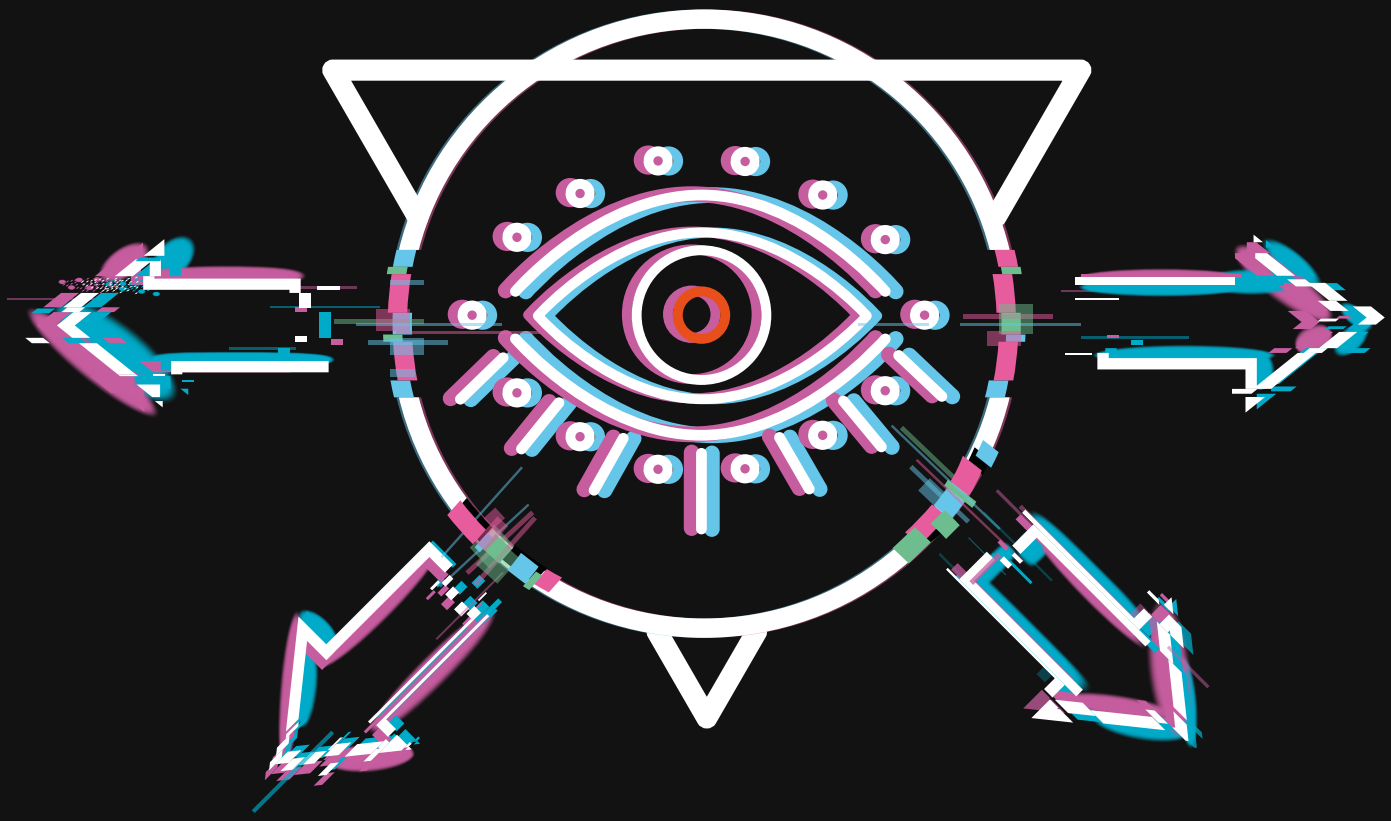
BAE SYSTEMS

Get a smarter managed security service with an intelligent detection and response approach



BAE Systems Applied Intelligence: Buyer's Guide

Intelligent detection and response

Think you can't have it both ways when it comes to managed security? Think again. Because you can now benefit from both supercharged detection and response capabilities and a robust partnership-led managed security approach.

