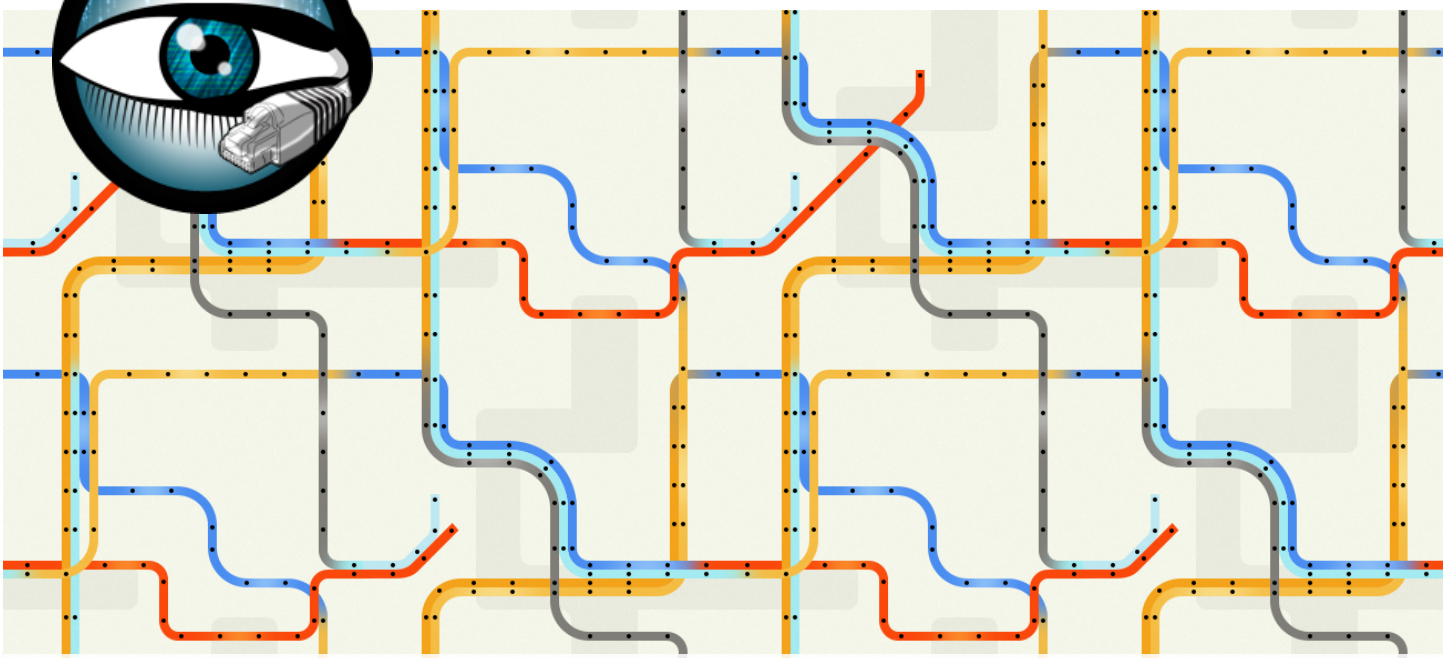
Why Choose Zeek?



Zeek is an open-source network security platform (formerly named *Bro*) that illuminates your network's activity in detail, with the **stability** and **flexibility** for production deployment at scale.

Features

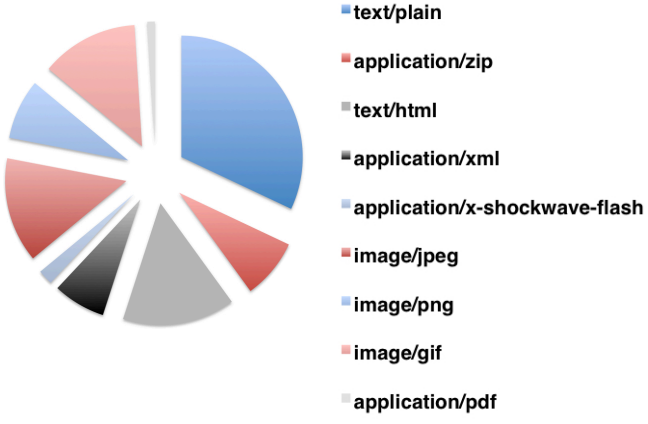
- **Flexible network security monitor with event correlation**
- **Traffic inspection**
- **Attack detection**
- **Log recording**
- **Distributed analysis**
- **Full programmability**

Powerful analysis, elegant design

Zeek reduces incoming packet streams into higher-level events and applies customizable scripts to determine the necessary course of action. This simple design allows you to configure an array of real-time alerts, execute arbitrary programs on demand, and log data for later use.

Detect what's on your network

Zeek's out-of-the-box installation gives you an immediate view of your network activity, including file types, software, and networked devices. You can export this data to a variety of visualization tools to provide meaningful interpretations to a broader audience.



"[Zeek is] not about trying to tell you what's bad, it tries to tell you what's happening."
- Richard Bejtlich, TaoSecurity

Listen passively, respond actively

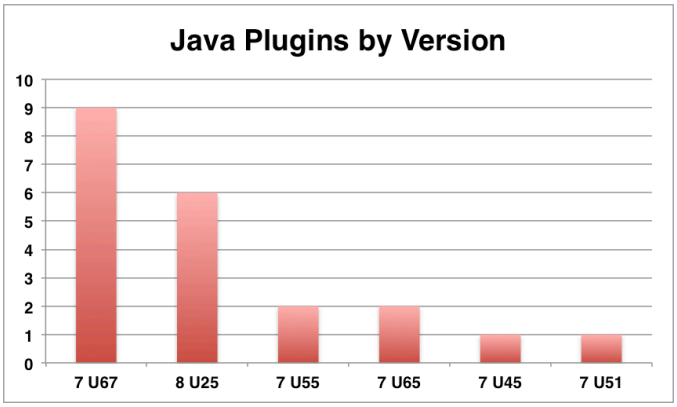
Whether you want to monitor all traffic using optical networking taps, analyze historical data when a zero-day attack is discovered, or build a black hole router to defend against attacks; Zeek's approaches to network security extend beyond traditional signature-based detection.

Scalable to 100G networks and beyond

Use Zeek to build a distributed monitoring system that is unified and scalable. Managing your installation is simple with BroControl, an interactive shell that executes commands across all systems. Zeek works with load-balancing tools like PF_Ring to increase packet capture performance in high-volume networks.

Well-structured data

Zeek's straightforward log structure makes it work well with products like Security Onion. It also integrates with data analysis tools like Splunk. Zeek's own log parsing tool, *bro-cut*, allows users to build simple queries at the command line when larger tools are unnecessary.



Vibrant development community

Zeek's growing community provides assistance and support; often releasing scripts to detect major vulnerabilities, like Heartbleed and Shellshock, shortly after their discovery. The Zeek Project fosters the community by managing public forums and infrastructure, including user meetings, mailing lists, issue tracker, an IRC channel, and Twitter account.

Grounded in years of research

Zeek began within a research project at the Lawrence Berkeley National Laboratory in 1995 and moved onto an operational deployment there a year later. Since 2003, the National Science Foundation has funded Zeek-related research at the International Computer Science Institute (ICSI), a non-profit research organization affiliated with the University of California at Berkeley. In 2010, ICSI announced a partnership with the National Center for Supercomputing Applications to jointly maintain The Zeek Project.

Dedicated support for NSF-funded projects

The National Science Foundation funds The Bro Center of Expertise to help academic institutions operate Zeek effectively. Contact us at nsf@zeek.org to learn more.