VECTRA®
SECURITY THAT THINKS

RESEARCH STUDY

Fit for Purpose or Behind the Curve?

Uncovering how today's organisations are tackling complex, modern cyberthreats

VECTRA
SECURITY THAT THINKS

Table of Contents

Executive summary

The genie is out of the bottle. Experts believe that during the course of 2020, many companies were pushed over a "technology tipping point" which accelerated digitisation by several years. Businesses will be forever changed for the better. But there's also bad news. The same digital transformation that is powering innovation is also expanding the attack surface. From the rapid proliferation of cloud to the growing adoption of microservices, DevOps, and APIs, new pockets of opportunity are opening up for threat actors to take advantage of. And they're doing so like never before.

> The same digital transformation that is powering innovation is also expanding the attack surface.

Hijacked Microsoft 365 accounts are now the largest single security threat vector in the cloud, with a 98% rise in compromised credentials between 2018-2020. There are multiple blind spots in cloud infrastructure environments – which are often misconfigured – that offer even more opportunities for threat actors. What's more, ransomware surged by 150% year-on-year in 2020, with average extortion amounts doubling. In the UK, nearly two-thirds of medium and large businesses admitted earlier this year that they'd suffered a breach during the previous 12 months.

This matters because breaches have the potential to cause widespread damage. They can disrupt operations, damage supply chains, destroy customer trust and open companies to regulatory fines. And cyberattacks cost big money today: an estimated $4.2m (£3m) on average per incident, in fact. Ransomware attacks that result in stolen data and lengthy operational outages can end up costing many times that. Some companies have reported losses in the tens of millions of pounds. It's no surprise that cybersecurity is now a board level issue.

Unfortunately for CISOs, the old ways of defending are no longer as effective. Whether it's through system exploitation, phishing, using stolen accounts, or bypassing multi-factor authentication (MFA), there's always a way in. And once inside, they're masters at staying hidden. Cybercriminals are constantly innovating, so cybersecurity has to constantly evolve to keep up.

To find out more about how security leaders are tackling these dynamic threats, Vectra commissioned Sapio Research to interview 200 IT security decision makers working at organisations with more than 1,000 employees.

> Ransomware attacks that result in stolen data and lengthy operational outages can end up costing many times more than the estimated $4.2m (£3m).

VECTRA
SECURITY THAT THINKS

In this report we will reveal that:

- **It's time to change the game when it comes to dealing with attackers.** The security industry is failing to keep pace with cybercrime tactics, techniques and procedures (TTPs), making it harder than ever to protect against modern threats.
- **Legacy 'prevention-first' thinking puts organisations at risk.** Legacy tooling and thinking is an impediment in the new threat landscape. Yet many continue to over-invest in doomed prevention strategies that fail silently and leave them open to being breached.
- **Security leaders must educate the board.** The board is waking up to the risks posed by cyber-attacks, but they are not the experts. Security leaders need to find more effective ways to communicate risk and educate on how best to mitigate such risks.
- **Regulators need a better understanding of life on the front lines.** Greater industry involvement and experience could help to make regulation more effective, but ultimately a hacker mindset, and rapid detection and response, give you the best chance.

Key stats:

89% think traditional approaches don't protect against modern threats and that we need to change the game when it comes to dealing with attackers

76% of security decision makers have bought tools that failed to live up to their promise – citing poor integration, failure to detect modern attacks, and lack of visibility as reasons

69% think they may have been breached and don't know about it—a third (31%) think this is "likely"

90% of respondents say recent high-profile attacks have meant the board is starting to take proper notice of cybersecurity

82% say the board's security decisions are influenced by existing relationships with legacy security and IT vendors

"

Digital transformation is driving change at an ever-increasing pace. Yet companies are not the only ones innovating. Cybercriminals are too. As the threat landscape evolves, traditional defences are increasingly ineffectual. Organisations need modern tools that shine a light into blind spots to deliver visibility from cloud to on premise. They need security leaders who can speak the language of business risk. Boards that are prepared to listen. **And a technology strategy based around an understanding that it's 'not if but when' they are breached.**

"

Tim Wade, Technical Director, Office of the CTO, Vectra AI

It's time to change the game when it comes to dealing with attackers

The ongoing cybersecurity arms race demands constant innovation from both sides. A cybercrime economy worth trillions annually provides a fertile environment for new TTPs to thrive and disseminate. So how is the industry coping with the challenge of defending against this ever-moving target?