Executive summary

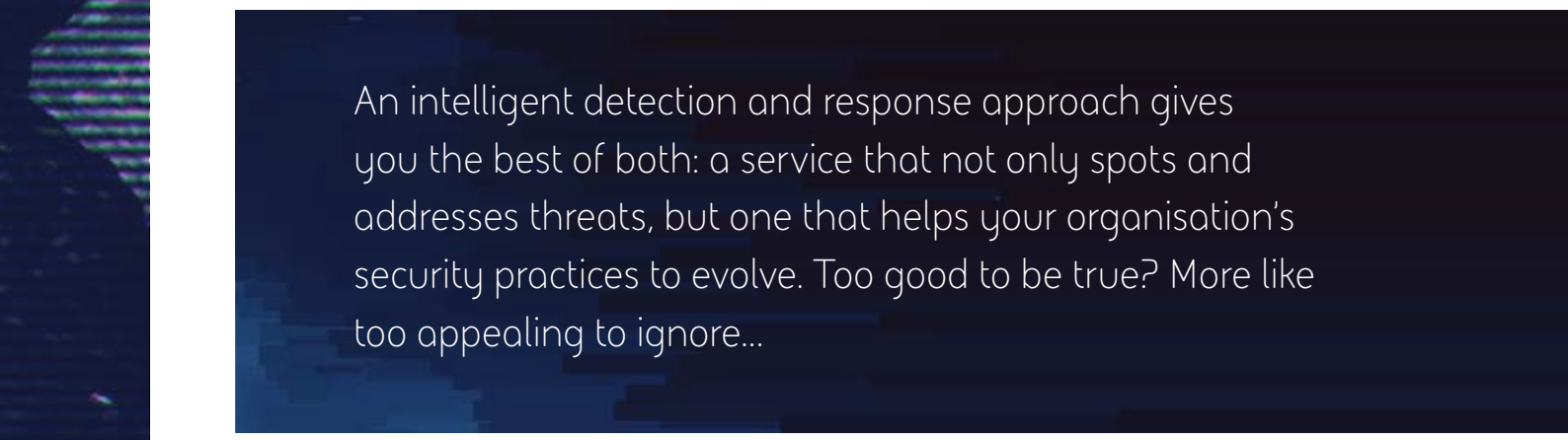
Threat detection and response is a balancing act. And like any balancing act, mastering stance is essential. For managed security service providers (MSSPs), that means being able to slip seamlessly between two stances – the reactive and the proactive – in order to deliver comprehensive, resilience-boosting security.

Those MSSPs who can find that balance are a rare breed. They're able to fend off multi-vector threats on the frontline while at the same time producing crucial intelligence that can be used to improve your security right here, right now. That's quite a challenge. But if your provider can walk that tightrope, you reach managed security nirvana. Or, as we refer to it, intelligent detection and response.

This guide outlines the characteristics that typify an intelligent approach to managed security provision. It explores the benefits you can experience by finding that all-important balance between robust detection and response, and actionable tailored security insights.

And (probably most useful of all) it'll help you to draw up your "must-have" list of requirements as you seek a transparent, comprehensive and tailored managed security service.

Find that all-important balance between robust detection and response, and actionable tailored security insights.



An intelligent detection and response approach gives you the best of both: a service that not only spots and addresses threats, but one that helps your organisation's security practices to evolve. Too good to be true? More like too appealing to ignore...

Shortcomings of the status quo

Poor old Managed Security Service Providers. They've come under a bit of pressure recently, for a number of reasons.

First, there's all that cynicism around their secretive black-box operating practices, with detection shrouded in mystery. And then, the more outdated MSSPs don't address advanced and novel threats. They often miss the type of nifty predators that regularly bypass controls, and they're guilty of allowing monitoring, incident response and dwell times to stagnate.

In response to the criticism directed at the humble MSSP, Managed Detection and Response (MDR) vendors have leapt into the spotlight – eager to flex their incident response muscles. Those sharp-suited MDR players arrive on the scene keen to tell you just how capable they are when it comes to addressing an MSSP's shortcomings.

They'll conveniently gloss over how little they do to improve your resilience. Sneaky. They might forget to mention how they often fail to prevent the same attacks from reoccurring by missing the key insights that would have helped your business to evolve over time. They'd much rather you patted them on the back for everything they've detected (and looked past the fact they haven't actually explained how it was detected). Similarly, they'll focus on advanced threats, and not those rather mundane (but no less important) day-to-day routine attacks.

