FIREEYE™

SOLUTION BRIEF

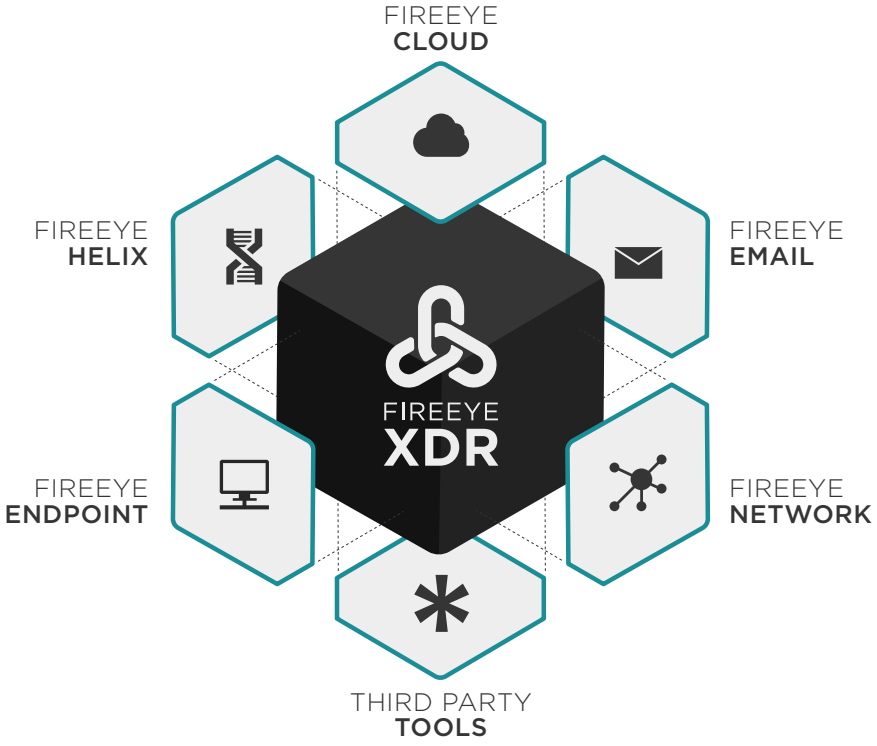
Unifying Your Security Architecture with FireEye XDR

The ever-changing threat landscape and the constant requirement for security teams to pivot across a multitude of products has given rise to extended detection and response (XDR). Its goal is to unify telemetry from security and business technologies such as endpoint detection and response (EDR), network analysis and visibility (NDR), email security, security information and event management (SIEM), security orchestration, automation and response (SOAR), cloud security, and more into a security-relevant protection, detection and response solution.

Even before XDR was defined, FireEye had worked to provide customers with XDR outcomes. We uncover threats by correlating incident data and applying unparalleled frontline intelligence and analytics to prioritize and respond to threats that matter. To reduce security complexity and raise the bar for security professionals, FireEye XDR not only provides our customers with simplified threat detection, investigation and incident response, but also up-level analyst proficiencies.

Figure 1.

Connect and unify FireEye technologies as well as a broad range of 3rd party data from multiple sources.



Current Security Challenges
Customers continue to invest in security solutions that attackers seem to easily bypass. There are three critical factors related to security investments that contribute to this situation.

- **Solving the last security threat, not the next one**
  Organizations may be proactive and up to date with the current threats. However, for most organizations, protecting against future threats continues to be a challenge. They simply do not have the expertise or staffing to review all incoming attacks. Most organizations simply lack the forward-looking intelligence needed to protect against potential attacks.
- **Relying on too many error-prone manual processes to manage security**
  Another challenge for organizations is the reliance on manual processes to manage their security infrastructure. For many organizations, the need to be absolutely confident that an alert is not a false positive cause many levels of manual review. As a result, many organizations lose valuable time as alerts wait for manual review. Attackers know that timing is critical; every day, they conduct more and faster attacks.
- **Internally developing costly homebrew security solutions**
  Many organizations believe they save money by developing in-house or "home brew" security solutions. Unfortunately, these solutions often cost organizations more than investing in off-the-shelf solutions. Inability to update, lack of expertise and other issues tend to plague in-house solutions, making them less secure and more burdensome than an established, reputable solution.

Respond and mitigate quickly with FireEye XDR
The unified FireEye XDR platform integrates and analyzes data from your security assets to give you real answers about the threats that matter.

With FireEye XDR your organization can:

- **Move from attack detection to future threat prevention**
  How: FireEye technology blocks inbound email attacks, network-based attacks, and endpoint attacks. By centralizing security data from all threat vectors to you can simplify root cause analysis.
- **Detect advanced attacks across all vectors**
  How: FireEye enables you to detect security Incidents with confidence by correlating data from multiple tools across your organization. Then you can apply the knowledge of the threat landscape across your FireEye and third-party security technology stack.
- **Respond with authority**
  How: FireEye provides guided investigation workflows. This allows you to reduce the impact of security incident workflows. Ultimately, you gain the ability to prioritize analyst time and mitigate risk, by addressing what is critical to your security operations.

FireEye XDR combines the automation of world-class technology with the power of unparalleled frontline human expertise, including industry-recognized services and nation-state grade threat intelligence. Among its many benefits, you can:

- **Improve analyst and SOC efficiency** by correlating disparate events from multiple tools into actionable investigations
- **Reduce organizational risk** by automating threat detection and investigation, accelerating response and prioritizing the prevention of incidents
- **Deliver high levels of detection efficacy** and analytics with incident response best practice playbooks updated daily to reflect the changing global threat landscape
- **Optimize the deployment mix** to suit your strategy, which gives you the freedom to use any combination of FireEye and third-party products

A Flexible XDR Approach

To optimize performance and improve your security posture against the most sophisticated threats, we recommend integrating FireEye Endpoint Security, Email Security, Network Security and Cloudvisory with Helix. This enhances the FireEye XDR platform with additional analytics capabilities for detecting advanced attacks and lateral movement.

FireEye XDR connects all FireEye technologies and expertise together, enabling them to seamlessly detect threats across endpoint, network, cloud, and email from a single platform. It easily integrates a broad range of third-party security tools, allowing you to tailor your strategy to your needs with an awareness of your existing security investments.

Contact Sales for more information.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.