Many respondents felt that the industry is falling behind. Nine-in-ten (89%) rightly acknowledged that legacy approaches don't protect against modern threats, and that we need to "change the game when it comes to dealing with attackers". This was echoed by the fact that 69% think that cybercriminals are leapfrogging current tools and that security innovation is years behind that of the hackers. A further 72% feel security guidelines, policies and tools are failing to keep pace with threat actor TTPs.

It is perhaps unsurprising that more than three quarters (76%) of security leaders reported they have bought tools that failed to live up to their promise, with integration, lack of visibility cited as key reasons.

Top three reasons security tools fail to deliver on promise:

1. Poor integration with other tools
2. Failure to detect modern attacks
3. Inability to drive visibility/security across all environments (including cloud, endpoints, data centres and IoT)

89%

acknowledged that legacy approaches don't protect against modern threats

69%

think that cybercriminals are leapfrogging current tools

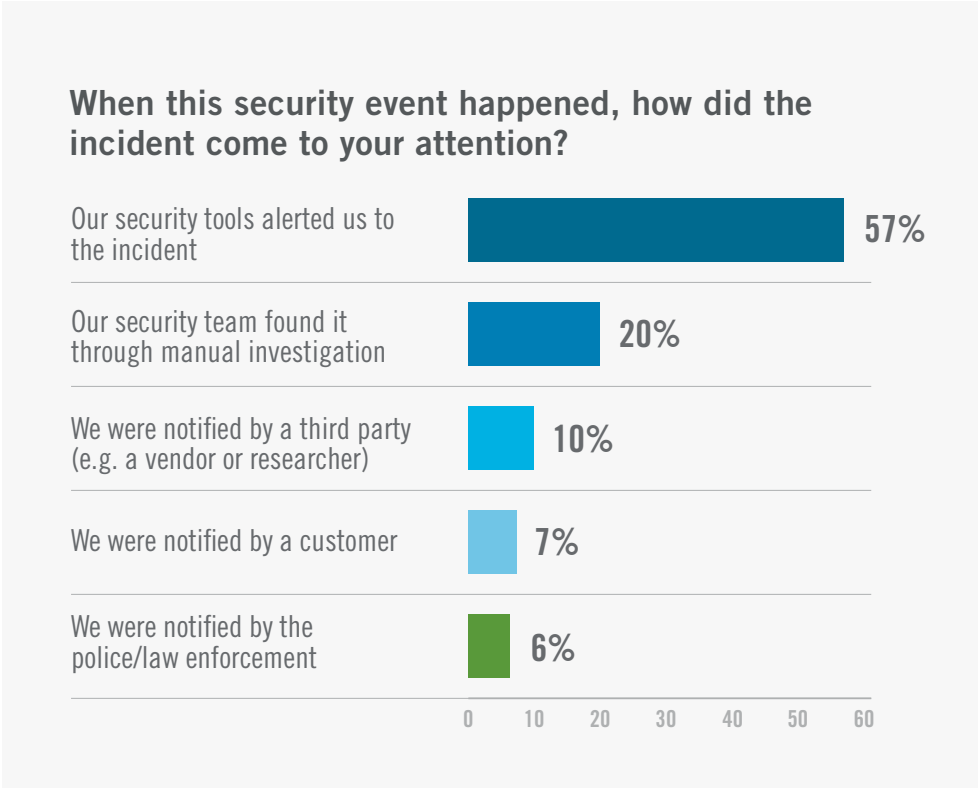
72%

feel security guidelines, policies and tools are failing to keep pace with threat actor TTPs

76%

reported they have bought tools that failed to live up to their promise

Despite these challenges, progress is being made. Of the 78% of respondents that experienced an event requiring significant incident response, just over half (57%) were alerted to the problem by their security tools. This is a positive development. Back in 2015, research indicated that 70% of breach incidents were discovered by a third party. So, detection and response tools are doing better. But it's also true that what worked yesterday might not work today.



"

The threat landscape is dynamic and volatile, so people are right to take an 'assume breach' stance. There's no such thing as total protection. If a determined threat actor wants to get inside your network today, they usually will. There are simply too many attack vectors they can prey upon, and too many potentially unmanaged and under-protected assets to target. They have the benefit of advances in malware, automated toolsets and 'as-a-service' models, which have opened the door even to tech novices. This is why it's vital to hunt for attackers hidden in your networks in order to find the needles in the haystack.