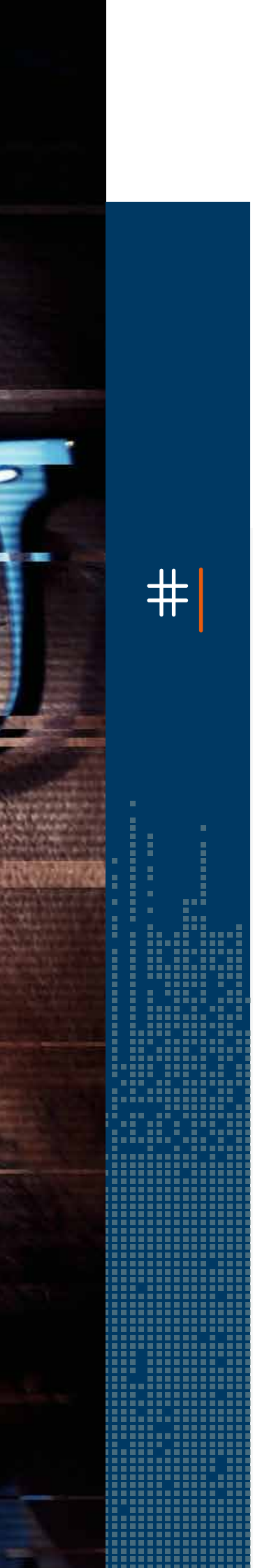
In this climate of compromise, businesses just can't seem to find what they really need. A complete managed security solution – one that marries the robust outsourced model of an MSSP with the leading-edge detection and response capabilities of an MDR. And then layers on insight-fuelled resilience-boosting capabilities.

An intelligent alternative

Good news, then, that the solution to those demands is actually already here. And it's called **intelligent detection and response.**

This approach stacks consummate detection and response capability atop a supercharged security insights engine – which generates information tailored specifically for your organisation. If that sounds like a distant security utopia, don't worry – it's not. This intelligent approach is not only possible in the here and now, it's also straightforward and can return immediate benefits – provided you find the right partner.

So, here are the five qualities your managed security partner needs if they're to deliver an intelligent detection and response service.



Threat detection expertise

Start with a prospective vendor's threat detection capability. If they're worth your consideration, a potential supplier will be able to prove their track record and showcase their threat detection nous – including how they work, and why that's the right approach for you.

Truly intelligent detection and response demands a partnership between advanced AI and the very best human insight and lateral thinking. That's exactly what we offer our clients – a team of threat-hunting experts working with the best machine-learning tools. This provides the optimum threat-detection balance, enabling us to better understand (and derive insights around) threat patterns.

Over and above that marriage between AI and real human expertise, an intelligent security services vendor will also be able to demonstrate a flawless performance when it comes to gathering data across all vectors – email, infrastructure, endpoint and network devices. They'll be able to use that intelligence to provide a consummate incident response service and conduct thorough penetration testing. And their overall aim will be to improve your resilience by employing a MITRE-aware approach to known Tactics, Techniques and Procedures (TTPs).

Intelligent attackers use **crafty custom methods to evade detection,** lying in wait for long periods, or iterating and attempting more and more advanced repeat attacks.

#2

Proven resilience pedigree

Speaking of resilience, that should be next on your shopping list. Providers who can address this element will help to prevent repeat or similar attacks from occurring (and disrupting your business).

The old school approach to managed security services was to detect previously seen attacks by sending you a mountain of alerts and if lucky a notification on a portal. Intelligent attackers don't rely on templates for known attacks, they use novel methods to evade detection, lying in wait or living off the land for long periods, or iterating and attempting more and more advanced repeat attacks. They use crafty custom methods to evade detection, as they probe and test, gain control and complete their objectives. That's why intelligent detection and response services are one step ahead – with an astute approach that builds sophisticated resilience from the new data they gather.

Intelligent detection and response actually requires an extremely broad set of data to create a baseline for your organisation. But as soon as you get that in place, you can build advanced behavioural detection analytics to identify anomalies. The key here is to combine this analysis with context – further data from sources such as HR, finance and TTP intelligence.

That's the precise approach we follow, in fact. And it's the reason we're able to detect (and respond to) a wide array of known, modified and brand-new attack techniques.

