VECTRA®
SECURITY THAT THINKS

RESEARCH STUDY | GLOBAL

Fit for Purpose or Behind the Curve?

Uncovering how today's organisations are tackling complex, modern cyber-threats

VECTRA
SECURITY THAT THINKS

Table of Contents

VECTRA
SECURITY THAT THINKS

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 micro-services, 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.

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 cyber attacks cost big money today: the average figure per incident is an estimated $4.2m (£3m), 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 against attacks 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, cyber criminals are masters at staying hidden – they're constantly innovating, so cybersecurity has to continually evolve to keep up.

To find out more about how security leaders are tackling these dynamic threats, Vectra commissioned Sapio Research to interview 1800 IT security decision makers working at organisations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

> 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-centric' 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 are aiding cybersecurity efforts.** Security leaders are confident that regulators are creating effective legislation, but ultimately a hacker mindset, and rapid detection and response, give you the best chance.

Key stats:

83% think traditional approaches don't protect against modern threats and that we need to change the game when it comes to dealing with attackers

79% 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

72% think they may have been breached and don't know about it— 43% think this is "likely"

87% of respondents say recent high-profile attacks have meant the board is starting to take proper notice of cyber security

83% 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 blindspots 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, Deputy CTO, Vectra AI

VECTRA
SECURITY THAT THINKS

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?

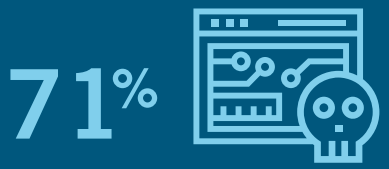
Many respondents felt that the industry is falling behind. More than eight-in-ten (83%) rightly acknowledged that legacy approaches don't protect against modern threats, and that we need to "change the game when it comes to dealing with attackers". This was echoed by the fact that 71% think that cyber-criminals are leapfrogging current tools and that security innovation is years behind that of the hackers. A further 71% feel security guidelines, policies and tools are failing to keep pace with threat actor TTPs.

It is perhaps unsurprising that more than three quarters (79%) of security leaders reported they have bought tools that failed to live up to their promise, with failing to detect modern attacks, only preventing low-level threats, and poor integration with other tools as key reasons.

Top three reasons security tools fail to deliver on promise:

1. Failure to detect modern attacks
2. Only prevented low-level threats
3. Poor integration with other tools

83% acknowledged that legacy approaches don't protect against modern threats



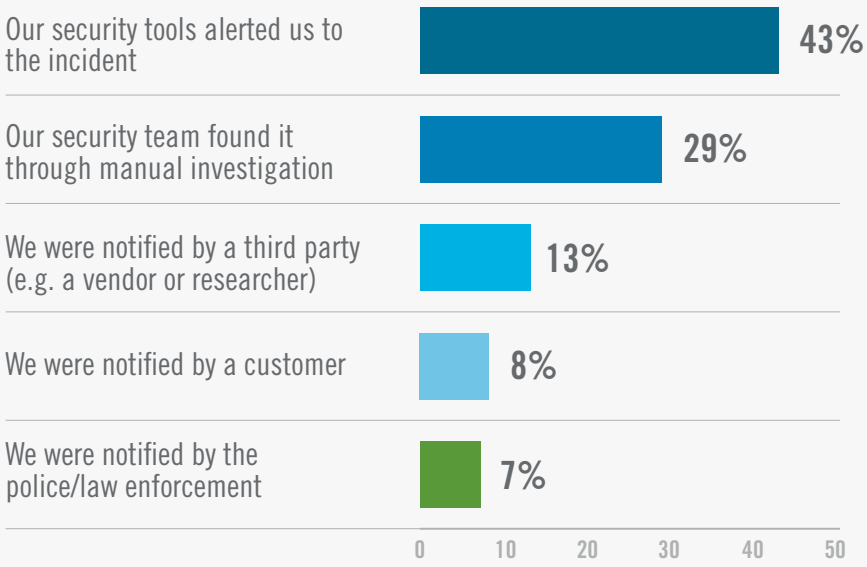
71% think that cybercriminals are leapfrogging current tools

71% feel security guidelines, policies and tools are failing to keep pace with threat actor TTPs

79% reported they have bought tools that failed to live up to their promise

Despite these challenges, progress is being made. Of the 74% of respondents that experienced an event requiring significant incident response, 43% 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.

When this security event happened, how did the incident come to your attention?



