



ENDPOINT SECURITY

From Prevention to Remediation

Comprehensive Endpoint Security

As endpoints proliferate, and the bring-your-own-device (BYOD) mentality becomes more pervasive, organizations face rapidly increasing security risks. Older endpoint protection platforms (EPPs) use static blocking to keep out known threats. But as attackers have become more sophisticated, and as more unknown threats emerge, static blocking has become less effective. Newer EPP solutions, often labeled "next-generation endpoint security", need to be able to combat these threats with advanced endpoint detection and response (EDR) capabilities.

It's time to prepare your EPP for new threats and risks.

KEY

— PROBLEM ● SOLUTION

 info@fireeye.com

 www.fireeye.com/endpoint

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035 / 408.321.6300 / 877.FIREEYE (347.3393)

© 2018 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. IG.FPR.EN-US.52018



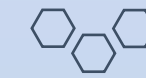
An attack may achieve its goal in the **time it takes a human to evaluate and respond** to it.



Automated solutions can accelerate effective responses.



The **quantity of undifferentiated alerts** from static defenses can overwhelm security teams.

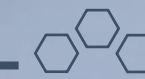


Intelligence provides alert context to respond to genuine threats.

Multiple adaptive defenses address evolving tactics.



Attackers rapidly **test and refine their attacks** to evade defenses against known threats.



A SMARTER ENDPOINT PROTECTION PLATFORM

A single, consolidated and well-designed agent can simplify security.

Maintaining a high quality security system is only continuing to be **more and more complex**.



Support for Windows, MacOS and Linux meets diverse needs.

Scalable on-premise, cloud and hybrid deployments can help provide protection in your network environments.

Integrated workflows can combat multi-flow, multi-stage attacks.



Endpoints can be a part of difficult-to-identify, **multi-vector, blended attacks**.



Users' **preferred environments** must be protected.



Diverse and **evolving security architectures** require flexible endpoint solutions.