



Visualising the invisible

Gain an instant view of vulnerabilities on your networks, applications and digital assets. Get the basics right to secure and reduce the risk to your business.

nccgroup[®]

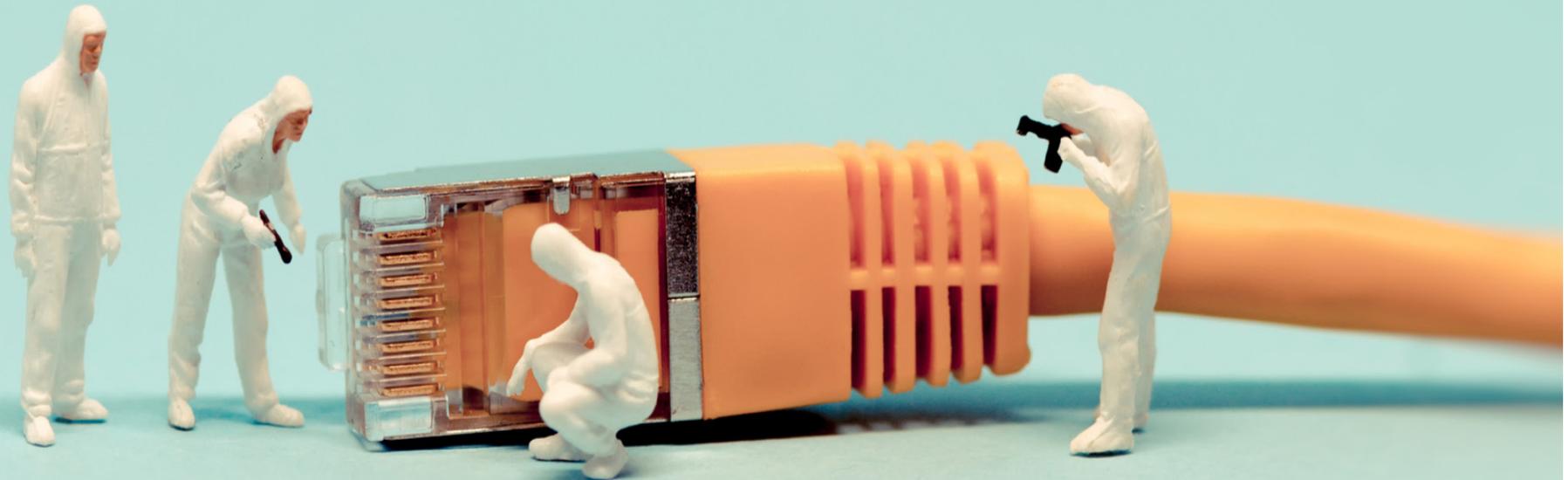
Finding vulnerabilities with attention to detail

Tens of thousands of endpoints, multiple networks, custom-written applications, billions of lines of code and blurred lines between public and private access.

These cause the biggest risk to today's businesses and can leave you overwhelmed.

From internal infrastructure to web applications, compliance and regulatory scans to a full distributed denial of service, our range of scanning services help business and organisations identify and resolve unknown vulnerabilities so they are more safe and secure to operate.

- **2 million vulnerabilities** found and remediated every year
- **4.5 million false positives** removed
- Over **400,000 out of date systems** identified in 2019
- Over **250,000 misconfigurations** made visible