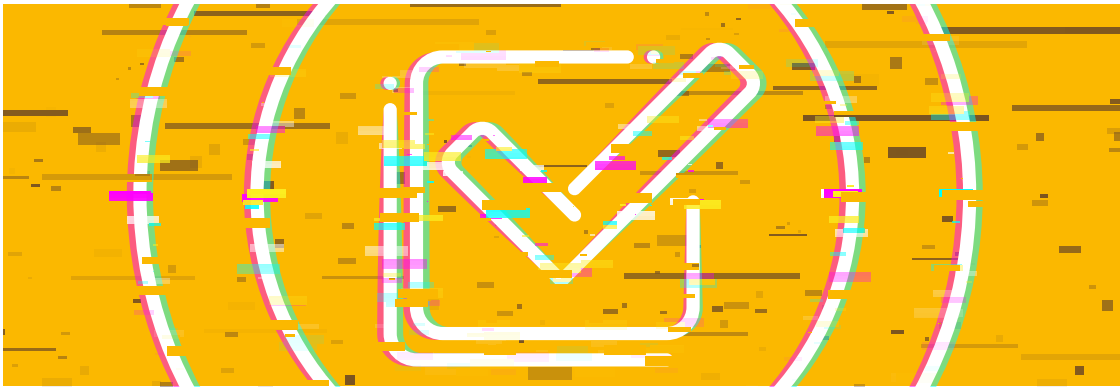
#3

Product and offering breadth

Intelligent detection and response is more than just a managed service. It requires vendors to bring their own tools to the party and maintain a comprehensive product range too. True – the core element is still a robust, tailored managed security service, but that needs to be allied with patented IP – such as high-performing endpoint technology. In fact, a recent Forrester report specifically namechecks just that.

Ask your vendor about their own endpoint technology, and what that means when it comes to their MSSP credentials. What you should expect them to tell you is that, firstly, this best-of-both, product-and-service offering ensures you (their customer) benefit from the most vigilant detection of unknown and non-malware-based threats. Ideally, they'd then go on to explain how their endpoint technology also ensures compatibility and integration with your existing technology stack.

We're proud of our IP estate, which features **Host Agent** – a leading endpoint monitoring and investigation tool – as well as other proprietary (and widely compatible) technology. By investing in our product suite, we're able to realise our vision of tailored, resilience-boosting intelligent detection and response services.



#4

Operational transparency

The true value of a security provider can often be felt not only in what they do, but why (and how) they do it. And, to make sense of that, you need to ensure your vendor gives you full transparency.

Intelligent detection and response requires a high-visibility reporting approach, and comprehensive remediation detail as standard. In practice, this means your vendor can show you how they've rectified security vulnerabilities. They'll actively break down threat analysis and then build it up into intelligence that means something to your business – providing even more clarity and helping you to prevent similar attacks in the future.

Providers with full-scale forensic capability leap ahead of the chasing pack here – offering the type of exacting detail and analysis that can supercharge your resilience.

At BAE Systems, we insist on robust reporting, in close partnership with our customers. This allows us to commit to (and stay on top of) SLAs, and also derive those all-important resilience-driving insights. We've even had our full-scale forensic capabilities praised by Forrester. And that means we're confident we can offer consummate, market-leading and resilience-boosting transparency.

#5

Security providers who offer a **tailored, made-to-measure service** will ultimately prove to be a more effective and trustworthy partner for your business.

A partnership you can **trust**

The final piece in the puzzle is probably the most valuable to your overall security. And that's the investment a prospective vendor is willing to make in order to provide the right, customised solution for you. Security providers who offer this type of tailored, made-to-measure service will ultimately prove to be a more effective and trustworthy partner for your business.

Seek out a vendor with specialised capabilities based on your sector, location, or technology stack. Vendors who are willing to go the extra mile – embedding themselves into your organisation, understanding how you operate and aligning accordingly – will be able to deliver a more intelligent detection and response solution.

A bespoke security service requires your vendor to understand how your organisation operates. This means they'll be better educated on the types of threat you may be exposed to. And crucially, finding a partner who works around you means you can rest assured they'll be providing the best (and most relevant) security service possible.