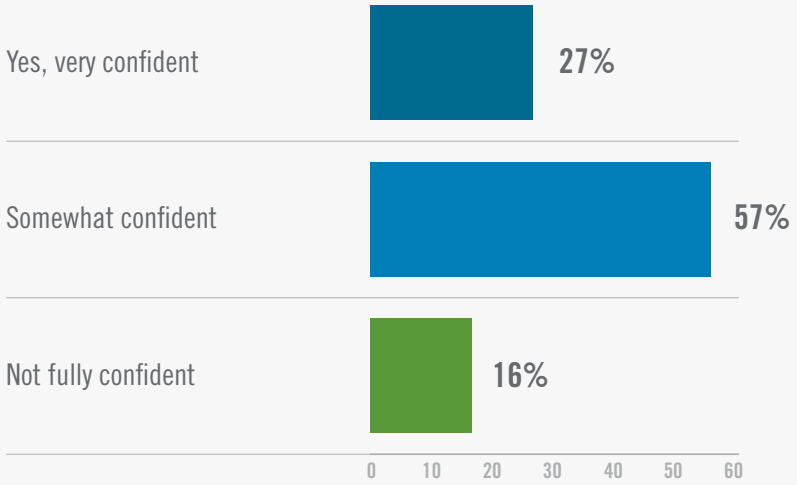
"

Tim Wade, Technical Director,
Office of the CTO, Vectra AI

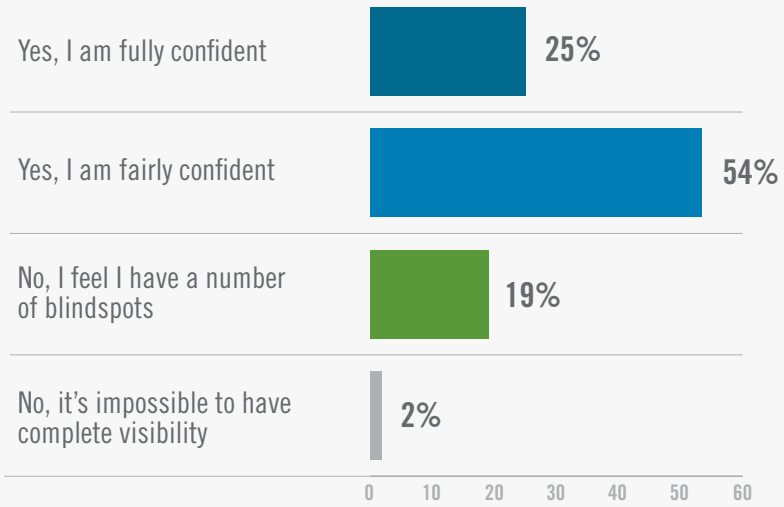
VECTRA
SECURITY THAT THINKS

Added to this, over a quarter (27%) of respondents said they're very confident their portfolio of tools could detect and protect them against the kinds of threats used in the Kaseya, SolarWinds and JBS attacks. A further 25% said they were fully confident that they have visibility of all threats facing their organisation.

Are you fully confident that your security tools would enable you to detect and protect against they type of sophisiticated tactics involved in recent attacks?



Do you feel confident that you have visibility of all the threats facing your organisation?

