Train them quickly and efficiently, so they can get on with their day jobs.
- A light-hearted approach to Awareness Training with a seriously memorable message.
- Use phishing tests to gain a clearer understanding of who your riskier users are and adjust their training accordingly.

INVALUABLE OF-THE-MINUTE INSIGHT

The ever-evolving threat landscape demands real-time visibility into how your environment is responding to security concerns as they arrive at your perimeter. This is where the potential for human error can rear its ugly head again. IT teams that are flooded with tools are likely to also be flooded with dashboards to help monitor them. With so many dashboards to digest and track, the potential for data misreads or misinterpretation increases.

Mimecast's Threat Intelligence Dashboard (TID) condenses a huge range of information into one easy-to-digest place. The dashboard gives you overarching live visibility of what's happening within and at your perimeter and gives actionable insight into how you can bolster your security to keep out the latest threats that lurk beyond it. While no means a SIEM solution, much of what TID achieves will be comparable to what many will have accomplished by taking this approach, but in a fraction of the time and cost. With a clear view of the most pressing threats you're up against, you can spend more time staying protected against them, and less time looking for them.

THE GROWING THREAT YOU CAN'T EVEN SEE

All security strategy is about staying ahead of the criminals. Something easier said than done. In the wild, as points of perimeter incursion are closed down, attackers are looking elsewhere for their pay-off. Unfortunately, where they're heading next will challenge protection measures more than ever and force businesses to look at security as something outside of the network.

THE RISE OF BRAND IMPERSONATION

Attacks on your brand can undermine your reputation and the effects can be more destructive and long-lasting than any other type of attack. Criminals are using brands as bait. By setting up lookalike domains and creating emails that resemble your own, criminals gain the trust of your customers, and can steal their credentials, data and money.

The most chilling part is that you might not even discover the attack has occurred until months later, and your customers are likely to be the ones informing you.

THE BEST DEFENCE IS A GOOD OFFENCE

Understanding if your brand is being misused online is outside the field of view for most organisations and the security measures they deploy. Those that have made the connection often spend substantial time and money both discovering attacks and attempting to litigate the perpetrators. Thankfully, Mimecast's Brand Exploit Protect (BEP) has upped the game significantly in how businesses can go about protecting their brands online, and is one of the most comprehensive reputation protection solutions we've seen at Koncise Solutions.

Importantly, BEP proactively goes beyond your traditional security to hunt out and take down attacks on your brand. It means impersonators are discovered faster and the repercussions of their actions minimised. In fact, with almost next to no manpower, Mimecast BEP can neutralise threats to your brand in a matter of hours.

By stopping your brand from being impersonated, you can prevent disruptions to your business and better protect your customers, partners and colleagues alike. Seamlessly integrating such an advanced solution with your email, web and human error protection strengthens your security posture enormously, allowing you to protect your property from attacks both within your perimeter, and beyond it.

WHY MIMECAST?

Mimecast is one of the world's biggest security vendors. They've got all the technology, the insight and the resources to quickly combat the newest and most dangerous threats, so that Mimecast users can feel the benefit.

85% of IT decision-makers believe that the volume of web or email spoofing they face this year will either increase or go unchanged. With threat levels in these core areas going anywhere but down, Mimecast has the solutions to help you protect what's important to you.

It's a bit like having the strongest, the cleverest and the quickest kids in the playground on your side when the trouble-makers come calling. Who wouldn't want that?

WHY KONCISE SOLUTIONS?

As Mimecast's Customer Excellence Partner of the year for both 2018 and 2019, we're experts in optimising Mimecast solutions to maximise commercial value for our customers.

Like any security measure, to get the best out of investment in Mimecast, the implementation is critical. With so many pressures on time, IT teams who go solo can get diverted away and may not see the process through. We eliminate this potential hurdle for our clients by ensuring every implementation is delivered by our Mimecast experts. Even better, in most cases this is a zero-cost implementation that not only helps your budget today, but accelerates the time-to-value from the solution for long-term payback.

At Koncise Solutions, we focus on using cloud-based tools to connect and protect businesses so that we can make the lives of IT teams easier, reduce overheads and minimise cost.

If you'd like to find out more about Mimecast, Koncise Solutions or going single vendor securely, get in touch:

info@koncisesolutions.com
+44 (0) 20 7078 0789

KONC!SE SOLUT!ONS
THE CLOUD. SIMPLIFIED.

mimecast®

SOURCES

[1] Cyber security skills in the UK labour market 2020, Department for Digital, Culture, Media & Sport (DCMS). [2] Cyber Resilience Think Tank, 2020. [3] Center for Internet Security: CIS Controls. [4] Gartner, 2020. [5] 2020 Data Breach Investigations Report, Verizon. [6] Mimecast State of Email Security Report 2020.