indeEDR

GET INTELLIGENT ABOUT SECURITY

Having an Endpoint Detection and Response (EDR) capability has become an essential security component for any organisation in New Zealand.

Keeping your environment secure is increasingly complex and expensive, but it doesn't need to be. IndeEDR is a comprehensive, fully managed EDR-as-a-service solution that provides centralised visibility and correlation across both your corporate endpoints as well as server infrastructure.

IndeEDR allows you to gain all the Endpoint Protection Platform (EPP) benefits including unified prevention, detection, and response in a single purpose-built agent. IndeEDR provides prevention and detection of attacks across all major vectors, rapid elimination of threats with fully automated, policy-driven response capabilities, as well as providing complete visibility into the endpoint environment with full-context, real-time forensics.

IndeEDR utilises the latest in machine learning technology, removing the reliance on traditional antivirus signatures for malicious content analysis. By removing the heavy dependence for frequent antivirus updates, your internal IT team is awarded significant cost savings while also mitigating previously unseen threats.

Product Highlights

STATIC AI

THREAT HUNTING

DEVICE CONTROL

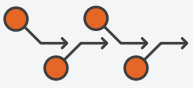
THREAT FEEDS

BEHAVIOURAL AI

REMEDIATION

APPLICATION INVENTORY

AUTOMATED ANALYSIS



LATERAL MOVEMENT

CONTAINMENT & ROLLBACK

VULNERABILITY & PATCH MANAGEMENT

SHARED INTELLIGENCE

indeEDR

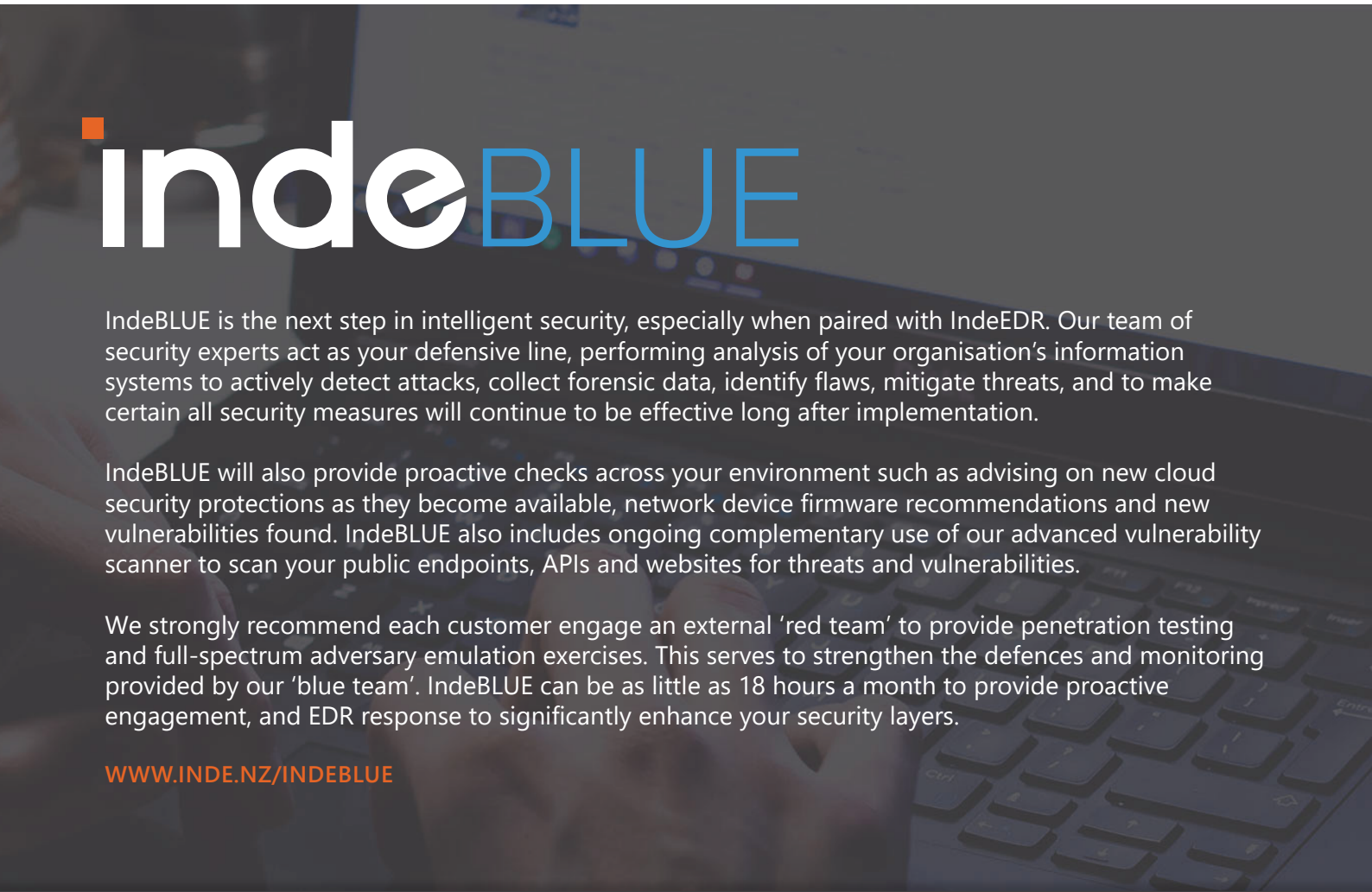
Why Inde?

Put simply, Inde strive to hire the best, and we heavily invest in training to keep our experts at the top of their field. With IndeEDR you can significantly improve your security posture, without the challenge of having to recruit and train specialised IT personnel in-house. Inde have experts across networking, cloud and application delivery who can translate events into meaningful analysis and remediation.

Why IndeEDR?

Developing strong forensic capabilities is the next evolutionary step in security, blocking threats isn't enough – our customers want to know where the threats have come from and what they tried to do inside their environment. Cross-platform visibility into endpoints combined with the ability to auto isolate infected devices as they are detected significantly reduces the impact to your organisation.

IndeEDR takes the hard work and ongoing management away with proactive identification of malicious intent within your organisation at a cost-effective price point per endpoint.



indeBLUE

IndeBLUE is the next step in intelligent security, especially when paired with IndeEDR. Our team of security experts act as your defensive line, performing analysis of your organisation's information systems to actively detect attacks, collect forensic data, identify flaws, mitigate threats, and to make certain all security measures will continue to be effective long after implementation.

IndeBLUE will also provide proactive checks across your environment such as advising on new cloud security protections as they become available, network device firmware recommendations and new vulnerabilities found. IndeBLUE also includes ongoing complementary use of our advanced vulnerability scanner to scan your public endpoints, APIs and websites for threats and vulnerabilities.

We strongly recommend each customer engage an external 'red team' to provide penetration testing and full-spectrum adversary emulation exercises. This serves to strengthen the defences and monitoring provided by our 'blue team'. IndeBLUE can be as little as 18 hours a month to provide proactive engagement, and EDR response to significantly enhance your security layers.

WWW.INDE.NZ/INDEBLUE