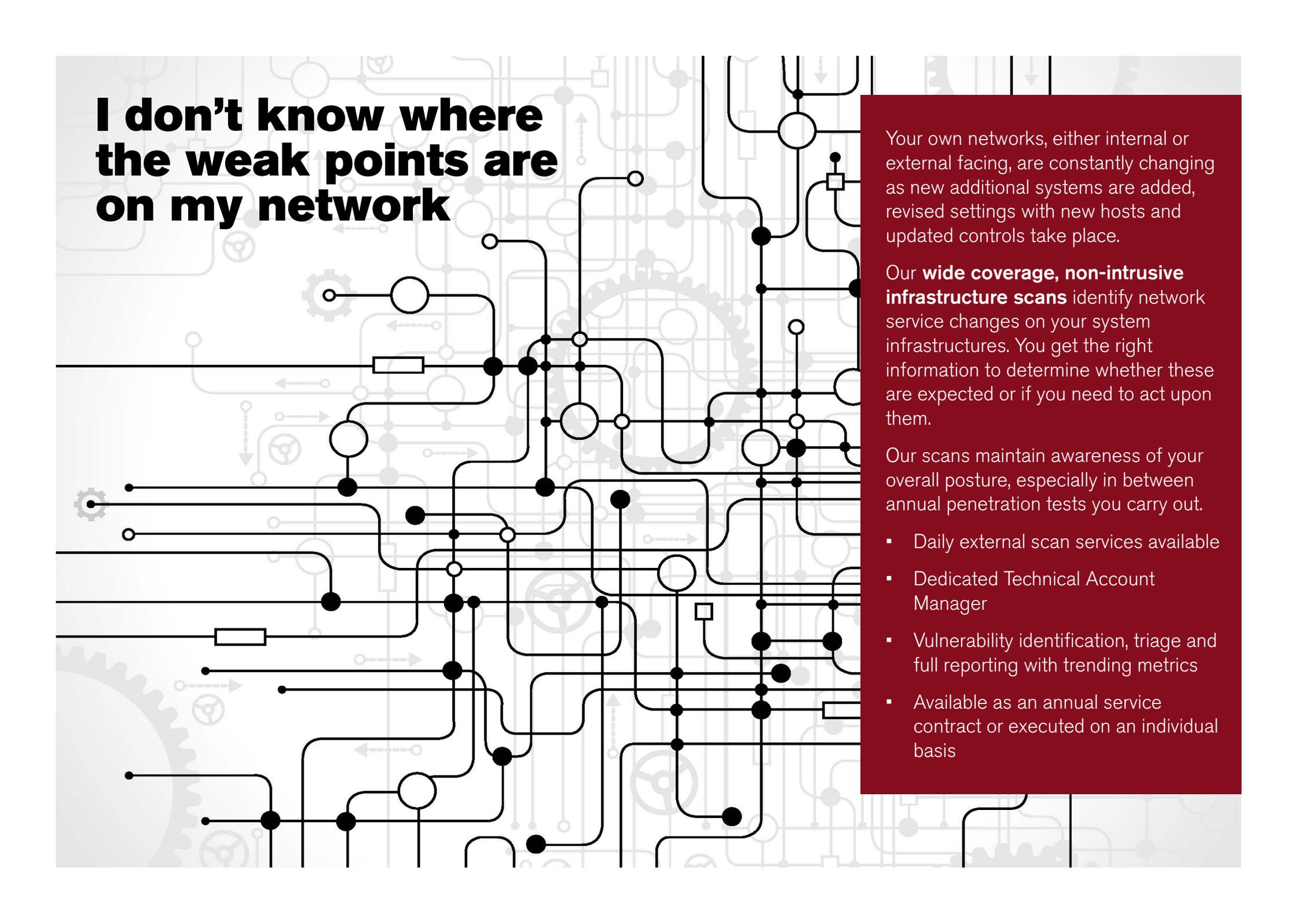
I need my web applications to keep my employee and customer data safe

As your business grows, so do the needs of your employees and customers. Web applications are fundamental to enabling a productive workforce and allowing customers easy access to your products and services. Stay in control and minimise the risks to external threats.

Our authenticated, in-depth **web application scanning** and testing supports you through all the key stages of software development. We use 'best of breed' scanning tools with high quality, experienced experts to test & verify the security of your applications.

- Identified over 60,000 web application vulnerabilities this year
- Process and logic application flaws
- Cross site request forgery
- Session fixation and management
- Username and password recovery methods
- OWASP Top 10 checks
- Full remediation advice and service





I don't know where the weak points are on my network

Your own networks, either internal or external facing, are constantly changing as new additional systems are added, revised settings with new hosts and updated controls take place.

Our **wide coverage, non-intrusive infrastructure scans** identify network service changes on your system infrastructures. You get the right information to determine whether these are expected or if you need to act upon them.

