ENCRYPTED TRAFFIC VISIBILITY

ADVISORY PAPER AND SOLUTION OVERVIEW

Our unique platform works with your existing infrastructure to deliver instant analysis, detection and response to cyber threats within your encrypted traffic.

THE ENCRYPTION SECURITY CONUNDRUM

The evolving cyber threats your business faces every day are well publicised. From ever more sophisticated malicious attacks and insider threats, to poorly configured infrastructure and simple employee error. Each one of these brings the real risk of brand, financial and reputational damage.

These high-profile issues have driven a reaction from organisations and governments around the world. Bringing privacy demands and new regulations that have resulted in around 90% of today's data traffic being encrypted. The growing adoption of TLS 1.3 means that decryption will no longer be a security option, and the demand to both achieve compliance and avoid fines brings a whole new set of challenges to every business.

Just as encryption is seen as a tool to protect data, cyber criminals also see it as an opportunity to steal it. Hackers have learnt to leverage encryption to hide malware inside encrypted traffic. Current estimates suggest that over 60% of cyber threats are now hidden inside encrypted traffic flows.

Governments and Financial institutions are particularly at risk here, as the spate of recent Calypso and Gozi attacks has shown.

Around 90% of today's data traffic is encrypted

Around 80% of cyber threats are now hidden inside encrypted traffic flows

"The value of your current cyber defences are decreased significantly through data blindness"

– Gartner

EXISTING DEFENCES ARE POWERLESS

Your current cyber security technology will have been developed to inspect your data, detect threats and alert you to action needed. However, whether perimeter, behavioural, SIEM or standard firewalls, these technologies can only inspect unencrypted data. In the words of Gartner, "The value of your current cyber defences are decreased significantly through data blindness".

The financial implications are significant; whether in the cost of lost investments in cyber security infrastructure that needs to be replaced, the significant efficiency drain of decrypting (if allowed) all data for inspection, or the pressure on your SOC and IT teams from a deluge of false threats. It would be a costly slow down in every way.

THERE IS A SOLUTION

Barac Encrypted Traffic Visibility provides a way to future-proof your compliance, deliver ROI on your existing cyber infrastructure and improve the efficiency of your encrypted business.

OUR UNIQUE PLATFORM

The Barac Encrypted Traffic Visibility platform gives your business true visibility of inbound and outbound SSL/TLS traffic without the need for decryption, using traffic flow and packet metadata to expose threats and stop attacks in real-time.

Our proprietary AI software combines machine learning and behavioural analytics to deliver early detection of threats, and quickly learn the "normal" working processes of your business, allowing the Barac platform to instantly recognise any changes to that pattern that may carry risk.

HOW THE BARAK ENCRYPTED TRAFFIC VISIBILITY PLATFORM WORKS

We achieve our high protection rates (99.99%) and deliver efficiency by using metadata to score encrypted traffic flows. We are platform agnostic, so cloud, on premise or hybrid. Your encrypted data is gathered by our collectors which extract metadata that is sent securely to the Barac platform for real-time analysis. Using machine learning and advanced behavioural analytics we identify known attacks, abnormal traffic and infected beaconing.

Alerts are sent via API to your cyber teams via an easy-to-use web interface, direct integration with your existing SIEM platform or straight into your SOC. We have proved that using the Barac platform reduces costly false positives in encrypted data by over 99%. In addition, these dataflows can be terminated or re-routed through defined service maps, allowing for optimal use of existing expensive network and security equipment.

REAL TIME AND SCALABLE

The unique use of metadata, powerful AI and advanced threat intelligence means that we detect attacks in real time. The Barac platform can manage millions of connections per second just by adding new virtual machines. So, as your traffic scales, your security will too.

SIMPLY ADD BARAC TO YOUR EXISTING CYBER INFRASTRUCTURE

With the Barac Encrypted Traffic Visibility platform there's no need to replace your existing cyber technology. Our solution is vendor agnostic – we can rapidly integrate with your existing infrastructure to deliver protection across all your encrypted and unencrypted data.

In fact, it is so easy to implement and so efficient in delivering protection that we'd be happy to provide you with a free trial. This will demonstrate just how quickly and cost efficiently you can protect your business.

Key benefits of using the Barac Encrypted Traffic Visibility platform

SECURITY

- Expose hidden threats without decryption
- Detect abnormal traffic
- Detect in real time
- Integrate with SIEM/SOC

COMPLIANCE

- TLS 1.3, FIPS, GDPR compliant
- No need to decrypt HTTPS traffic
- Crypto-compliance monitoring improved

ROI

- Maximise security investments
- Improve efficiencies & false positive reductions
- No traffic slowing for decryption

Rise Building, 41 Luke Street,
London EC2A 4DP

+44 7555 684 074

barac.io