

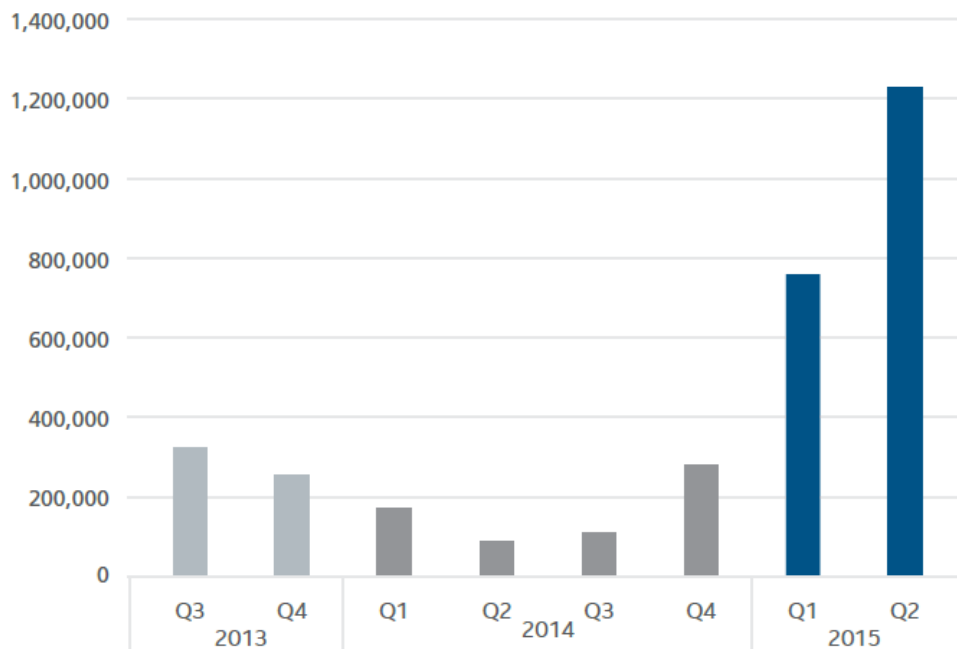
McAfee Labs 2016 Threats Predictions

Ransomware

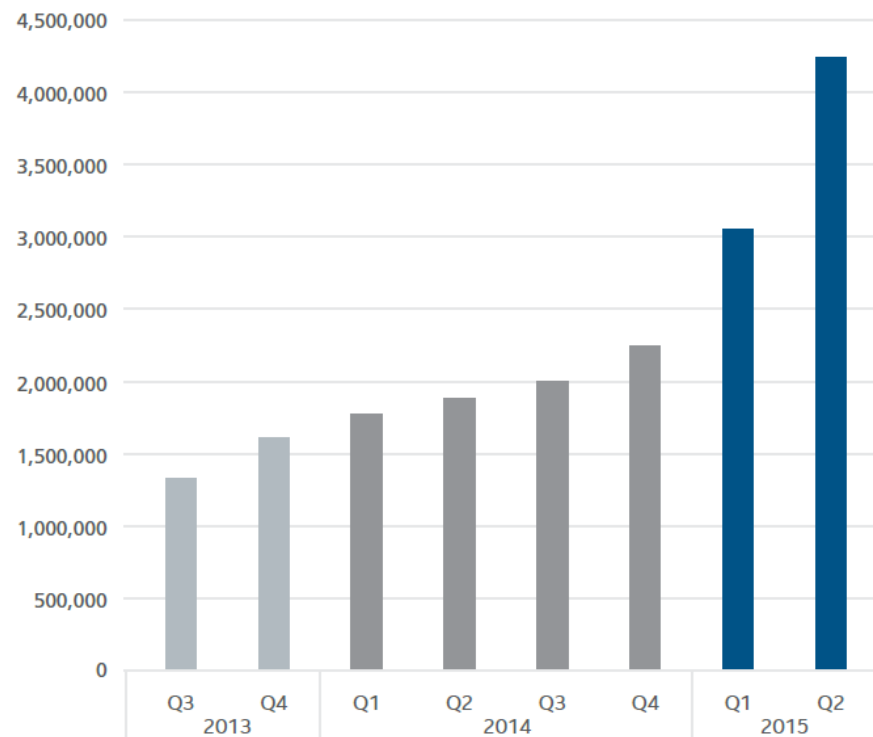
Ransomware zůstává hlavní a rychle rostoucí hrozbou v roce 2016, využívající anonymitu sítě a nových platebních metod – bitcoin.

