



# CNC Complete Security Protection

**Computer & Network Consultants Limited**

CNC House, Lady Bee Enterprise Centre, Albion Street, Southwick, Brighton, BN42 4BW

01273 386333 [sales@cnc-ltd.co.uk](mailto:sales@cnc-ltd.co.uk)

[cnc-ltd.co.uk](http://cnc-ltd.co.uk)

Registered in England and Wales Company No. 3105747

Classification: Confidential

ISO 9001 & ISO 27001 Certified



## CONTENTS

Contents.....	2
Executive Summary.....	3
Proposal.....	4
Core Services.....	5
Next Gen EndPoint Protection (All Services).....	5
Endpoint DNS Filtering (All Services) .....	5
Microsoft and Third-Party Patching (All Services) .....	5
Phishing Service (Not Lite) .....	6
Monthly External Vulnerability Scanning (WAN) (Not Lite).....	6
Monthly Internal Vulnerability Scanning (LAN) (Plus Service Only) .....	6
Cyber Essentials or Essentials Plus Certifications (Not Lite).....	6
DarkWeb & Risk Assessment Reports (Not Lite) .....	6
SSL Wildcard (Not Lite) .....	7
Proactive Firmware Updates (Not Lite).....	7
Workstation Disk Encryption (Not Lite) .....	7
Add-On Services .....	7
Security Information and Event Management (SIEM) .....	7
Penetration Testing.....	8
About Us .....	9



## EXECUTIVE SUMMARY

This proposal is aimed to significantly improve the overall delivery and management of IT security within the business.

This process has been driven by a variety of circumstances but the primary focus of this proposal is to ensure that going forward, the business reduces the risks of Cyber incursions from the outside world that could result in data loss or compromise.

There are some interesting facts regarding Cyber incursions that many business are unaware of:

**Dwell Time is the length of time a cyber attacker has free access in an environment before they are eradicated.**

- The average dwell time for ransomware is 23 days
- The average downtime for ransomware is 21 days

**Most data thieves are organized professional criminals deliberately trying to steal information they can turn to for financial gain.**

- 40% of ransomware incidents involve Desktop sharing software
- 35% of ransomware incidents involve the use of email with malicious links
- 62% of system intrusion incidents involve threat actors compromising business partners

**A human being is typically involved at the centre of most security events**

- 82% of breaches result from human elements
- 66% of breaches involve phishing or stolen credentials

Although nothing can 100% guard against malicious attacks, CNC's Complete Security Protection Services will help the business to reduce significantly the risks by introducing multiple layers of protection, using a variety of different techniques. This, coupled with staff behavioural training, by far offers the best protection.



## PROPOSAL

CNC can offer competitive services to augment or replace existing technologies such as Anti-Virus to provide a more proactive solution to Cyber Security.

Our Complete Security Protection Services are offered in conjunction with our standard support services portfolio of products as it's important that we have a full understanding and management of your network to provide a holistic approach.

The products comprise several key features, each of which is detailed below and coupled with some additional, optional services that can form part of a more comprehensive Cyber Security approach.

There are three key offerings, Lite, Standard and Plus based on your individual requirements.

	<u>Lite</u>	<u>Standard</u>	<u>Plus</u>
<b>EndPoint Protection</b>	✓	✓	✓
<b>DNS Filtering</b>	✓	✓	✓
<b>Application Patching</b>	✓	✓	✓
<b>Phishing Testing and Training</b>		✓	✓
<b>Vulnerability Scanning</b>		External	Internal & External
<b>Cyber Essentials Accreditation</b>		✓	Plus
<b>Dark Web Monitoring</b>		✓	✓
<b>SSL Wildcard</b>		✓	✓
<b>Firmware Updates for CE</b>		✓	✓
<b>Disk Encryption</b>	✓	✓	✓

Before we implement any service, we'll ask you to complete a questionnaire and provide you with a risk assessment that will highlight any areas of the business that are potential hot zones for security weaknesses.



## **CORE SERVICES**

### **NEXT GEN ENDPOINT PROTECTION (ALL SERVICES)**

As we have stated, human action causes 82% of security events and when a breach occurs it's rarely detected until it's too late because the threat actor has already been in your systems for an average of 23 days., so called Dwell Time.

Therefore, keeping this Dwell Time to an absolute minimum is essential in stopping attackers in their tracks.

