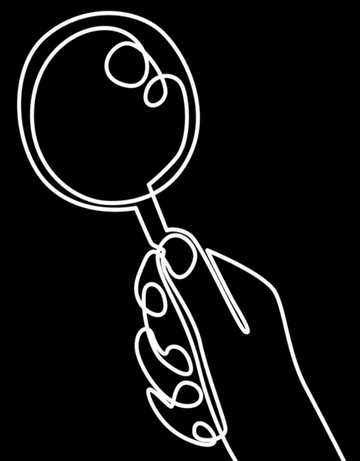
acora
Led by Experience

KEEPING UP WITH ENDPOINT THREATS AND SECURITY RECOMMENDATIONS

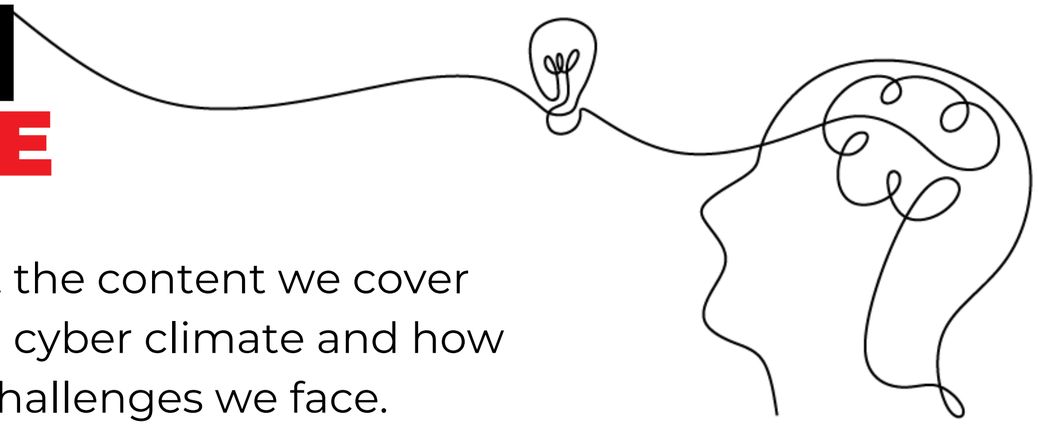
CONTENTS



1

CYBER CLIMATE

INTRODUCTION
TO THE CYBER CLIMATE



Thank you for downloading our eBook. We hope that the content we cover strengthens your understanding of the ever-growing cyber climate and how the market has and is continuing to respond to the challenges we face.

RANSOMWARE EVOLUTION

DISTRIBUTED WORKFORCE

NEW GENERATION EVOLVING THREATS

It is no secret that hackers' skills are advancing, making it easier to bypass traditional security measures. This expresses the importance of regularly reviewing the tools currently in place, evaluating them honestly and judging if they are fit for purpose as threats evolve.

There is no, and never will be a silver bullet, however, acknowledging the changing threat landscape and addressing the risk is a step in the right direction.

Continue reading to explore how specific tools such as endpoint security have advanced. We will highlight some of the challenges you may be familiar with around traditional cyber security measures and how they continue to fall behind in their ability to adapt. The truth is, what may have been reliable a few years ago, may not be good enough in today’s cyber climate.

2

THREAT DETECTION

IN 2022, OVER A 12-MONTH PERIOD, RANSOMWARE ATTACKS AFFECTED 73% OF UK ORGANISATIONS.

SOURCE: CYBER EDGE

Security challenges are the number one reason for keeping business leaders up at night.

CAN YOU BLAME THEM?

Ransomware is growing every day, the pressure of protecting the endpoints of a distributed workforce is heightened and we are constantly getting reminded of the disruption that evolving threats are causing. Let's take a step back and go back to basics...endpoint security.

It goes without saying that threat detection is a key factor to improve security posture. Detection capabilities are changing to reflect the fact that threat actors are always evolving and defenders need to stay one step – or more – ahead.

INSIGHTS FROM OUR VERY OWN THREAT HUNTING LEAD

> Endpoints often act as the entry points for threat actors aiming to infiltrate the estate. Therefore, threat detection across all endpoints is one of the most critical and important controls for an organisation of any size.
>
> Threat actors have significantly evolved over the years both in terms of resources and sophistication. As a result, modern malware utilises impressive evasion techniques, stay mostly in memory and are able to transform and bypass all signature-based methods. Threat detection and response is a crucial control to not only detect threats at early stages but also be able to contain them as quickly as possible and minimise their impact.

OUT WITH THE OLD

Traditional detection tools were designed decades ago when you could count the number of discovered threats on one hand. Their techniques are primarily known for only working with file-based malware which relies entirely on what is known. However, we all know that “there are also known unknowns” – Donald Rumsfeld.

Viruses can go undetected for extended periods of time, and with the scale of the threats today along with the long-term impact that they can have on your business, it is important that you have access to in-depth threat hunting. This way, you gain more control and the threats have a decreased chance of going unnoticed!

