Cybersecurity insights to empower you

5 things the bad guys don't want you to know

Symantec by Broadcom | Arrow

You don't need us to tell you that cybersecurity is one of the most serious threats facing businesses today.

$4.45M

The average global data breach cost was around $4.45 million in 2022.

Source

560K

new pieces of malware are detected every single day.

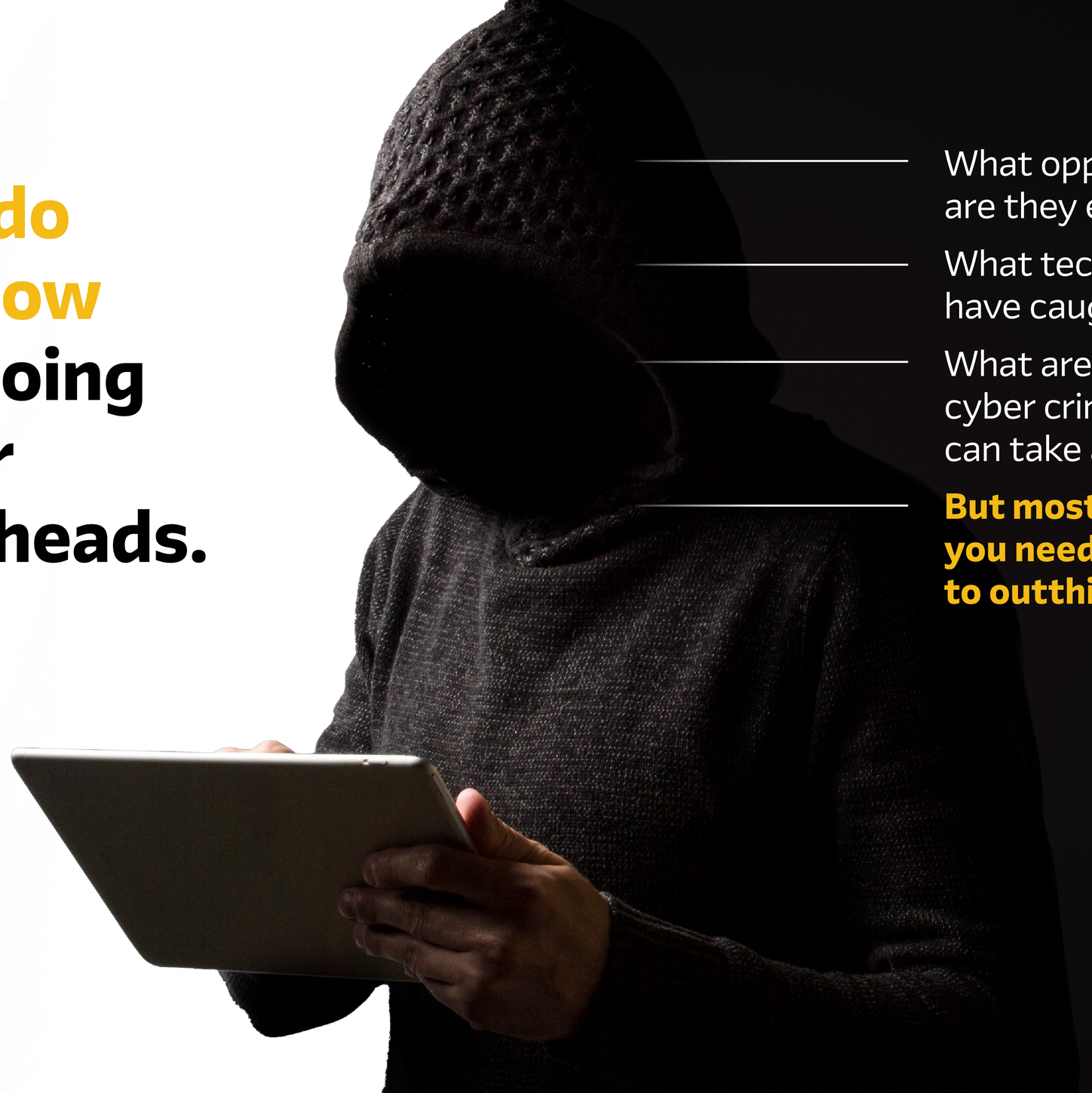
Source

76%

of organisations were attacked with Ransomware in 2022, with 64% victims of a successful infection.

Source

What you do need to know is what's going on in cyber criminals' heads.



What opportunities are they excited about?

What techniques have caught their eye?

What are the new trends in cyber criminality that they can take advantage of?

But most importantly, you need to know how to outthink them.

This guide will empower you to stay one step ahead of the cyber criminals.

You'll get an advantage so that you can protect, innovate, and adapt to whatever they throw at you.

Get the inside track on how:

1. Generative AI means you need to be clever about spotting phishing emails
2. Ransomware attacks are about much more than just ransoming data
3. While you focus on next-generation security threats, the basics are still being exploited
4. The weak links in supply chains are attackers' biggest targets
5. Wherever your people work from, they're a target

Let's get started.

Generative AI means you need to be clever about spotting phishing emails

Generative AI has changed the game when it comes to phishing attacks.

In their efforts to imitate employees and businesses, cyber criminals are now using malicious AI language models like WormGPT and PoisonGPT to scour public social media profiles and online information.

These models then use this data to write emails that mimic the person's exact tone of voice to a tee, using their colloquialisms, referencing their personal lives and even replicating their commonly used mistakes.

This can create a replica of, say, a supervisor's email in a workplace, making it much harder for even the most clued-in tech professionals to spot and report phishing emails.

Interaction rates with **AI-created emails (65%)** have now overtaken those of **human-generated emails (60%)**

Source

What you can do about it:

Give your teams the tools to spot malicious links

You can't rely on your people to spot fraudulent emails generated by AI – you need to back them up with the right technology.

That means technology that helps you identify suspicious emails and block malware from being downloaded through malicious links in those emails. You need software that does both of these things to ensure that no matter how genuine an email might seem to an employee, your cyber defences can step in to prevent infiltration.

Where Symantec can help:

Stop spear phishing attacks with Symantec Email Security.cloud. This software isolates suspicious email links, attachments and web downloads, authenticates senders by ensuring your email domain can't be replicated, uses an impersonation engine to spot spoofed email addresses, and much more – all to keep your people safe from fraud and malware phishing.

Find out more >

Did you know?

Symantec Web Protection can keep users safe from malicious, phishing or risky websites. It adds a layer of protection around email security.

The unique web security intelligence that Symantec Web Protection gathers is directly integrated into Symantec Email Security for a stronger defence.

Ransomware attacks are about much more than just ransoming data

The Organised Crime Groups that are behind Ransomware attacks have found new ways to make money. As part of this, new ransomware attacks do much more than just encrypt data for a ransomware payment.

At the same time as the encryption attack, they'll also steal the data to use it for other methods of data extortion – like threatening to tell your customers for example.

They'll even sell that data on the dark web for a third payout to make the absolute most of their work.

That means you'll have to deal with sophisticated and evolving attacks that not only result in financial loss, but also extortion and the black market illegally trading your data – the disruption this can cause is immense.

Just 1 in 5 modern ransomware attacks focus on encrypting data alone.

Source

What you can do about it:

Your last line of defence against ransomware – and therefore one of your most important – is your endpoint security solution.

Naturally, your network, web and email security play their part in identifying and eliminating attacks, but anything that gets through will need to be dealt with endpoint security that's up to the task.

So it's more than worth investing in software that can cover all endpoints across the attack surface.

Where Symantec can help:

Symantec Endpoint Security Complete is an on-premise, hybrid or cloud-based solution that protects all traditional and mobile endpoints – all in one, unified cloud-based management system.

And it's all connected to the Symantec Global Intelligence Network – one of the largest civilian security threat intelligence networks in the world. It uses AI and a team of specialist threat hunters to analyse over 9 petabytes of security threat data – bringing together knowledge about websites, malware, email risks and more to help better defend your business' endpoints.

Find out more >

Did you know?

Data Loss Prevention (DLP) can help you identify and protect your most sensitive data. Once you know where your most confidential data is, you can then take the appropriate measure to protect it from exfiltration.

While you focus on next-generation security threats, the basics are still being exploited

Many ransomware attacks happen, and are successful, because of bad security hygiene.

Sometimes IT teams can overlook basic security weaknesses in their setups because they might be focused on the bigger picture and upcoming threats – such as AI for example.

And as cybersecurity environments get more complex and the attack surfaces get wider, (with new tools, users and devices), it becomes more difficult to make sure all the essentials are in place.

This is the perfect situation for a cyber criminal, especially in hybrid and multi-cloud environments; they'll take advantage of thinly spread IT coverage to spot holes and infiltrate your organisation.

Only 15% of businesses have undertaken cybersecurity audits.

Source

What you can do about it:

Basic cyber hygiene goes a long way towards achieving optimal cybersecurity – while implementing advanced security tools is important, not getting your fundamental defences in order can lead to security incidents, data compromise and data loss.

Bringing your cyber hygiene up to a good level is crucial to protect all of your systems. It keeps sensitive data secure, protects it from threat, minimises attacks and prevents operational disruptions.

So make sure you've enabled everything your security tools have to offer – and trust in the expertise of a proven security provider who can conduct a comprehensive security review of your setup.

Where Symantec can help:

Symantec security products feature configuration health reports, designed to help you spot ways to improve your cybersecurity.

These reports show you the areas that need improvement and give you product advice on how to improve your team's security settings. They'll tell you where to look, where policies aren't being deployed and where the basics aren't being covered – all so you can tighten things up and get your cyber hygiene back on track.

Find out more >

Did you know?

Arrow and its expert resellers can help to ensure your Symantec software is up and running at its optimal efficiency – and better yet, they can review the particular threats your organisation is concerned about and identify what gaps those threats might be able to exploit.

4

The weak links in supply chains are attackers' biggest targets

Effectively securing a supply chain is a tough ask – they're often large, complex and have multiple parties involved. But if a supply chain is successfully attacked, it can cause significant disruption to an organisation.

If cyber criminals find a weak link through a supplier and use it to attack a bigger partner, the supplier can face major repercussions – including loss of business and serious reputational damage.

That's why many of your biggest customers may now require an audit of your cybersecurity measures to ensure they're up to the necessary regulations and standards.

Supply chain cyber attacks **increased by over 600% in 2022**

Source

What you can do about it:

To ensure you and your partners' safety, and to make sure you're meeting compliance standards, you need to ensure you have the best security you can get – security from a provider that has proven credentials.

Symantec software, for example, is relied on by major organisations across the finance, retail, manufacturing and professional services sectors – so you know it has what it takes to keep your suppliers, customers and partners safe.

Avoid inadvertently putting your supply chain at risk by basing your security strategy around tried-and-tested, industry-trusted security.

Where Symantec can help:

Symantec technology provides you with enterprise-grade security that is already deployed by the world's leading businesses and organisations to protect them and their supply chains.

Rethink your security strategy by putting your trust in validated software that's backed by the Symantec Global Intelligence Network, so that you can stay compliant with the standards required by your partners.

Find out more >

Did you know?

As part of the Symantec Global Intelligence Network, the Symantec Threat Hunter team carries out regular investigations into global attacks that might affect your supply chain, building out profiles of the attackers and their tools, targets and motivations. It's all to develop actionable intelligence to improve the Symantec software's ability to protect your organisation.

Wherever your people work from, they’re a target

Now that many businesses have adopted a hybrid working model, their employees need security – wherever they are.

Driving all your business traffic through a VPN is expensive, slow and delivers a poor user experience. A better alternative is to build security around the end-user – to ensure they can directly access your network or cloud knowing they’re safe and secured.

But working remotely also places greater responsibility on the user to understand the risks of mishandling the information they work with. Shadow data – data your organisation keeps in data stores that aren’t regulated or governed – can be a serious risk in hybrid businesses so it’s more important than ever to know where your sensitive data is.

40% of organisations reported a cyber attack focused on their remote work infrastructure.

Source

What you can do about it:

You need security that protects users anywhere, anytime, by ensuring secure access from any device to any location.

Three foundational elements are Secure Web Gateway (SWG), Data Loss Prevention (DLP), and Cloud Access Security Broker (CASB) technology.

Secure Web Gateway solutions ensure that traffic to and from the web is inspected for threats, complies with your web access policies and can be paired with DLP to prevent data loss.

Data Loss Prevention monitors, controls and protects sensitive data to reduce data breaches and ensure compliance. It can be paired with CASB or Secure Web Gateway solutions to provide data security.

A Cloud Access Security Broker (CASB) governs access to cloud applications and infrastructure and can respond to user behaviour risk, detect malware and identify Shadow IT.

Where Symantec can help:

Symantec software lets you implement these technologies with just 2 offerings – Symantec Web Protection and Symantec DLP Cloud, which includes CASB.

These cloud-friendly and highly effective technologies wrap security around your users wherever they work from, whether they're at home, in the office or on the road. It's all to keep you and your data safe from attackers who are looking for vulnerabilities in your hybrid working setup.

Find out more >

Did you know?

Symantec Web Isolation keeps web sessions away from your endpoints, providing only a safe rendering of web pages to your teams' browsers. This stops any zero-day malware on malicious websites from ever getting to your devices, allowing users to safely access content without security controls impacting their productivity.

Adaptive DLP: User Behaviour Risk scores can be used to determine data access policies. For example, high risk users can be restricted from printing or downloading sensitive data.

How Symantec Enterprise Cloud can help empower you

Symantec Enterprise Cloud is uniquely qualified to address the most complex cybersecurity challenges in the world – from blocking unauthorised access and assuring data compliance, to stopping the newest generation of enterprise attacks.

The solution supports every deployment model from on-premises, to the cloud, to multi-cloud. We're here to empower you in your fight against cyber criminals, putting the best cybersecurity tools in your hands.

Here's how we do it...

Expert empowerment

You get the combined expertise of two industry leaders together to empower you: The Symantec Enterprise Cloud solution and Arrow

Symantec supports your unique security needs and relieves your resource burden or skills gaps

Symantec meets the exact security needs of your business, from implementation to a fully managed service

Security innovation

Symantec technology gives you an innovative, integrated security posture that works seamlessly for your business

Symantec's integrated security solutions are perfect for small and mid-size businesses, keeping workers secure, wherever they are

Symantec products operate through a high-speed Google Cloud infrastructure for a smoother user experience

20% of Broadcom's Symantec revenue is re-invested into research and development every year to keep you ahead of sophisticated threats

Best-in-class protection

With Symantec, businesses of all sizes get the cyber strength of enterprise-level businesses, trusted by many of the world's largest organisations

With integrated AI across Symantec solutions, your cybersecurity adapts to your business so you're ready when issues strike

The Symantec Global Intelligence Network gives you 24/7 monitoring and threat intel on 50 ransomware families

The network uses over 50 protection technologies, built on over 9 Petabytes of threat data

Symantec has blocked over 362,600 ransomware attacks, over 1.2 million Living-off-the-Land threats and over 2.3 million unknown and zero-day attacks

Security and compliance

Symantec data-protection tools enable a single policy across multiple control points, including key devices

Symantec experts serve in an advisory capacity to the regulatory bodies of the U.S. Government and European Union, ensuring we keep you abreast of the evolving compliance landscape

Whatever cyber criminals are planning, we can empower you to stay one step ahead.

Find out more about how Symantec can help you.

Symantec by Broadcom | Arrow