Our "always-on" endpoint defence service delivers enterprise-grade threat detection, incident response, remediation and the benefits of a dedicated 24x7 Security Operations Centre (SOC).

No matter where your staff are working, or what time, with our managed endpoint detection and response service, your environment is continuously monitored for not only the traditional virus & malware threats but also the very latest Behavioural Artificial Intelligence, Lateral Movement around systems and internal behaviour, i.e. your employee trying to do something untoward.

Designed to rapidly identify the root cause of a threat, when malicious behaviour is detected, immediate response and remediation measures are initiated on the device in question, including disconnect, quarantine or roll back to an acceptable no-risk state. Threats are therefore contained before they can do harm and you stay operational.

This service typically replaces standard anti-virus software.

### **ENDPOINT DNS FILTERING (ALL SERVICES)**

Post COVID, the working world has changed and the traditional enterprise grade-firewall protection is great for those people in the office but for those that are taking company equipment to work from home, an additional solution is needed.

Domain Name System is the backbone of networks and converts a new human readable address, such as [www.google.co.uk](http://www.google.co.uk) into an IP address, such as 172.217.16.227, that computers can understand and process.

Our solution blocks access to malicious websites or destinations and filters out harmful or inappropriate content so you can be sure your employees are protected no matter where they are working.

### **MICROSOFT AND THIRD-PARTY PATCHING (ALL SERVICES)**

One of the most common exploits into and around systems is by out of data software so it's important to keep this up to date and run a supported version from the vendor. Quite often ad-hoc software will be installed on computers for a specific task but then left there, which is then a risk waiting to be exploited.

This service offers automatic updates for Microsoft applications and over 120 others, including some of the most common ones in use such as Adobe Acrobat, Chrome, Firefox, Skype, and



Zoom. It's also configured to remove known risks such as peer to peer sharing software and out of data versions of Java.

### **PHISHING SERVICE (NOT LITE)**

With 35% of ransomware incidents involving the use of email with malicious links, this is a major path of potential incursion to the business. To help educate users and minimise that risk, CNC will setup an annual campaign comprising 12, separate, monthly phishing tests on pertinent subjects to send to each member of staff. Then afterwards we'll send out training to people to help them to help raise awareness of the risks, what to look for when dealing with emails and how to avoid becoming a victim. These will be run at random times throughout the month/year and a monthly report of users who have taken action will be provided to a nominated contact within the customers' organisation.

### **MONTHLY EXTERNAL VULNERABILITY SCANNING (WAN) (NOT LITE)**

A monthly scan of your Internet facing services will be undertaken, the results reviewed and any appropriate action taken. This uses the very latest information about vulnerabilities and exploits so you know that you're always going to have the clearest picture of your public facing assets.

### **MONTHLY INTERNAL VULNERABILITY SCANNING (LAN) (PLUS SERVICE ONLY)**

Building on the external scanning takes it to the next level and all internal systems on your office network will face the same scrutiny and action, ensuring that risks are dealt with and you're protected.

### **CYBER ESSENTIALS OR ESSENTIALS PLUS CERTIFICATIONS (NOT LITE)**

These are fast becoming the 'norm' for taking your company's cyber security seriously and obtaining Cyber Insurance. It can be an arduous task to obtain these by yourself because this isn't just a tick exercise, the assessors need a lot of proof but depending upon the level of CNC's Security Protection service taken out, we will ensure that you attain these accreditations annually as part of the managed service costs.

### **DARKWEB & RISK ASSESSMENT REPORTS (NOT LITE)**

The DarkWeb isn't as dark as it once was and now it's possible to search and find out if your company email addresses have had their credentials compromised, bringing unnecessary risk to your organisation.

You might also use this to keep an eye on any critical parties in your supply chain to make sure their problems don't become your problems.

Coupled with this, we will take you through a high level risk assessment to help identify not only technical areas for improvement but also business processes too because as you know, a lot of the time the weak link in security is the human factor.



### **SSL WILDCARD (NOT LITE)**

Encryption isn't just used by bad guys, it's been protecting websites and communications for years. Most websites you visit are now secured by a trusted certificate and you'll see a small padlock in the browser to prove it. We will provide you with a free wildcard certificate as part of this service which means you can protect any device or system that's typically public facing. For example if you have a remote access server in the office or a firewall you connect to using a VPN, they would both be protected by this.