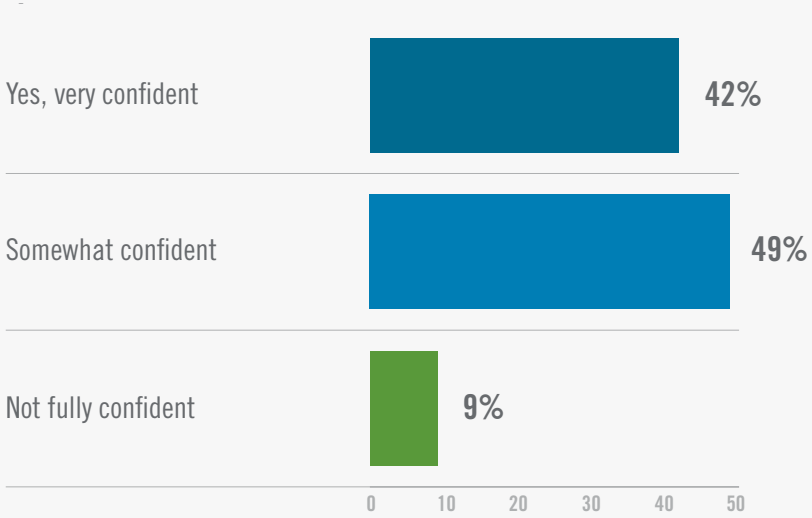
"**The threat landscape is dynamic and volatile, so people are right to take an 'assume breach' stance.** There's no such thing as total protection. If a determined threat actor wants to get inside your network today, they usually will. There are simply too many attack vectors they can prey upon, and 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, Deputy CTO,
Vectra AI

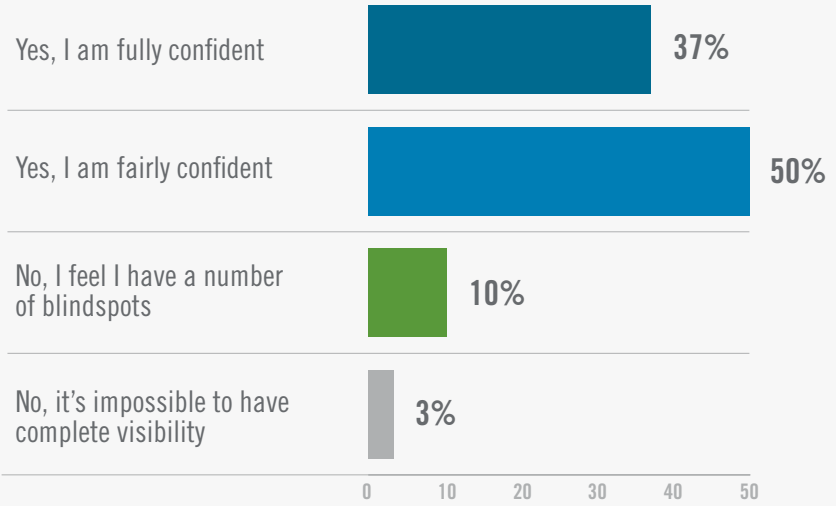
VECTRA
SECURITY THAT THINKS

Added to this, over two fifths (42%) 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 37% 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?



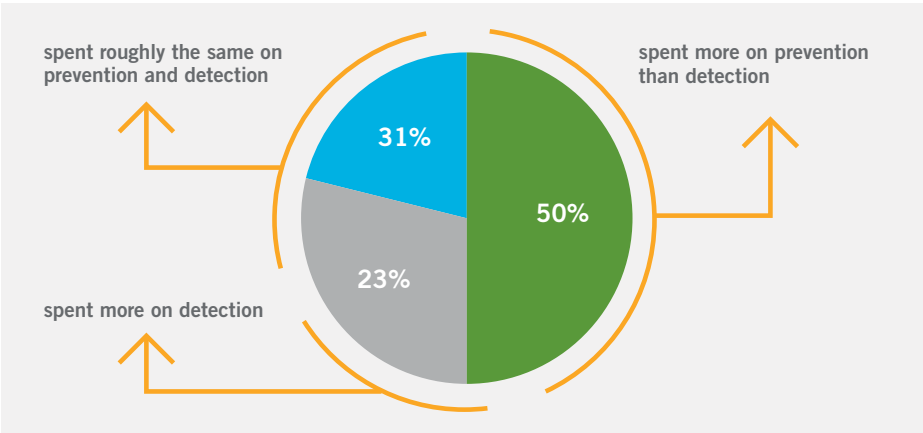
Legacy ‘prevention-centric’ thinking puts organisations at risk

Recent advances in attack methods have been made which enable attackers to bypass prevention technologies – such as multi-factor authentication – with relative ease. Yet legacy ‘prevention-centric’ thinking continues to prevail. Although organisations should still continue taking preventative steps such as enabling MFA, these are not enough in isolation.

