Comprehensive Network Protection

Detect. Prevent. Hunt

Features & Benefits

- **Full Network Visibility**
  Provides enterprise-wide visibility and remote location defense

- **Automated Threat Detection**
  Convicts on basis of signatures, stateful anomalies, and AI-based file assessments

- **Enriched Alerts**
  Delivers alerts with critical enhanced data to understand the full scope of the problem

- **Reduced Time to Containment**
  Up to 80%-time reduction with instant access to critical details

- **Ease of Use**
  Intuitive and productive UX that eases transition from known threats to unknown malicious activities

- **Flexible Deployment**
  Physical and virtual options that scale to your environment

Network threats are business threats. You rely on your networks to run your business and to interact with your customers. Networks carry valuable business transactions and sensitive customer information. Hackers are relentlessly trying to monetize them both via currency, credit, and identify theft and through business disrupting ransomware. Adding to the challenge is the complexity and random growth of today's networks driven by business demands that can provide hackers with hiding places from which to attack.

To protect your business, you must protect your network. From unparalleled visibility to automated full-spectrum threat detection to true threat hunting, Bricata protects your network with a single, integrated, easy-to-use system.

Designed and developed by experienced network security professionals, Bricata delivers a complete suite of best-of-breed network security capabilities integrated to work together seamlessly as a single technology with a mission focus of providing comprehensive network protection. Bricata's intuitive and productive user experience reduces otherwise complex and tedious tasks to simply requesting the results that are desired rather than specifying how to obtain them from one or more technologies.
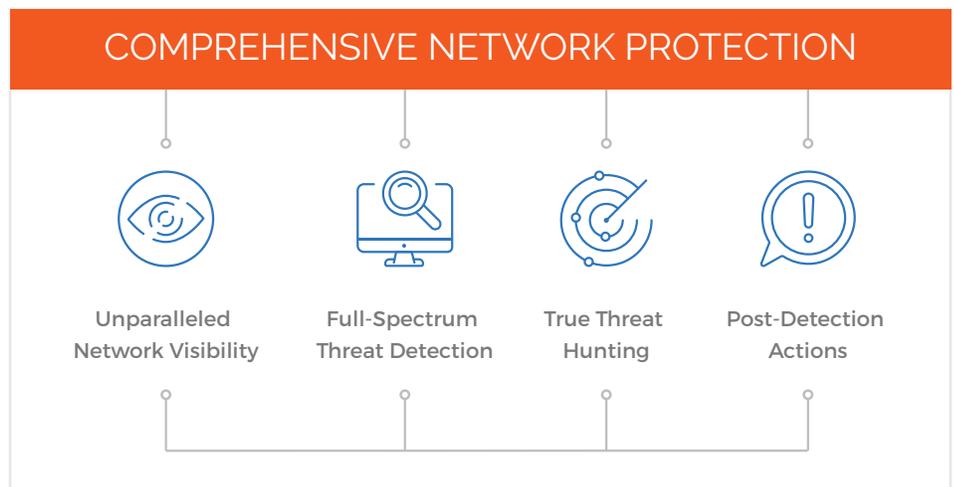
COMPREHENSIVE NETWORK PROTECTION

Unparalleled Network Visibility	Full-Spectrum Threat Detection	True Threat Hunting	Post-Detection Actions

Unparalleled Network Visibility

To protect your network, you need to see and understand everything that's happening on it. Bricata's foundation for network visibility is the network traffic itself, packets/PCAPs. PCAPs provide a 'perfect fidelity' recording of your network, but their volume, repetition, and transmission-level datatypes make them tedious to use for regular visibility. Bricata generates rich network metadata that provides meaning to PCAPs, but also greater detail than NetFlow, to facilitate not mere visibility, but deep understanding of what is happening on your network. Bricata enables drill-down from metadata to PCAPs to give you both network comprehension always and detailed 'perfect fidelity' visibility when you need it.

Full-Spectrum Threat Detection

As much as you might want to personally inspect every packet that comes onto your network for threats, it's just not possible—there's too much and it's coming too fast. Automated threat detection is required, but which method is best: signature detection, stateful anomaly detection, or zero-day malicious file detection? Bricata's full-spectrum threat detection employs all of these methods and we continue to add more to keep you always ahead of the attackers. Bricata's approach minimizes your network's attack surface and maximizes detection rates.

True Threat Hunting

Bricata is your license to threat hunt. Whether Bricata alerts you to a potential threat, you're trying to explore suspicious network behavior, or you just want to gain deeper insight into your normal operations, Bricata's rich network metadata is indexed and available in an unconstrained threat hunting environment. Unlike other tools that only provide the data associated with threats they have detected, Bricata gives you access to all of your network metadata and PCAPs. It provides an intuitive query interface along with workflows, visualization techniques, analysis methods, and reports to support rapid threat investigation and resolution to keep your network free of threats and your business open.

Post-Detection Actions

Detecting threats is good, but acting to contain them and prevent their damage is even better. Bricata gives you time, information, and options to deal with threats quickly. Bricata's full-spectrum threat detection engine catches attacks as early in the kill chain as possible so they can be contained and eradicated prior to causing damage. When Bricata detects a threat it immediately generates an alert to the security analysts, provides them with immediate context to understand the threat, and delivers analysts into the threat hunting environment in context to further investigate its trail and propagation across your network. When deployed inline on the network, Bricata can be configured to drop packets and immediately stop threats upon detection. It can also export all of its case details, rich metadata and PCAPs to your other cybersecurity tools, SIEMs, and orchestration mechanisms.

Comprehensive Network Protection

Bricata is a single system purpose-built to deliver comprehensive network protection. Bricata's component technologies work together seamlessly to produce results that none of them can generate without the others. Anyone who has tried to deploy, use, and manage a multitude of tools, with their varied user interfaces and APIs, will appreciate Bricata's single, intuitive GUI across every function. And, whether you are managing just a single Bricata sensor on your network or hundreds, we've simplified systems management down to a single task in either case. Instead of multiple technologies with different user interfaces operating at many locations on your network, Bricata is the one system, with one user interface, you need on your network to keep your business protected.