Nezkušení útočníci využijí Ransomware-as-a-service, čímž zvýší množství útoků Ransomware.

New Ransomware

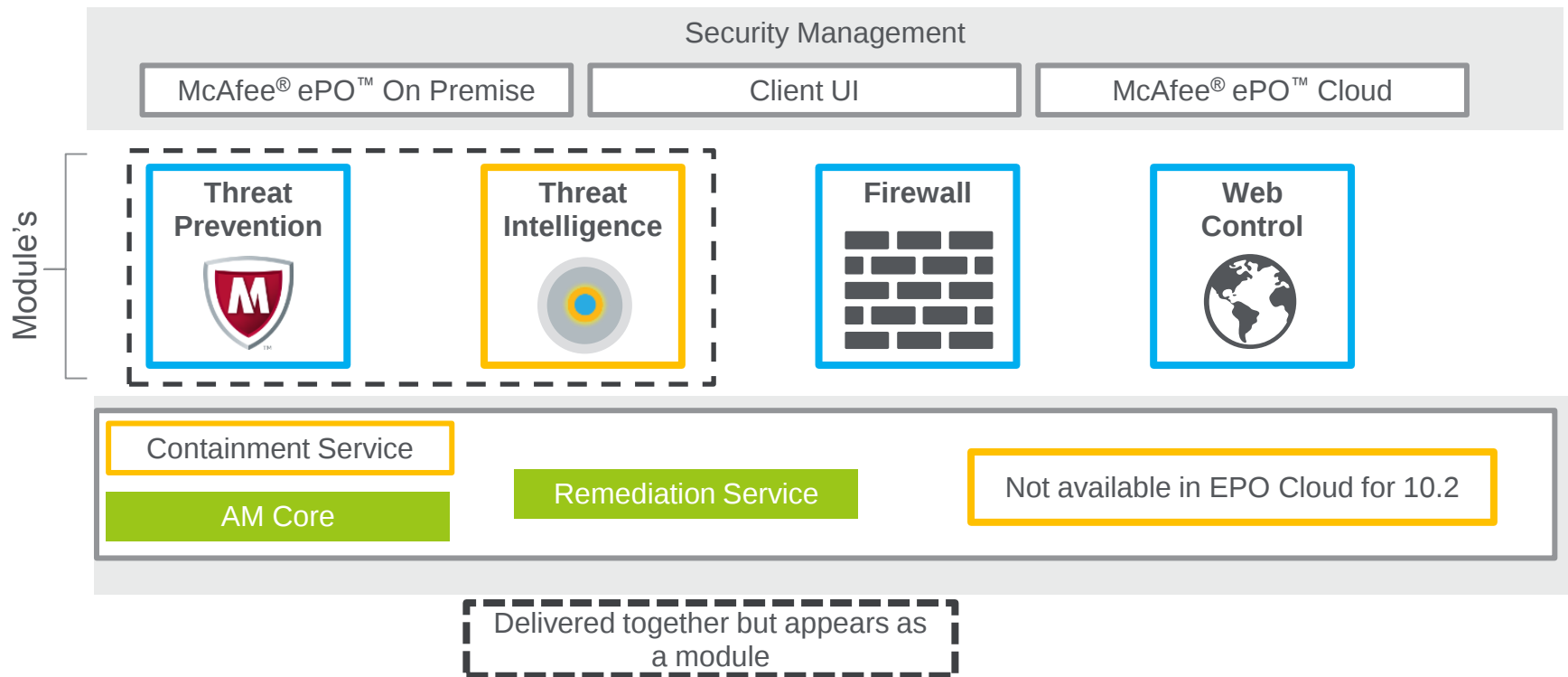


Total Ransomware



McAfee Endpoint Security 10.x

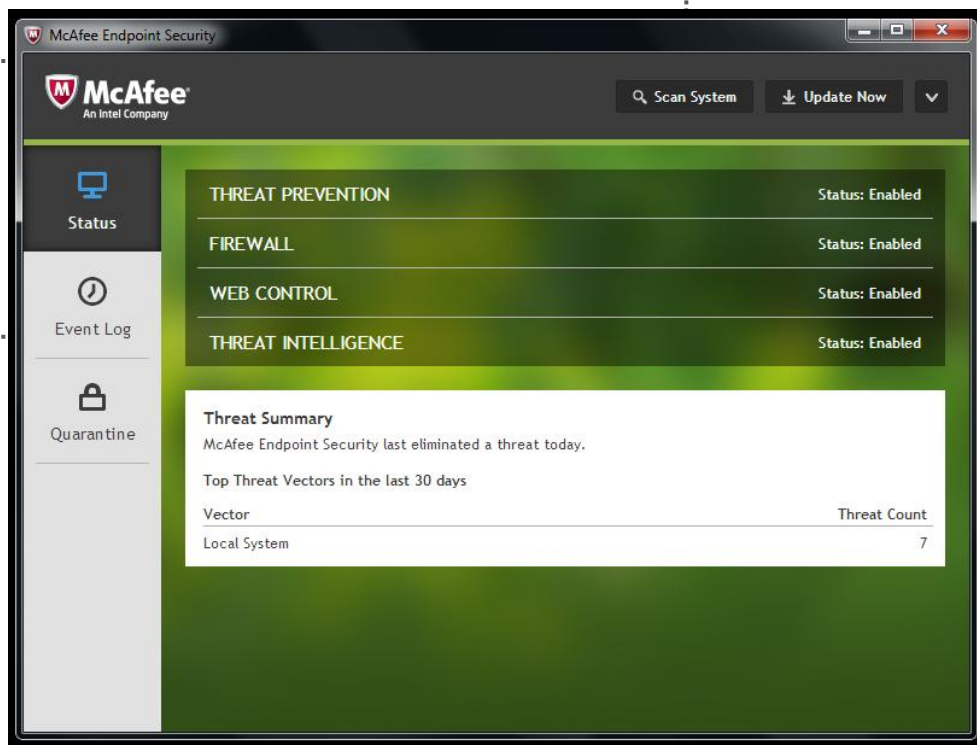
McAfee® Endpoint Security 10.2 Client



McAfee Endpoint Security 10.2 klient

Dotykové
ovládání

Srozumitelné
zobrazení událostí



Inteligentní a rychlé skenování

Ochrana heslem
Politiky nabízí
Základní / Rozšířené
klientské nastavení

Integrované
bezpečnostní moduly

Modulární a
rozšiřitelný design

Detailní pohled na detekované události

The screenshot displays the McAfee Endpoint Security console. On the left, a sidebar contains 'Status', 'Event Log', and 'Quarantine' options. The 'Event Log' is selected, showing a list of events. A red box highlights a specific event: 'DEMO\administrator ran 1002.EXE, which attempted to access C:\USERS\ADMINISTRATOR\APPDATA\ROAMING\CVEOJSMONGXTTFZZ.EXE, violating the rule "Creating files with the .exe extension", and was blocked. For information on how to respond to this event, see KB85494.' Below this, a detailed view of the event is shown, including a table of metadata and a threat summary.

Analyzer / Detector	
Analyzer content creation date	1/19/2016 11:11 AM
Analyzer content version	10.2.0.0000
Product name	Threat Intelligence
Analyzer rule name	Creating files with the .exe extension
Product version	10.2.0
Feature name	Dynamic Application Containment

