

ABOUT INFRARAY

Longstanding experience

Infraray was founded in 1998 by a German engineering team with many years of experience in the field of IT operations management and has been part of the Beta Systems Group since the beginning of 2018. The company offers solutions for network management, network security, IT infrastructure management, network automation and control of the complete business infrastructure.

CONTACT

Are you interested?

Then don't hesitate to contact us. We are at your disposal for all questions regarding our products, solutions and services.



+49 (0) 30 254 690 0



info@infraray.com



www.infraray.com

Maximum transparency and control for your IT infrastructure



infraray

powered by [_betasystems](#)



Infraray BICS: the multi-talent for network security & management

Discover, manage and control everything connected to your network in unprecedented detail with infraray BICS - securely and easily. Create maximum transparency and control, monitor critical resources and automate management tasks to gain full control over your IT infrastructure.

Key features:

- ✓ Automatic recognition of up to 1 million end and connection points
- ✓ clear topologisation
- ✓ Simple event and alarm handling as well as comprehensive dashboards
- ✓ Centrally controlled through modern graphical user interface

One tool for several applications

Discover, manage and control everything connected to your network: Network Management and Network Security as well as Asset Management.



Network Management

Infraray BICS enables administrators to centrally monitor, control and secure their complex IT infrastructure. Switches and gateways are automatically queried in a heterogeneous IT infrastructure, all connected end devices as well as ports and uplink connections are identified and displayed regardless of manufacturer and model.



Network Security

Infraray BICS can centrally monitor IT networks independent of manufacturer with the Network Security Module. New, unauthorised and compromised devices are detected, unplanned/unauthorised changes to device configurations are identified and suspicious communication relationships are reported and prevented.