### **PROACTIVE FIRMWARE UPDATES (NOT LITE)**

Just like the software patching, all physical devices run on software and this is called firmware., which are just as open to vulnerabilities and exploits if they aren't kept up to date. The photocopier in the corner of the room might look brand new but when was it scanned last to make sure it doesn't have any known exploits?

This service works in hand without vulnerability scanning so any key network device will be patched as required to meet Cyber Essentials requirements.

### **WORKSTATION DISK ENCRYPTION (ALL SERVICES)**

All Windows 10/11 workstations will, where the hardware supports it, be encrypted using Microsoft Bitlocker to prevent unauthorised access to hardware drives should they be removed from the computers. We can also bolster protection with a Power On password should you wish to go that stage further.

### **ADD-ON SERVICES**

The following additional services may be procured in addition to our monthly service.

#### **SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)**

Pronounced 'seam', this service is designed to consolidate and review log information from all your key systems, look for suspicious or unusual behaviour and then act upon it. Once again, this is managed by the dedicated 24x7 Security Operations Centre (SOC) who are constantly monitoring for threats to your business.

It integrates with many different systems, some of which are AWS Cloud Trail, Cisco Duo, G Suite, Microsoft 365, Microsoft Teams, Sales Force, Slack and our Next Gen Endpoint client.

You may need this service if your Cyber Insurance insists on keeping log information for a specific period of time or if you need the ability to 'replay' events after they happened to trace back potential cyber attackers and see the cause of any incursion.



## **PENETRATION TESTING**

A penetration test, also known as a “pen test” or “ethical hacking”, is an authorised, simulated cyberattack on a computer system designed to evaluate the security of the system.

Unlike a vulnerability assessment, this actively tries to breach systems by exploiting weaknesses but with no malicious results. A full report is provided detailing if / how access was gained, and the steps needed to strengthen the security and prevent it from happening for real.

This is not normally a requirement of Cyber Insurance or Cyber Essentials but we are seeing more companies who are insisting that you have this performed at least once a year before they will deal with you.



## ABOUT US

Established in 1996, Computer and Network Consultants (CNC) deliver IT infrastructure services to an established client base, many of which have been working with us since our first year of trading.

In 2023 CNC became part of the Fluid One group of companies and is now part of a £104 million nationwide business but still continuing to deliver to local businesses, leveraging all the benefits of being part of the larger group.

CNC currently has around 200 clients, for many of which we act as the IT function and strategic partner to allow the business to provide their users with an outstanding IT service, deploying the very latest technologies using up to date best practices.

For most organisations, the IT infrastructure is essential to the day to day operation of the business, driving and facilitating business processes. CNC work with our business clients to 'Refresh' their networks to ensure IT policy is aligned with business strategy and maximise investment in technology.

Our focus is on the human interaction with IT services for people with all different levels of IT understanding, allowing us to work with the senior management team to create an experience that suits these different types of individual but with a commercial awareness not always available to an internal IT team.

This can mean looking at things differently to how you've been used to and leveraging existing services, hardware and human resources in the most cost-effective way but also one that suits the ethos of the business.

We have undertaken a similar journey that you are embarking on for many other customers, to which you are welcome to speak to and gauge their experience of CNC.

We provide a unique service, with no sales people to speak of, instead relying on people with both commercial and technical know how to work with customers to put in the right solution, not the most commission rich.

We have a team of over 45 technical people to provide support from 7:30am to 8:00pm and 24x7 cover available if required, with many of our staff having worked within CNC for over 10 years.

On top of this, we are an accredited **ISO 9001**, **ISO 27001** and **Cyber Essentials Plus** organisation, to give you the peace of mind that the service will be to a high standard and interaction with your systems is secure, not something many organisations have.

We achieved the Investors in People award in 2022 and strive to provide a good working environment for our team allowing people to develop within the business. Many people have started at junior positions and worked their way into Team Lead/Management.

All in all, we will be a good, strong partner of your business and look to forge a long-term relationship with you.



Endpoint Protection



Microsoft Azure Consultancy



Specialist Disaster Recovery



Bespoke Software Design



Business Broadband Services



Cloud & Hosting



Cyber Security Training



Email Archiving



IT Hardware & Software



IT Infrastructure Consultancy



Microsoft 365 Solutions



Offsite Data Backup



Outsourced IT Support



Patch Management



Remote Working



IT & Cyber Security



Telephony & VOIP Solutions



Switching IT Support Partners



Apple Mac Support



Managed IT Service Provider