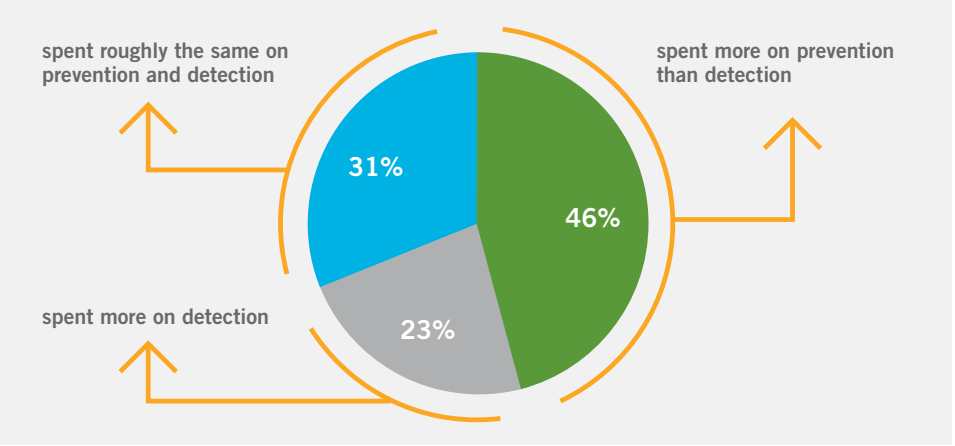


Legacy ‘prevention-first’ thinking puts organisations at risk

Recent advances in attack methods which enable attackers to bypass prevention technologies – such as multi-factor authentication – with relative ease. Yet legacy ‘prevention-first’ thinking continues to prevail. Two-thirds (65%) of respondents still believe prevention is more important than detection — believing that if a hacker manages to gain access to a corporate network, the company has already lost. As a result, 46% said they spend more on prevention than detection, with only a fifth (23%) spending more on detection and a third (31%) roughly the same. Of course, organisations shouldn’t stop investing in tools like multi-factor authentication outright – it’s still a valuable way to reduce the attack surface – but they can’t be relied upon to protect against modern threats.

65%

of respondents still believe prevention is more important than detection



“

If you put all your faith in prevention then you are in for a rude awakening. While organisations should certainly try to make life as difficult as possible for an attacker, prevention should not come at the expense of detection. Time, motivation and resources are usually on the attacker’s side—and they only need to get lucky once to succeed. But if a threat actor successfully gains access to a corporate device or network, there are still several stages of the attack chain they need to complete before they reach their target. A rapid response can effectively neutralise the threat before any damage can be done. In a high-risk game where the bad guys hold many of the winning cards, detection and response is increasingly the best option to minimise the impact of any breach as quickly as possible.

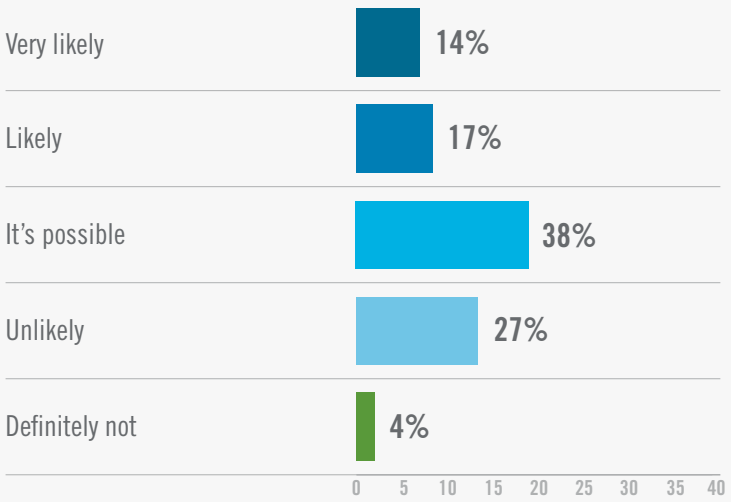
”

Tim Wade, Technical Director,
Office of the CTO, Vectra AI

This is a typical example of potentially harmful legacy thinking. A 100% successful prevention strategy in today's threat landscape is almost impossible. Cybercriminals have simply too many ways to gain entry: from vulnerability exploits to social engineering. Use of stolen or brute forced credentials, and bypass MFA with ease, mean they may not even set off any anti-malware alarms. Then once inside networks they can use legitimate tooling and techniques to remain hidden.

However, most respondents understand that prevention cannot be 100% effective. Over two thirds (69%) of respondents think they may have been breached and don't know about it – 31% of whom say they think is likely. Furthermore, 50% of respondents said they believe traditional prevention security is becoming obsolete, because hackers have access to such tools and can therefore design ways to circumvent them. This suggests an important shift in mindset is occurring.

How likely is it you have been breached and you don't know about it yet?



50%

believe traditional prevention security is becoming obsolete because attackers can use tolls to circumvent them.

Security leaders must educate the board about modern threats

It's not just legacy thinking within security departments that is opening teams up to potential risks. Traditional top-down ways of thinking and corporate culture can also have a negative impact. 82% of respondents believe that the cybersecurity decisions their boards make are influenced by existing relationships with legacy vendors. Over half (58%) said they think the board is a decade behind when it comes to security discussions.

> Traditional top-down ways of thinking and corporate culture can also have a negative impact.

This highlights an urgent need for security teams to educate the board on new threats that the organisation is facing and the most effective strategies for defences. Yet this could be a challenge. Two-thirds (68%) of respondents said it's hard to communicate the value of security to the board, as it is notoriously difficult to measure. This suggests communication between the board and security teams continues to be a challenge.