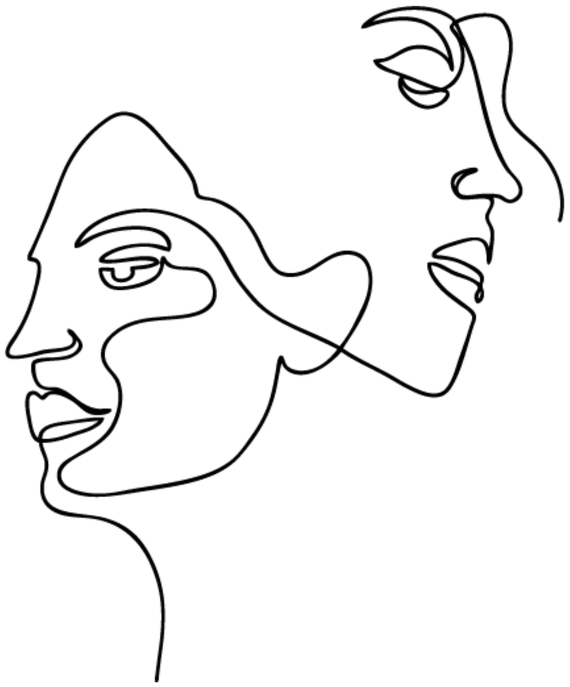
IN WITH THE NEW

The security industry has evolved and we are moving into a new era of detecting threats. Visibility goes further than just scanning file-based malware, data can now be picked apart and examined to digest patterns in real-time.

In-depth, threat hunting has been introduced to identify file modifications, process creations and network connections that have occurred on an endpoint. There are also enhanced capabilities around searching for indicators of compromise applied to historical data. These are all vital elements for incident response and digital forensics.

3

INCIDENT RESPONSE



THE IMPORTANCE OF A ROBUST INCIDENT RESPONSE PROCESS CANNOT BE OVERSTATED.

The ultimate goal is to contain an incident, reduce the risk, and remediate or roll back any potential effects from a threat back to an operational state as quickly as possible. Are you confident that your security solutions are providing you with the relevant insights enabling you to act quickly?

Without in-depth visibility of threats and data points, connecting the dots is tricky. Let's put this into perspective. Your endpoint has identified a threat. Data is located in multiple locations. Your team have to gather the data and make sense of what is happening. At this point, the hacker has the upper hand. There is no time like the present and the clock is ticking. This is viewed as a reactive and delayed approach.

TIME TO REFLECT

Lessons have been learned and incident response parameters have evolved. Software that can coordinate and expedite incident response processes is the way forward. Quietly in the background, a granular view of threat activity is absorbed at scale while AI-powered analytics are used to reconstruct threat events, presenting the required data on a silver platter. All at machine speed, accelerating the response time.

Wait for it. In this day and age, all of this can happen without human intervention.

4

IMPROVING EFFICIENCY

We all want to be faster and better to improve our business processes. But this can’t be more prominent in the cyberspace .

According to Forbes, security success is based on operational efficiency and we couldn’t agree more.

With overstretched IT and Security teams, every second counts. The last thing businesses need in today's cyber climate is spending significant amounts of time juggling projects, updating security tools, manually correlating and contextualising alerts and tediously writing scripts for remediation. Unfortunately, this is the reality of dealing with traditional tools.

THE LONG RUN

The endpoint security market has listened. We have moved into a world where automation is now an expectation instead of a wow factor. Integrations and automations are both critical to helping Cyber Security and IT functions vastly improve productivity and speed, making teams far more efficient and effective. Next-generation anti-virus platforms are leading the market in response to the evolution of threats.

The sole aim is to prevent, detect, and remediate modern attacks without additional overhead costs and sluggish manual workflows.

5

A SNAPSHOT OF THE NEXT-GENERATION

SO, WHAT'S NEXT?

No matter how big or small your business is, every company is a target. And we all have operational, brand and revenue pipelines that are at risk. According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.

Just let that sink in for a second. We may sound like a broken record however, it is clear that in line with the ever-growing threats, tools and security measures need to evolve simultaneously. They need to be fit for purpose to build confidence and resilience company-wide, from end-users through to a board level.

WHAT DOES THIS MEAN FOR YOU, AS AN IT LEADER?

THE CYBER CLIMATE HAS EVOLVED, AND THIS BREAK DOWN IS THE HARSH TRUTH

Traditional threat detection tools are primarily designed for relying entirely on what is known. We hate to break it to you, this isn't good enough. Viruses can go undetected for extended periods of time.
Gain the control you desire, and stand up to the threats by using in-depth threat hunting.

Incident Response lessons have been learned and parameters have evolved. There's no time like the present. Time is precious, and you should most certainly have confidence in your tools that you can act quickly based on relevant endpoint threat insights.

We all crave efficiency. We want to be faster and better to improve processes. In the cyber world, every second counts. We are all familiar with juggling projects, completing manual tasks and contextualising alerts. In the unfortunate event of an attack, you need the assurance that you don't have to rely on sluggish manual workflows.

WE ALL WANT THE SAME OUTCOME. TO PREVENT, DETECT AND REMEDIATE MODERN ATTACKS.

Ask yourself the following question: Is your current endpoint protection living up to expectations? If you are unsure or know that the answer is a definite no, this should spark concerns.

Everyone desires the assurance that their security controls are not only sufficient for yesterday's attack but today's and tomorrow’s.

ACCORDING TO THE GARTNER STRATEGIC TECHNOLOGY REPORT

> Gartner predicts that by 2024, organisations adopting a cybersecurity mesh architecture will reduce the financial impact of individual security incidents by an average of 90%.

A NEXT-GEN ENDPOINT PROTECTION USER SAYS

> The ability to have a miniature SOC on every endpoint is fantastic because the agent handles 99% of all situations arising. That leaves you to deal with only the edge cases.

GET IN TOUCH

To find out how you can strengthen your security posture by keeping up with endpoint threats and next-generation security recommendations, contact us via phone, email or through our website.

OUR TEAM WILL BE HAPPY TO HELP.

TELEPHONE
0844 264 2222

EMAIL
hello@acora.com