riverbed

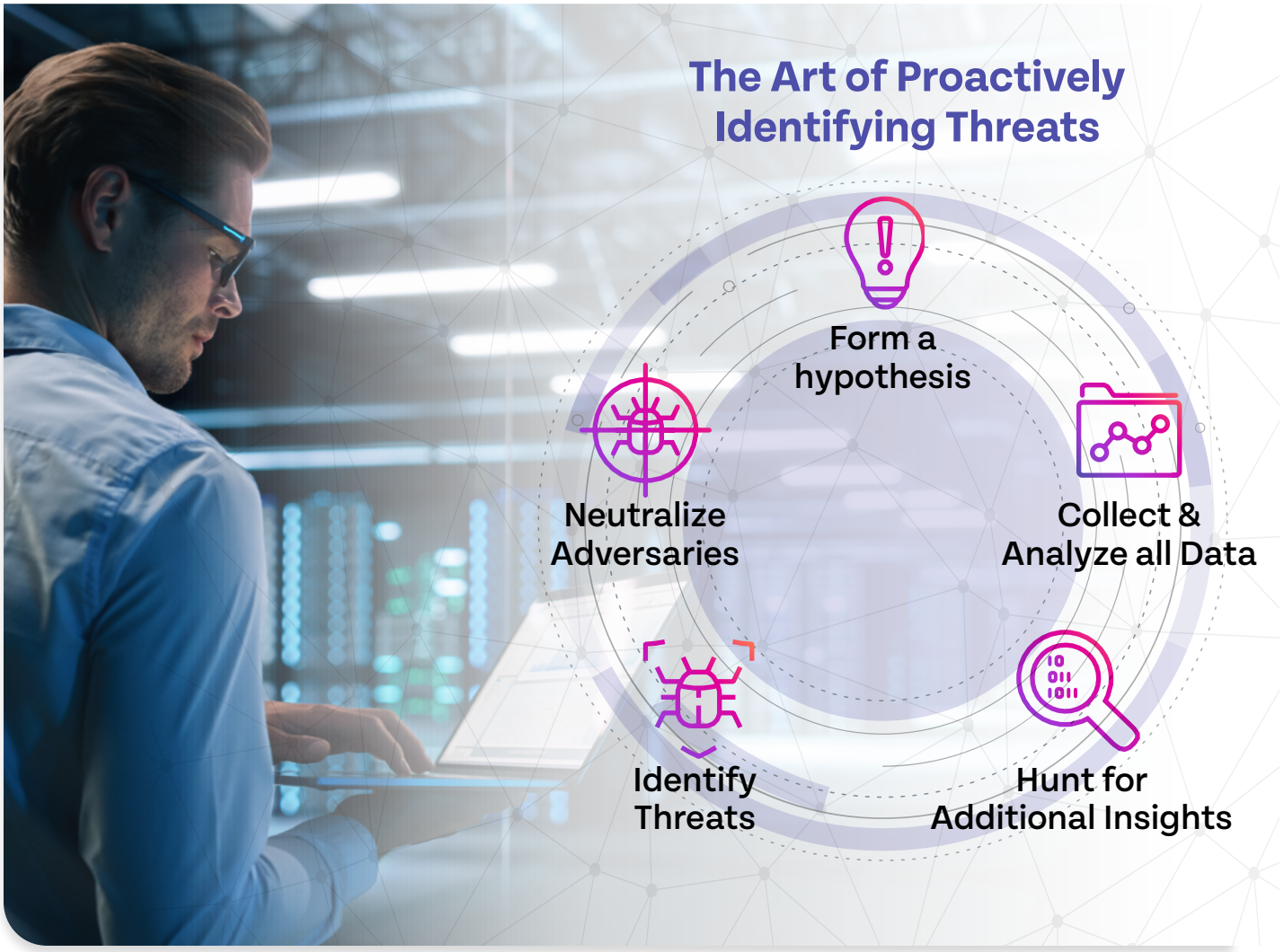
U.S. Public Sector

SOLUTION BRIEF

# Cybersecurity Threat Hunting

## NetOps & SecOps teams need to proactively find and eliminate threats.

Cyber threat hunting is the practice of proactively and iteratively seeking out, identifying, isolating, and disabling threats that may have penetrated an organization's network. The threat hunting process aligns NetOps and SecOps teams and challenges them to think like their adversaries based on recognized tactics, techniques, and procedures (TTPs). Instead of waiting for an intrusion detection system to issue alerts and then react, the most successful threat hunters leverage visibility across the entire network – from the endpoint to data access – to eliminate threats that have evaded traditional defenses and controls.



## A Threat Hunter's Arsenal

**The tools needed to proactively hunt threats help to achieve end-to-end visibility across the entire network environment and offer actionable insights.**

The Riverbed Observability and Optimization Platform allow threat hunters to see across their entire network environment. By integrating data from every user, device, application, and network, across a common dashboard, threat hunters have a single source of security truth from unified insights.

Armed with this data, threat hunters can fundamentally transform their approach to seek out and eliminate threats before serious damage occurs.

**Resolve**
security threats & performance issues up to **90% faster**

- **Full-Fidelity Flow Monitoring** with port and dependency mapping as well as long-term data retention offers broad visibility into all network traffic.
- **Packet Capture with Deep Packet Inspection** (DPI) examines protocol details and offers abundant packet storage for data-level forensic analysis.
- **Infrastructure Monitoring** provides details into change management, and detects unusual activity on network devices, such as saturation of an interface by an attack.
- **Endpoint Detection** monitors desktops, laptops, and other end user devices to detect and investigate suspicious activities.
- **Log Analysis** extracts data from log files for trend and pattern analysis.
- **Anomaly Detection** recognizes changes in volume and velocity of traffic between IPs.

Learn more at
riverbed.com/solutions/security-compliance

riverbed

### Riverbed – Empower the Experience

Riverbed, the leader in AI observability, helps organizations optimize their users' experiences by leveraging AI automation for the prevention, identification, and resolution of IT issues. With over 20 years of experience in data collection and AI and machine learning, Riverbed's open and AI-powered observability platform and solutions optimize digital experiences and greatly improve IT efficiency. Riverbed also offers industry-leading Acceleration solutions that provide fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of market-leading customers globally – including 95% of the *FORTUNE* 100 – we are empowering next-generation digital experiences. Learn more at riverbed.com.