> Over half (58%) said they think the board is a decade behind when it comes to security discussions.

82%

believe the cybersecurity decisions by their boards are influenced by legacy vendor relationships

68%

of respondents said it's hard to communicate the value of security to the board, as it is notoriously difficult to measure

While it's certainly true that communicating and measuring the value of security is not always straight forward, it is possible to measure specific security capabilities. To do so in the most effective way, security leaders must always look to align their metrics with business objectives, quantified in a risk-based way that will resonate. Failure to do so will likely mean important funds for new technologies aren't released by the board.

However, there are signs that things could be changing, thanks to increased media exposure. Some 89% of respondents said that recent high-profile attacks have meant the board is starting to take proper notice of cybersecurity.

> 86% of respondents are grateful for the guidance of these organisations in helping them to sort the good from the so-so vendors.

Fortunately, the expertise of channel partners is proving invaluable in countering the negative impact of the board's legacy attitudes. Some 86% of respondents are grateful for the guidance of these organisations in helping them to sort the good from the so-so vendors. Channel organisations provide new opportunities for customers to explore different types of technology, using their business relationships to arrange early demos and proof-of-concept trials. Their teams are usually well trained and highly motivated, bringing extra expertise to bear at a time when in-house corporate cybersecurity teams are struggling under the weight of skills shortages.

"

In an age when digital transformation is table stakes for global businesses, the Board need to inform themselves about security and understand the potential risk. Recent high profile attacks have helped to illustrate the importance of cybersecurity, security leaders now need to grasp this opportunity to deliver change. Education is key to this. Security leaders need to help business leaders what the different risks and potential outcomes are and the different strategies that could be used to mitigate these risks. Critically, we need to start speaking the same language and translate risk into a vernacular that everyone can understand – it's time to drop the acronyms.

"

Tim Wade, Technical Director,
Office of the CTO, Vectra AI

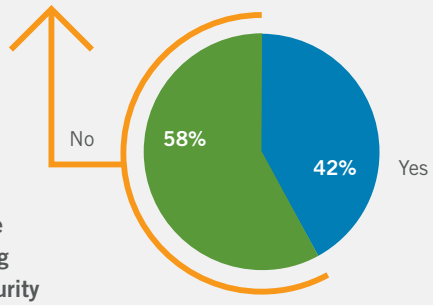
Regulators need a better understanding of life on the front lines

Depending on the type of organisation they work for, the role of a cybersecurity professional may be heavily influenced by a complex set of overlapping regulatory and legislative mandates. Most recently, the EU's General Data Protection Regulation (GDPR) has raised the stakes considerably for data breaches by sanctioning potentially astronomical fines for erring companies. And the EU Network and Information Security (NIS) directive, currently being rewritten, lays out new minimum requirements for "operators of essential services" in various sectors. On top of this come the various sector-specific regulatory requirements enforced by the likes of the Financial Conduct Authority (FCA) and the Bank of England's Prudential Regulation Authority (PRA). And there are cross-sector compliance mandates like PCI Data Security Standard (DSS), for organisations that process card details.

However, a majority (58%) of respondents claimed legislators aren't well-equipped enough to make decisions around cybersecurity matters and called for more industry input and collaboration. A further 43% argued that regulators don't have a strong enough understanding of life on the front lines to be writing in laws for cybersecurity professionals.

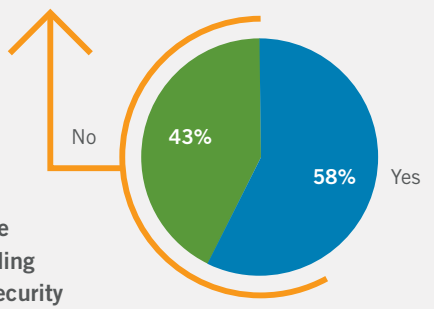
Both responses would seem to suggest that security workers feel those responsible for creating and enforcing regulatory and legislative mandates are too divorced from the day-to-day experiences of industry professionals. It's a concern in many sectors, but especially in cybersecurity where technology innovation on the attacker and defender sides moves so quickly that, if not written well, rules can quickly become out of date.

58% claimed legislators aren't well-equipped to make decisions around cybersecurity matters



Do you think legislators are well-equipped to be making decisions around cybersecurity related regulations?