The commonly held belief remains that if a hacker manages to gain access to a corporate network, the company has already lost. As a result, 50% said they spend more on prevention than detection, with only a fifth (22%) spending more on detection and less than a third (29%) roughly the same.

50%

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.

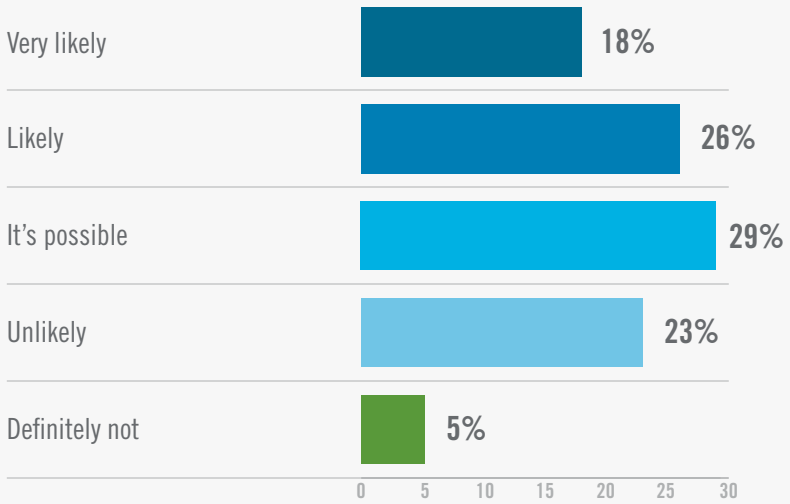
”

Tim Wade, Deputy 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. Cyber-criminals have simply too many ways to gain entry: from vulnerability exploits to social engineering. Use of stolen or brute forced credentials, and bypassing 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 (72%) of respondents think they may have been breached and don't know about it – 43% of whom say they think it is likely. Furthermore, 62% 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?



62%

of respondents believe traditional prevention security is becoming obsolete

VECTRA
SECURITY THAT THINKS

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. 83% of respondents believe that the cybersecurity decisions their boards make are influenced by existing relationships with legacy vendors. Over half (54%) 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. Almost two-thirds (61%) 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 (54%) said they think the board is a decade behind when it comes to security discussions.

83%

believe that the cybersecurity decisions their boards make are influenced by existing relationships legacy vendors

61%

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 straightforward, 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 87% of respondents said that recent high-profile attacks have meant the board is starting to take proper notice of cybersecurity.

> 92% 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 92% 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, Board members need to inform themselves about security and understand the potential risk. Recent high profile attacks have helped to illustrate the importance of cybersecurity, and security leaders now need to grasp this opportunity to deliver change. Education is key to this. Security leaders need to help business leaders understand 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, Deputy CTO,
Vectra AI

Despite complex legislation, regulators are on the right 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. According to data from the United Nations Conference on Trade and Development (UNCTAD), 156 countries (80%) have enacted some form of cybersecurity legislation. But with no overarching international laws currently enforced, security professionals must adhere to differing rules and regulations across various regions, making worldwide compliance a daunting task.

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. Although EU-centric, GDPR in particular has been implemented to safeguard the data of EU citizens and residents wherever it is stored – meaning that it has global implications for international organisations.

However, there is widespread global support for cybersecurity regulators and legislators. More than three quarters (76%) believe that regulators have a strong enough understanding of life "on the front lines" to be writing laws for cybersecurity professionals. A further 65% think that, as the experts, legislators are well equipped to be making decisions about cybersecurity related regulations. So the consensus seems to be that, although cybersecurity laws are challenging both to implement and follow, the best people are currently in place to be making these decisions.

The majority of respondents across most countries had read the specific regional guidance we asked them about. This suggests that for many, these instructions provide everything cybersecurity professionals need to enhance threat detection and response. 57% agreed that 'following these guidelines will help protect us from the majority of threats', whilst over half also agreed that they 'help to encourage best practice' and 'protect us against modern threats' (both 55%).

"

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, Deputy 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 global majority of 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 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, organisations globally 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-led approach, which supports Security Operations Centre (SOC) teams by enabling them to prioritise events based on accurate threat assessments.

The Vectra AI-driven 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 earlier. Stop breaches.

Request a Demo

Email info@vectra.ai vectra.ai