NODE4

Technology Enabled Outcomes

SECURITY PRODUCT PORTFOLIO

INTRODUCTION

Experts advocate a multi-layered approach to cyber security, avoiding the tendency to rely on any one product or solution. Each strategy should be effectively managed and overseen through the existence and constant application of policies, governance and compliance.

Node4 seeks to encourage its clients to put greater emphasis on preparation, not simply reaction. Our range of solutions are both standalone and complementary, providing a holistic solution that's set to the most common of cyber security attacks, whilst simultaneously improving your overall cyber security posture.

At Node4, our experts practice security discipline every day, and as a result, deliver outcomes faster and to higher quality than a generalist inhouse deployment. This delivers a better ROI and quicker timescales.

Our VCISOs and SOC analysts work with an extensive list of organisations, giving them visibility of a wide range of attacks and vulnerabilities. We then take the lessons and learnings from them to support all our security clients.

PREPARE

CONSULTANCY

VCISO (Virtual Chief Information Security Officer): Our Virtual CISO is designed to become part of your team, giving pragmatic and structured advice on your security posture.

They can discuss cyber insurance, help with and create Business Continuity and Disaster Recovery plans, guide on NIST and other compliance standards, and look with a critical but independent eye at your security architecture, making appropriate recommendations.

They will recommend partners that provide the best fit for your environment, even if not in Node4's portfolio. The VCISO will manage the Node4 security relationship, and if you wish, manage your other security partners.

GOVERNANCE, RISK AND COMPLIANCE

By using Node4 and partner experts with vast experience with multiple compliance standards, we are able to provide faster, more reliable and improved ROI, helping you to meet your compliance needs and aspirations.

Cyber Essentials: A requirement in most instances for supplying to Government, as well as simply being viewed by the industry as a 'best practice' guide to good cyber security. Node4 experts, with their first-hand experience, together with their IASME certified partner, will guide you through to successful Cyber Essentials or Cyber Essentials Plus certification.

Compliance Management: Compliance should not just be an exercise in box ticking. With access to national and international security frameworks and standards, including ISO27001, NIST, CIS controls, and PCI DSS, this SaaS enables you to implement, self-assess and manage your ongoing status against key frameworks.

DORA: Known as the Digital Online Resiliency Act, DORA is the regulation that impacts UK finance sector and its suppliers. Although not all UK firms are subject to the EU's DORA, it presents a valuable framework for all businesses seeking to safeguard their assets, reputation and clients, while also positioning themselves for growth.

Our consultants will give timely and pragmatic advise on DORA compliancy and related security controls. Importantly, we can also give a rapid assessment on the relevancy of DORA to your organisation.

IDENTIFYING THREATS

Spot issues before they arise, whether that be with testing, training, assessments or intelligence sources.

Vulnerability Scanning: Automated and manual scans of your infrastructure that test the resilience of your defences are carried out, giving you visibility of exactly what criminal hackers can see. By assessing your risk exposure and identify weak spots that need attention, it allows you to act quickly to fix them before they are found and exploited.

Penetration Testing: The next step on from vulnerability scanning. There are many types of penetration test, but this is in effect an authorised simulated cyberattack on your computer system. It's designed to evaluate the security of the system and identify weakness that an unauthorised parties could use to gain access to its features and data. The testing procedure is conducted by our CREST certified team.

Ethical Hacking: This is the practice of testing a computer system, network or application to find security vulnerabilities that could be exploited by malicious hackers. The techniques are the same, but unlike malicious hackers, our CREST certified team do so with your permission. They will test the ability of criminals to move across and through your infrastructure.

Dark Web Scanning: Cyber criminals operate like businesses - there are customers and there are suppliers, buying and selling data or skill sets, and they communicate and transact on the dark web. Working with partners who are specialists in the dark web, it's possible to read these signals and interpret if an attack on your infrastructure is in the reconnaissance and planning phase. That then provides actionable outputs to keep you one step ahead of the criminals.

Phishing Testing and Training: Training is an important addition to tools such as PDNS and Zero Trust architecture. This service runs phishing tests against your organisation, followed by automated tailored training on a per-user basis. Every user will respond differently, which is why a set of pre-programmed training packages exist. They can be deployed depending on how users respond to inbound phishing tests.

INFRASTRUCTURE SECURITY

Providing a range of platforms and technologies backed by SLAs and hosted in Node4's high availability datacentres and the cloud, ensuring that you don't need to worry about uptime and infrastructure resilience.

Endpoint Security: This provides end-point virus protection and integrates with our SOC, where appropriate. We help you to build suitable images for your devices and collate logs and data from the AV surface.

DMARC: This prevents your emails from being spoofed and protects your brand from reputational damage. In this service, we help you to configure and manage your DMARC configuration and support you through the journey from 'None' to 'Reject'.

Additionally, using client aggregated DMARC RUA reports, Node4 can produce a list of common IP addresses that are the source of spoofing and phishing emails, and use them to enhance existing threat intelligence to the benefit of all our security clients. Our commitment is to pass all threat intelligence to law enforcement or other bodies who can affect take-down of criminal infrastructure.