43% regulators don't have a strong enough understanding of life on the front lines to be writing in laws for cybersecurity professionals

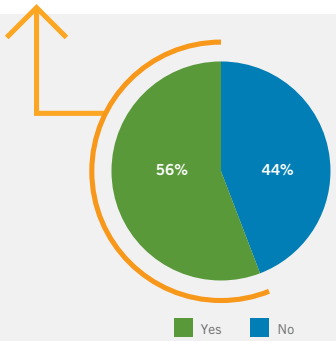


Do you think regulators have a strong enough understanding of the harsh realities that security teams are experiencing?

Even where guidelines are drawn up by security experts, like those working at GCHQ's National Cyber Security Centre (NCSC), praise from industry professionals can be in short supply. Only 56% said they had read the NCSC's *10 Steps to Cyber Security* guide for medium and large businesses, and just a third (34%) said they found it gave them everything they needed to enhance threat detection and response. Over half (51%) argued that it needs to be more instructive.

56%

said they'd read the guide for medium and large businesses



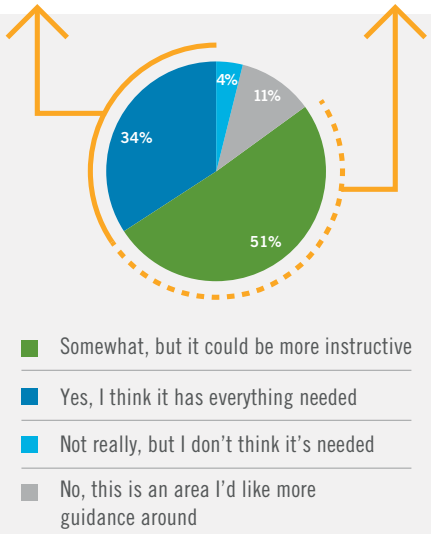
Have you read the NCSC's latest "10 Steps to Cyber Security" guidance for medium to large organisations?

34%

found it has everything needed

51%

felt it could be more instructive



Have you found this guidance useful?

"

Good cyber hygiene should be a goal for any security function. It's about going back to basics and understanding what data and assets you have, and who has access, before applying the appropriate controls. Effective regulations, laws and standards should codify this common-sense approach and inform every part of the job. But, it's important to remember they only give you a floor, not a ceiling. Threat actors are innovating faster than most regulators or legislators can issue new edicts, so your security strategy should move at the same pace.

"

Tim Wade, Technical Director, Office of the CTO, Vectra AI

VECTRA
SECURITY THAT THINKS

Conclusion

Legacy, prevention-focused security approaches give attackers the advantage when dealing with complex, modern threats. There are no silver bullets in security. Everything is fallible. Attackers have access to tools. They can test and see what can and can't get through. In the end, they will succeed. As an industry, we must shift focus to building resilience-based programs.

Resilience must begin with the right attitude. Assume breach. So the majority of UK cybersecurity professionals that believe they've already been breached without knowing it are on the right track. They simply can't rely any longer on legacy prevention-based tools, government advice and outdated input from the board.

However, by accepting this evolution in strategy, CISOs can create the right conditions for effective cyber-risk management. Understanding that threats may slip under the radar is not the same as admitting defeat—far from it. The new approach should be to do everything possible to stop hackers from getting in, but then to have the tools to spot suspicious behaviour if they do slip through the net. By doing so effectively, UK organisations can detect and contain incidents before they even have a chance to turn into something more serious.

Everything is containable up until an attacker has reached its target. But incident responders can't work in a vacuum. They need the right tools to maximise analyst productivity and help to spot the needle in the haystack of needles.

How Vectra can help

Our leading threat detection and response platform helps organisations to stay out of the headlines by detecting and disrupting attackers before they can cause any damage. How do we do this? By taking an AI-driven cloud security-lead approach, which supports Security Operations Centre (SOC) teams by enabling them to prioritise events based on accurate threat assessments.

The Vectra Cognito platform accelerates threat detection and investigation by using intelligent ML-algorithms to enrich the cloud and network metadata it collects and stores with the right context. It's this context which enables SOC analysts to detect, hunt and investigate known and unknown threats in real-time. The result? Proactive security that allows your organisation to leverage the best of man and machine to minimise cyber-risk. A safer, more secure digital world awaits.

See threats. Stop breaches.

Request a Demo

Email info@vectra.ai vectra.ai