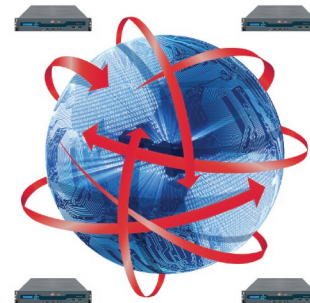


*The FireEye MAX Network is a real-time exchange for malware threat data to maximize preemptive protection against broad and targeted attacks.*

# FireEye Malware Analysis & Exchange Network

## Malware Protection System



The FireEye Malware Analysis & Exchange (MAX) Network is a real-time exchange for malware threat data to maximize preemptive protection against a dynamic cyber threat. Within locally deployed FireEye appliances, the FireEye Analysis & Confirmation Technology (FACT) engine automatically generates real-time malware intelligence to protect the local network against zero-day malware and advanced persistent threats. The FACT engine fingerprints zero-day malware and captures its callback IP address, communication protocol(s), port(s), and other details. Through the MAX Network, subscribers get real-time updates of global threats to their local network.

### Global Network to Share Local Malware Intelligence

The FireEye MAX Network is formed from interconnected FireEye appliances deployed within customer networks, technology partner networks, and service providers around the world. FireEye has built a worldwide Malware Analysis and Exchange (MAX) network to share and efficiently distribute the auto-generated malware security intelligence, such as its covert callback channels. The MAX Network is essentially an Internet cyber crime watch system to provide subscribers the latest intelligence on inbound attacks and unauthorized outbound callback destinations to prevent data exfiltration, alteration, and destruction. Real-time detections of inbound targeted attacks take place in the local FireEye network appliances. It performs outbound callback analysis based on its local callback database and further maximizes the detection of modern malware infections by subscribing to the global MAX Network.

### Advancing the State-of-the-Art For Malware Protection

FireEye has significantly advanced the state-of-the-art for malware protection, and has now made it possible to accurately stop modern malware in real time. With inbound attack detection and outbound malware transmission filtering tied into a global security exchange network, administrators have a clientless solution that is easy to deploy and maintain to provide modern protection against today's modern threats.

### KEY FEATURES & BENEFITS

- ➔ Global distribution of targeted modern malware intelligence
- ➔ Pull-based data feed on Trojans, bots, and advanced persistent threats
- ➔ Prevents modern malware infiltration within the network
- ➔ Real-time updates to cut off outbound malware transmissions and stop data exfiltration

