DATA SHEET

N4 BRAND PROTECTION

PREDICTIVE AND PROACTIVE BRAND PROTECTION

YOUR BRAND IS EVERYTHING. IT'S HOW YOU'RE KNOWN, IT'S WHAT BRINGS NEW BUSINESS, IT'S WHAT MAKES PEOPLE WANT TO WORK FOR YOU. WHAT HAPPENS IF THE REPUTATION OF YOUR BRAND IS DAMAGED? TRUST EVAPORATES, REPEAT REVENUE DROPS, NEW CUSTOM REDUCES, ALL OF WHICH WILL HAVE SIGNIFICANT IMPACT ON YOUR ORGANISATION'S FINANCIAL STABILITY AND ABILITY TO DELIVER.

Phishing is the key driver of cybercrime and fraud – but there are numerous other criminal activities that can be carried out through malicious domains, putting your organisation at risk of cyber attack. These include:

- Malware Distribution
- Command and Control (C&C) Servers
- Drive-By Attacks
- Fake Software Updates
- Pharming
- Spamming

Prevention is the best cure. At Node4, we want to support our clients to reduce the risk caused by malicious domains and empower them to be proactive in tackling the threat.

We've partnered with BforeAI to deliver a predictive and proactive brand protection solution. Using their patented AI technology, our partners can predict the likelihood of a new domain being created for malicious purposes. Their threat intelligence feed has an impressive <0.05% false positive rate. Being able to anticipate a threat, coupled with the ability to neutralise it, is a significant step in protecting your organisation and brand.

Node4 offers two independent but complementary Brand Protection services:

KEY BENEFITS

PREDICTIVE AND PROACTIVE PROTECTION
Brand Protection that provides the ability to not merely protect your organisation and your customer from attack, but to neutralise the threat.

RELIABILITY AND PRECISION
Continuously replication runs without using disk snapshots, ensuring you have the most recent version of your data without negative impact on your production environment.

SPEED

- Identification of threats from impersonation 96 hours ahead of other brand monitoring vendors.
- In under 60 mins, 65% of network traffic blocked to malicious domain.
- 90% of takedowns completed in under 24 hours.

PERSISTENCE
If a registrar ignores or declines requests to take the domain down, 10 further attempts are made with the provision of further evidence to persuade them to do so – and all the while, the domain is blocked.

NO TAKEDOWN, NO CHARGE
If a domain isn't taken down, you're not charged.

1. BRAND MONITORING AND ALERT

Our partners monitor their AI-powered predictive threat intelligence feed to identify squatting domains that could potentially impact you or your customers and alert you to their existence. This enables you to keep one step ahead of the criminal and informs your next move, such as blocking it on your estate or requesting the takedown of that domain.

2. DISRUPTION AND TAKEDOWN

Building on Brand Monitoring and Alert, two things happen: traffic disruption and domain take down. You can choose to assess the threat first or automatically request a takedown of the malicious domain. And in parallel to the takedown, the domain is blocked, suppressing any incoming traffic to that domain. This neutralises the ongoing threat. But the service doesn't stop there. Once a domain is taken down, the infrastructure is monitored for 90 days to ensure it isn't spun back up.

Rather than react to a threat, get ahead of the criminal with our Brand Protection service.