Email Security: Node4 provides a managed email service that scans for inbound malware and suspicious links, integrating with PDNS and DMARC services.

DEFEND

THREAT MANAGEMENT

Threat Detect: Our Managed SOC and SIEM service, powered by Microsoft. Our 24*7 service monitors your infrastructure and alerts our support teams when anomalies are spotted. The SOC is the hub for Node4 threat intelligence, collating, analysing and then acting on that intelligence for the benefit of our clients. As well as a core service, we can work with your SOC or Analysts to provide an augment to your own capability or a support function. We work constantly to improve the proactive threat intelligence within the SOC, aiming to stop attacks before they impact our clients.

NETWORK SECURITY

A range of services that connect to your Node4 network and cloud infrastructure, ensuring the security of the perimeter of your estate and protecting the users and assets within.

Managed Firewall: Our Managed Firewall service ensures the security of your network perimeter through proactive monitoring and maintenance. Our network and security experts work to identify and resolve issues, intervening proactively so your networks remain up and operational.

Our software vulnerability management, threat intelligence and policy configuration audit services are available for added assurance. Our service optionally ensures that your firewall protection has intelligence gathered by our SOC.

PDNS: A protective DNS that stops your users from getting to any of over 5 million known current malicious or criminal domains, including Malware C2 (command and control) domains.

DDoS Protection: Despite the rise in sophisticated malware attacks, DDoS attacks are still on the rise and a tool used by many criminals. Our automated, always-on and scalable DDoS mitigation service identifies and discards malicious traffic, while legitimate traffic is forwarded as normal. We deliver this in a simple and transparent offering for a fixed monthly fee.

Secure Web Gateway: Our Secure Web Gateway solution delivers consistent endpoint security, regardless of user location. Using a cloud-delivered model, benefit from advanced web protection, without the need to transit your internal physical security appliances. This ensures your users remain safe and productive while working from anywhere.

Secure SD-WAN: Our secure managed SD-WAN service keeps your team members connected and protected, wherever they choose to work. It continually prioritises traffic flows to optimise the experience for every user.

This software-defined network solution also has integrated advanced security to connect the distributed Enterprise and seamlessly protect every edge. SD-WAN also has the advantage of easy reconfiguration in the event of an attack or a disaster scenario.

Web Application Firewall: With an ever-expanding attack surface, more complex threats, and increasingly persistent attackers, it's a challenge just to stand still. Coupled with application sprawl across the multi-cloud, it's become exceptionally challenging to deliver high-performing and secure web applications.

Our WAF solution simplifies these challenges, through cloud-delivered and cloud-native content delivery and application security, packaged and delivered as a simple managed service.

ZERO TRUST

Moving to a zero-trust position assumes that all devices are hostile, which then gives layered and segmented defence against an attack that has breached your external perimeter.

Privileged Access Management: Controls admin accesses and role-based access control.

Network Access Control: Ensures that rogue or infected devices are prevented access or quarantined, awaiting recovery.

Zero Trust Network Access: Creates an identity and context-based logical access boundary around an application or set of applications.

Cloud Access Security Broker: On-premises or cloud-based software that sits between cloud service users and cloud applications, monitoring all activity and enforces security policies.

Secure Remote Work: Allows your staff to work securely remotely, including VPN and authentication technology.

RESPOND

INCIDENT RESPONSE

The “999” emergency line you call if the worst happens. Working with our partners, we will help you to contain and manage the incident, restore your environment and remediate as required. And, where necessary, we assist with threat actor engagement. Additionally, you’ll receive support including advice on notification obligations and media engagement. The service is available to everyone on a retainer or on-demand. The benefit of the retainer service is a lower hourly rate of prepaid pool of guaranteed support hours, which you can draw down in the event of a cyber incident, and also convert to other partner services in support of obtaining cyber insurance or incident preparedness.

DATA PROTECTION

Helping you to secure and recover your data after an incident.

Immutable Backup Storage: Allows your backups to be secured from ransomware and gives a known secure state to recover from. This also includes ERP data security and restoration.

Disaster Recovery as a Service: Our DRaaS solution allows an organisation to back up its data and IT infrastructure in our cloud computing environment, alongside enabling the user to regain access and functionality to IT infrastructure after a disaster.

Backup as a Service: Our BaaS solution provides virtual machine-level backup and supports N4Cloud based virtual machines by enabling backups to be completed, without affecting the operation of virtual machines.

Data Loss Prevention: DLP is a complex subject and requires expert configuration, but provides an excellent level of protection against accidental and malicious data export.

PARTNERS

We work with best-in-class partners to ensure we deliver the best for our customers.

Node4 Ltd Registered in England No. 04759927 VAT: 192 2491 01
Registered Address: Millennium Way, Pride Park, Derby DE24 8HZ
T: 0345123 2222 **E:** info@node4.co.uk
www.node4.co.uk