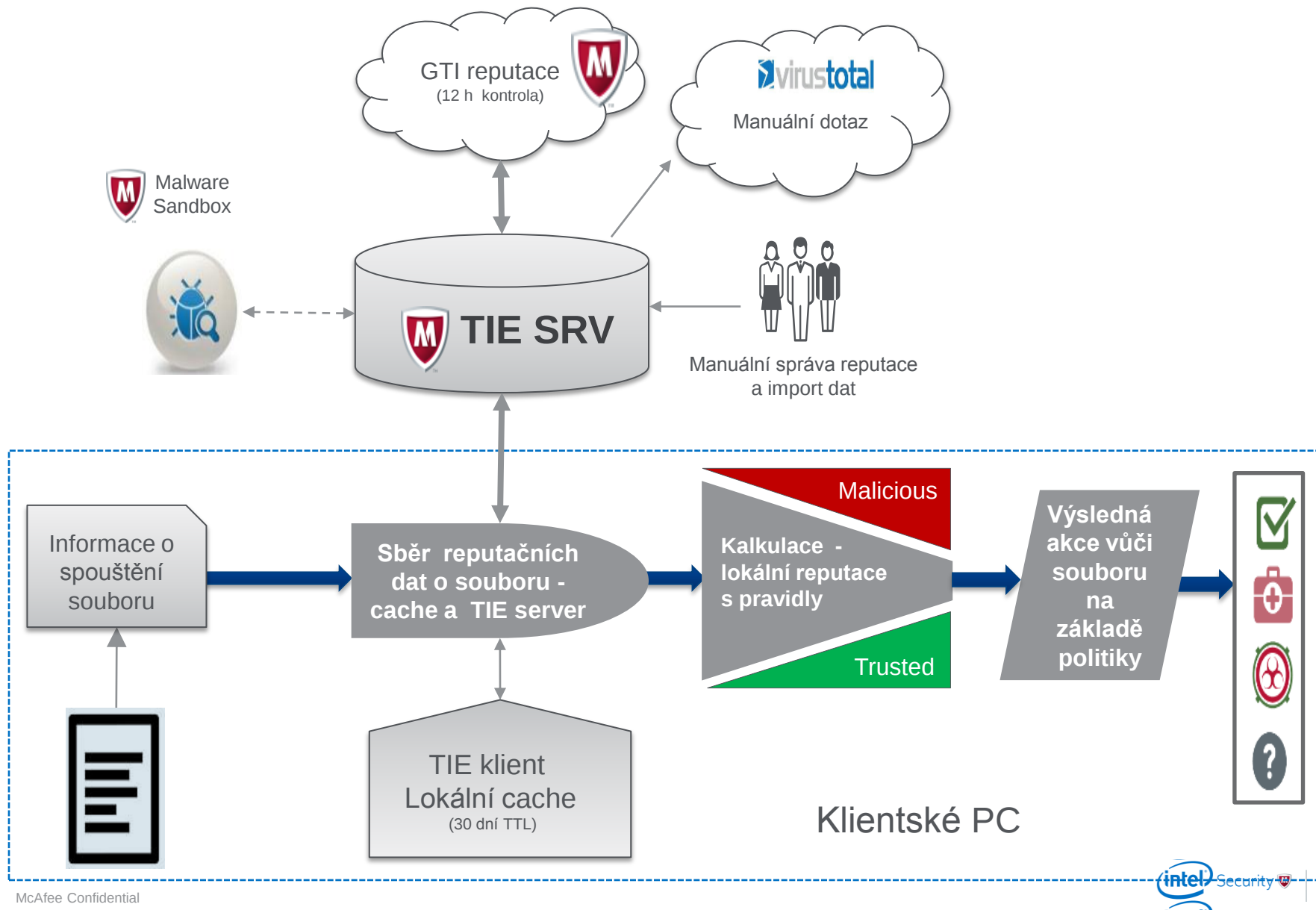
Threat	
Action taken	Blocked
Threat category	'File' class or access

Integrovaná inteligence,
která okamžitě informuje o
hrozbě

Více detailů o zdroji a cíli útoku na
základě DAD (Descriptive Attack Data)

Události zobrazované ve srozumitelné
podobě pro uživatele

Logika TIE technologie



Příklad reputace TIE - porovnání třech spouštěných souborů



Microsoft Visio

- ✓ Podepsaný důvěryhodným certifikátem
- ✓ Silná globální reputace z GTI

Důvěryhodnost: **Velmi vysoká**
Akce: **Povolit**



Zákaznická aplikace

- Žádný podpis
- Žádná globální reputace
- ✓ Mnohokrát spouštěný v lokálním prostředí / důvěryhodná lokální aplikace
- Žádné další atributy
- ✓ bezpečnostní hrozby

Důvěryhodnost : **Vysoká**
Akce: **Povolit**



Neznámý soubor - malware

- Žádný podpis
- Žádná globální ani lokální reputace
- ✗ První spuštění v lokálním prostředí
- ✗ Podezřelý atribut – download z Internetu

Důvěryhodnost : **Nízká**
Akce: **Blokovat**

TIE/DAC 10.2 – bezpečnostní politika s možnostmi nastavení

Spolupráce TIE a DAC rozšiřuje možnosti pro „unknown“ aplikace, které jsou zapouzdřeny pomocí DAC technologie

