Field/Customer FAQs

On April 22, 2015, FireEye, Inc. was issued "Certification" under the SAFETY Act for its Multi-Vector Virtual Execution (MVX) Engine and Cloud Platform by the Department of Homeland Security (DHS). Below, please find answers to the most frequently asked questions about this important award:

What is the SAFETY Act?

The SAFETY Act is a 2002 federal law that created a liability management program for providers of anti-terrorism technologies. The Act creates certain liability limitations for "claims arising out of, relating to, or resulting from an Act of Terrorism" where anti-terrorism products have been deployed.

Under the SAFETY Act, certain security product and service providers may apply for liability protections – in the form of a SAFETY Act award – from the Department of Homeland Security (DHS). If awarded SAFETY Act protections, the provider is entitled to specific protections from third-party liability stemming from the use of that product or service in relation to an "Act of Terrorism" and those liability protections associated with this award "flow down" to the buyers of these technologies.

View the DHS Safety Act website: www.safetyact.gov

What is SAFETY Act Certification?

SAFETY Act protections can only be earned after successfully completing a comprehensive and rigorous review process administered by DHS. There are two levels of awards available under the SAFETY Act: Designation and Certification. The awards correspond with different levels of liability protection.

Certification is the highest level award available under the SAFETY Act. In order for a product or service to become SAFETY Act "Certified," the provider must prove to DHS that the product is not only effective, but also that it performs as intended, conforms to set specifications, and is safe for use.

What is the practical effect of this SAFETY Act award for FireEye and its customers?

There may be significant legal claims and potential liabilities arising from a cyber-attack. Should a cyber-attack take place and tort claims be filed against FireEye (as the manufacturer of the product) or our customers (as the user of the product) relating to the use, performance, design etc. of the MVX Engine or Cloud Platform, SAFETY Act certification provides a strong defense up to and potentially including dismissal of such claims.

The MVX Engine is a core component of FireEye's appliances and most of FireEye's appliances are designed to connect with its Cloud Platform. Both of these technologies are now SAFETY Act Certified, and FireEye will receive numerous benefits, including:

- The MVX Engine and Cloud Platform are on the DHS "Approved Products List", which is an exclusive roster of highly effective security products and services.

- When the SAFETY Act is triggered by the DHS Secretary following a cyber-attack, FireEye is entitled to liability and procedural defenses, including:

    - Exclusive federal jurisdiction; and

    - A rebuttable presumption of **immediate dismissal of all third-party claims** based on the alleged failure of the MVX Engine or Cloud Platform that arise out of or relate to the cyber-attack in question.

      Indeed, the only way to defeat that presumption of dismissal is to show fraud or willful misconduct in the submission of the SAFETY Act application to DHS.

      And, even if for some reason fraud or willful misconduct is shown, FireEye still receives liability protections that include a maximum cap on damages, a bar on punitive damages and prejudgment interest, a bar on joint and several liability, and a reduction in any award to plaintiffs equal to amounts they receive from other parties (such as victim compensation funds, life insurance policies, etc.).

    - FireEye's customers, suppliers, vendors, and all others in its supply chain are immune from third-party claims related to any alleged

failure, or negligent design or implementation of the MVX Engine or Cloud Platform. In other words, FireEye's **customers cannot be sued** for buying such FireEye products or any alleged failure of these products in a cyber-terrorist attack.

- FireEye receives an official "seal" that it may use on all its marketing material indicating that it has received the Certification award.

That's too good to be true. What's the catch?

There is no "catch" per se, but the SAFETY Act may only be invoked in certain circumstances:

- First, the DHS Secretary has to declare that the cyber-attack in question is an "Act of Terrorism." However, under the law, "Act of Terrorism" is broadly defined. The attack only needs to be 1) unlawful, 2) cause harm, including economic harm in the United States, and 3) the attacker has to use a weapon or other items that are intended to cause such harm. There is **no need** to demonstrate "terrorist" motivations or connections to terrorist groups. As such, the SAFETY Act can apply to a broad range of attacks, including state-sponsored or criminal cyber-attacks.

- Second, the SAFETY Act protections only apply to the products running on the MVX Engine and Cloud technology. This means that if you, as the customer, so materially change FireEye's products that they are no longer the "same" product that DHS reviewed, the SAFETY Act award may no longer be applicable. It also means that claims unrelated to these certified products are not protected.

- Third, FireEye's award only protects those MVX Engine and Cloud Platform products purchased from July 1, 2008 and the act of terrorism/cyberattack must have occurred on or after April 22, 2015.

- Lastly, the SAFETY Act only provides for dismissal of third-party claims – regulatory and other types of claims can still proceed.

What if the DHS Secretary refuses to declare that the SAFETY Act applies after a cyber-attack?

No official or automatic protections would apply. However, customers will still be able to demonstrate that when the attack occurred, they were using a product that was thoroughly tested and reviewed by DHS, and found to be so "useful" and "effective" that it was "Certified" under the SAFETY Act. This may provide powerful evidence to rebut any claims that they were negligent in the selection of vendors or the design of their security program.

Has the SAFETY Act been tested in court?

No, the SAFETY Act has never been tested in court. Until recently, the vast majority of SAFETY Act awards were issued for physical security products (like x-ray machines), and we as a nation have fortunately not experienced an event to trigger the SAFETY Act for such products during past years.

However, the SAFETY Act is premised on the "government contractor defense," a well-established common law defense. The Supreme Court has reviewed and affirmed the government contractor defense, and the SAFETY Act simply represents a codification of these basic principles. Thus, if the SAFETY Act is tested, there is very high confidence that the SAFETY Act will be upheld in federal court.

What if the attack originates from or occurs overseas? Could the SAFETY Act protections apply in those situations?

Yes, the SAFETY Act can apply even when an attack originates from or actually occurs outside the United States. So long as the attack impacts the United States (either physically or economically) and the ensuing litigation is being decided under U.S. law, both U.S. and international customers may take advantage of the defenses of the SAFETY Act.

As a FireEye customer, do I need to do anything to enjoy these SAFETY Act protections?

That's the best part – you don't! If you are using the MVX Engine or Cloud technologies, the SAFETY Act protections automatically flow down to you, the customer.

Are any other cybersecurity products or services SAFETY Act Certified?

FireEye's MVX Engine and Cloud Platform are the first and only true cybersecurity technologies to be deemed so "useful" and "effective" by DHS that they are SAFETY Act Certified. Once again, FireEye has broken new ground with its products.

Currently, the following product offerings run on the MVX Engine and Cloud Platform:

- Network Threat Prevention (NX Series)
- Email Threat Prevention (EX Series)
- Email Threat Prevention Cloud (ETP)
- Content Threat Prevention (FX Series)
- Malware Analysis Platform (AX Series)
- Mobile Threat Prevention (MTP)

This award also applies to older products running the MVX engine, such as MPS.

I have more questions! Who can I contact at FireEye?

Alexa King, General Counsel: alexa.king@fireeye.com
Reena Paraguya, Commercial Counsel: reena.paraguya@fireeye.com