Our scans maintain awareness of your overall posture, especially in between annual penetration tests you carry out.

- Daily external scan services available
- Dedicated Technical Account Manager
- Vulnerability identification, triage and full reporting with trending metrics
- Available as an annual service contract or executed on an individual basis

A close-up photograph of a credit card. The gold-colored chip is on the left, and the embossed numbers '4511' are visible in the center. The background is a blurred blue and white gradient.

**I need to keep my
business
compliant and
customer's
credit card data
secure.**

All businesses must undertake at least a quarterly internal and external network vulnerability scan to comply with Payment Card Industry Data Security Standard (PCI DSS). This is essential should you change anything significantly on your network.

Our scan reduces the risk of a card holder data breach and provides you with peace of mind your business is PCI DSS compliant and operating securely.

Our **PCI ASV & Internal Scanning** achieves PCI Compliance with the guidance of an experienced and dedicated Technical Account Manager. We use vulnerability trending metrics to stay on top of new threats and developments in the industry.

- Remediation advice at all stages
- We are an Approved Scanning Vendor since the start of the PCI program.
- Performed over 7,000 scans for businesses

I need to demonstrate we protect ourselves from common online threats

Conducting regular vulnerability scans of your external systems puts your organisation in a stronger position to re-certify each year, by allowing you to identify and remediate critical findings regularly between assessments

Our CREST **Cyber Essentials** assessment conducts a certified vulnerability scan of all externally facing corporate infrastructure and web applications. This scan identifies any vulnerabilities which, if exploited, could result in the theft of sensitive corporate data.

- Work with industry leading consultants to achieve CE certification
- Assistance with remediation from a dedicated TAM
- Nationally recognized scheme
- Regular scanning and annual service available
- CREST Cyber Essentials Certificate for Stage 1 or Plus provided



I need my business to cope with high demands of online traffic

How do you know your online business can cope with high demand and serve your customers when they are under an attack?

Our **Distributed Denial of Service (DDoS) Assured service** assesses the coping mechanisms of your business, your DDoS mitigation and helps you prepare your defence strategy.

We have the ability to emulate a real life attack in a secure, controlled manner. We test all aspects of your business' ability to detect and respond to increased demand on your business network.

- Multiple traffic and attack types performed
- Delivered by dedicated technical consultants
- Stress level outcomes provided
- Sophisticated testing with controlled BOTnets
- Process and policy review
- Performed individually or on a regularly basis



I want to assess my applications before implementing them into my business

A person's hands are shown holding a white smartphone. The person is wearing a dark blue shirt and a black watch. In the background, there is a whiteboard with various diagrams, sticky notes, and a green pushpin. The diagrams appear to be flowcharts or process maps. The overall scene suggests a professional setting, likely a meeting or a presentation about software development or security.

When developing new software or applications, it's vital to test how secure they are before moving forward and implementing them. Leaving it to the last stage can result in it costing fifteen times more to fix than assessing earlier in the design stage*.

Our **Static Application Security Testing (SAST)** service uses market leading scanning technology combined with an experienced consultant to analyse application source code and binaries for coding in design conditions. Our service goes to the heart of the application, from the inside out, in a non-running state.

Full verification, analysis and remediation support provided by a dedicated Technical Account Manager

- Scan service supports your secure development lifecycle
- 23 programming languages supported
- Regular or individual scanning available

* IBM System Science Institute Relative Cost of Fixing Defects

Why NCC Group

We are a global expert in cyber security and risk mitigation, working with organisations the world over to protect their businesses against the ever-evolving threat landscape.

Through an unrivalled suite of services, we provide companies with confidence that their most important assets are protected, available and operating as they should be at all times.

Headquartered in Manchester, UK, with over 34 offices across the world, we employ more than 1,800 people and are a trusted advisor to 15,000 clients worldwide.

- Approved PCI ASV vendor
- Approved Cyber Essentials vendor
- Approved Distributed Denial of Service simulation vendor with Amazon Web Services (AWS)



Call (0) 161 209 5111

Email response@nccgroup.com

www.nccgroup.trust/vulnerabilityscanning