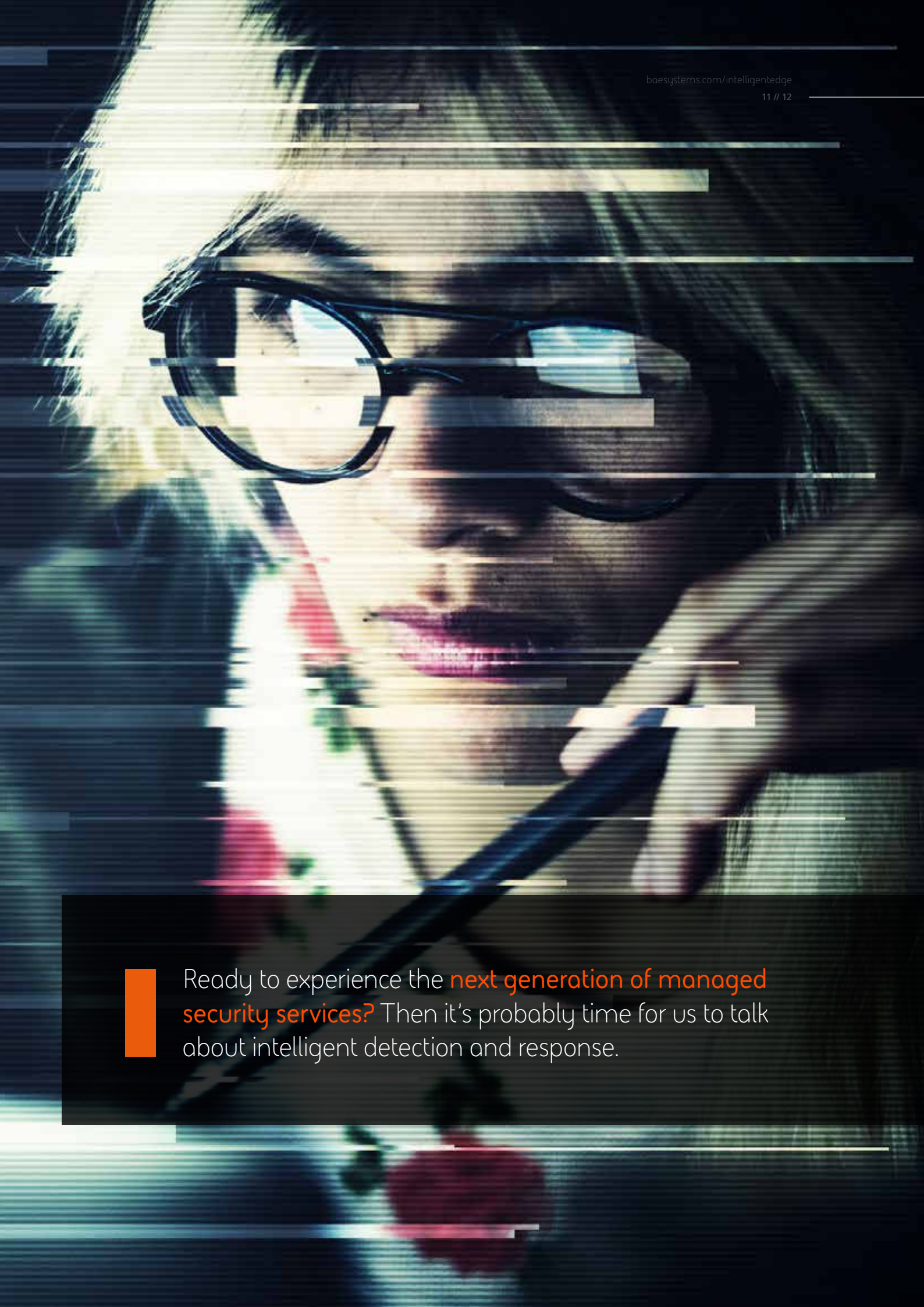
Intelligent detection and response means big benefits

Find the right managed security partner, and you'll experience much more than just best-practice box ticking or SLA observance.

You'll see a genuine return on your business investment, with your ability to detect and respond to advanced cyber threats continually improving. And that means reassuring peace of mind.

The benefits of intelligent detection and response include:

- Reduced business risk, as threats are detected and addressed faster.
- Industry-leading technical know-how and security expertise on tap.
- Confidence that your security services are constantly evolving and actively seeking to address emerging threats.
- A versatile solution that adapts and scales according to your specific requirements.
- Full visibility over how intelligence is handled, and what the outcomes are.
- Resilience-driving remediation detail and actionable security recommendations.



Ready to experience the next generation of managed security services? Then it's probably time for us to talk about intelligent detection and response.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/intelligentedge

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai