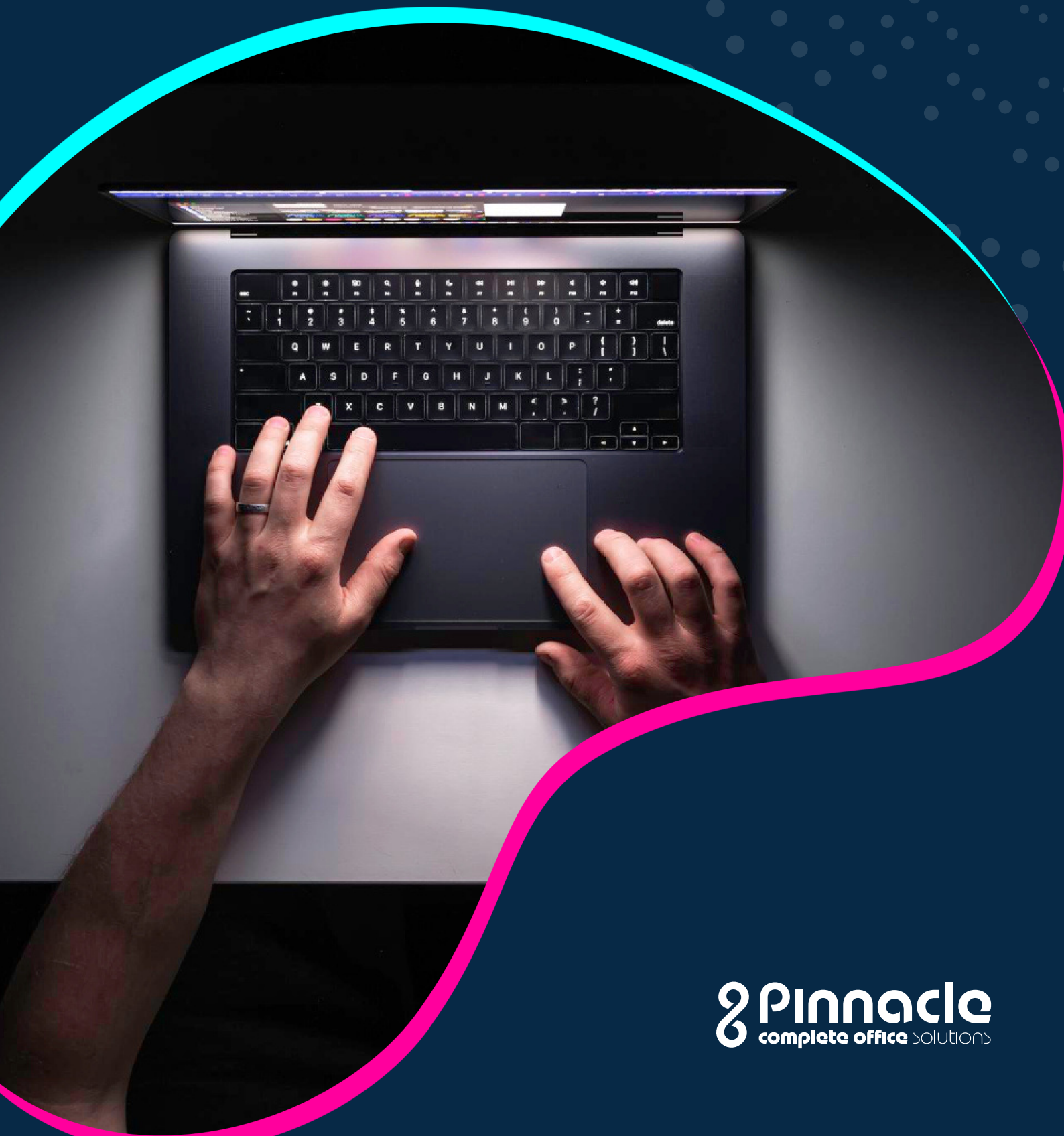
Dark Web Scanning

Understanding the why and how



Pinnacle complete office solutions

The need for Dark Web Scanning

Dark web monitoring is emerging as a crucial element of a solid, advanced cybersecurity strategy.

Unfortunately, many organisations are not aware of the dark web and its dangers.

Others don't take it seriously, thinking it can't possibly be a threat to their organisation. Don't let your business fall victim!

What you and your employees don't know can hurt you.

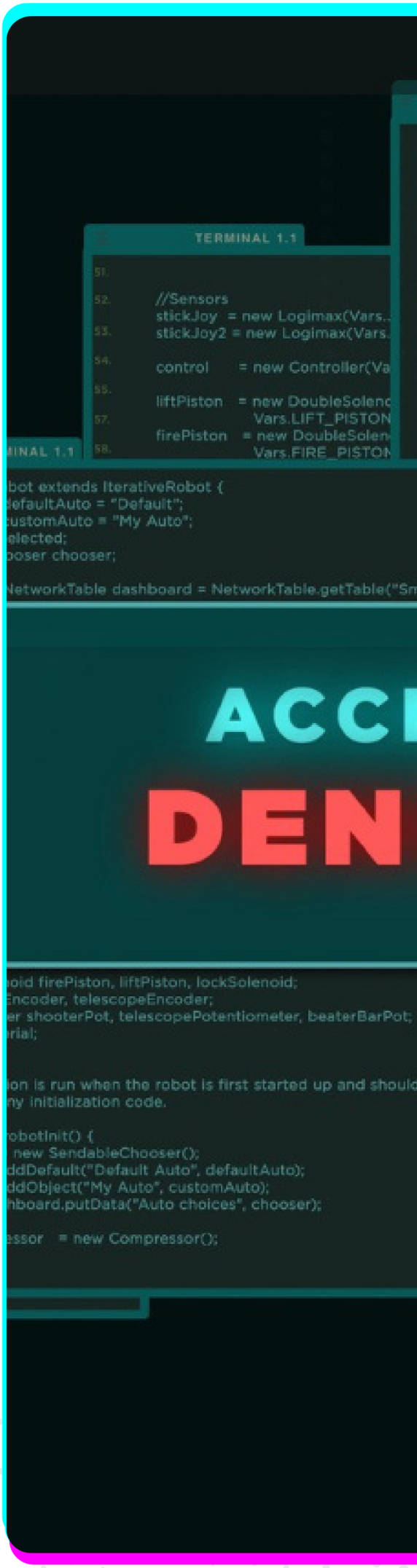
Today's hackers are working smarter, not harder. They have become increasingly adept at lucrative opportunities tied to the hostage of business email. Yet, many companies aren't prioritising their business success.

Take, for example, employee training. Many businesses don't realise their employees are one of their most significant security risks. You've probably heard the stories of cybercriminals dumping thumb drives loaded with malicious hacker code in employee parking lots, waiting for someone to pick one up and plug it into a work laptop.Pretty clever, right?

Unfortunately, research studies have found that more than 60% of people who find a thumb drive will do just that - potentially handing over network access to an enterprising hacker.

Research finds that most breaches are not initially detected and may not be discovered until several months after the initial attack. According to IBM's Cost of a Data Breach Report2020, the average time to identify and contain a data breach is 280days (approximately nine months).

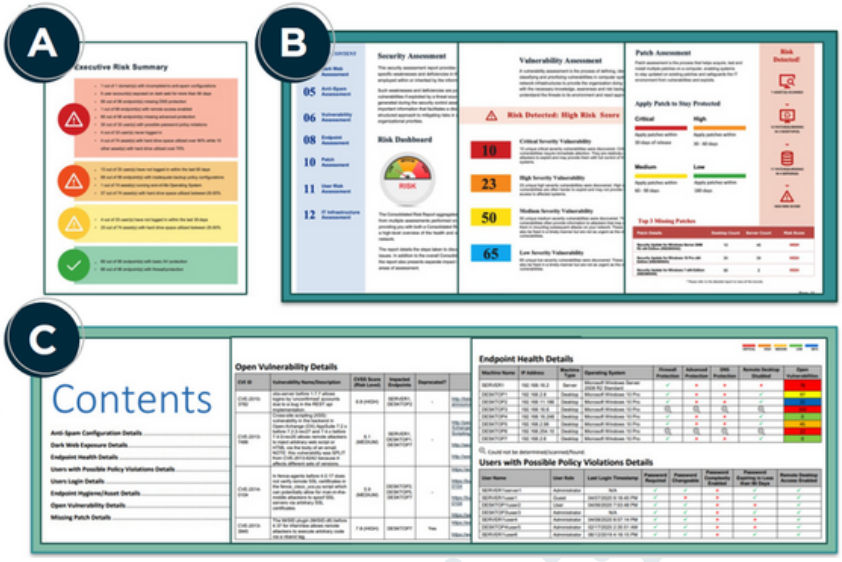
Often, breaches are only detected after it is discovered that compromised, sensitive information has been released or is for sale on the dark web.



Do you have Employee Credentials on the Dark Web

Running a dark web scan against an email domain can provide illuminating results.

For example, one organisation's email domain scan uncovered 30compromised emails, including the business owner's bank account login credentials. Keep in mind, this is just one example. There have been instances where several hundred or even a few thousand compromised emails have been found.



Sample Reports

Report A - Risk Summary
Report B - Assessments
Report C - Partner Report

Brushing up on password best practices

If your credentials have been exposed publicly, you can never use that password again. Once that password is part of a public list, especially one that is associated with your email address,you can be sure it will be used in a future attack.

The risk is too great to even consider using it again, and another account that uses the same password should be immediately changed as well. Similar passwords used with other accounts should be changed, too.

Cybercriminals will use your password in an attempt to gain access to other accounts like banking and social media. This is why business email addresses should NOT be used for non-business-related activities.

Separate passwords should be used for each site or application you use.

The results of a dark web scan will show if any of your employees may have used their business email for non-business reasons and had their credentials compromised, bringing unnecessary risk to your organisation.If you identify any of your users' credentials for sale on the dark web, take the necessary steps to remediate the situation and prioritise strengthening your security posture for the future.

That includes training your users on their role in defence of the organisation. While a clear dark web scan may provide peace of mind today,be sure not to develop a false sense of security. Instead, use the assessment to identify other potential vulnerabilities that require resolution.

Using a Dark Web scan as an early warning tool

Think of a dark web scan as a regular checkup with your doctor.

You may feel fine, but medical tests could uncover underlying problems. A dark web scan is just like the routine tests your doctor orders. It's one more way to understand the strength of your current cyber defence.

Additional tests, like a vulnerability scan, can further identify specific areas of weakness and recommend appropriate remediation.

01.

Discover

Assess current IT infrastructure, operational challenges, risks and opportunities for improvement.

02.

Deisgn

Create a tailored Managed IT strategy aligned to business goals, users and operational requirements.

03.

Deliver

Implement, support and continuously optimise performance through proactive management and strategic guidance.

WHO ARE WE

Pinnacle is a Managed IT and technology partner that helps SMEs modernise, secure and optimise how they work.

We bring together Managed IT, cybersecurity, cloud, communications, connectivity and automation services into one connected ecosystem, making it easier to manage technology, reduce operational complexity and improve business performance.

With a strong focus on long-term relationships and proactive support, we help organisations create secure, resilient and future-ready workplaces where teams can work productively and confidently every day.

Contact Details

www.pinnaclecos.co.uk
info@pinnacle-group.co.uk
02920 365 222

Xerox™ | Lexmark™ Global Accelerator Network
ADVANCED MANAGED PRINT SERVICES

Xerox™ | Lexmark™ Global Accelerator Network
SIGNATURE PARTNER
Platinum