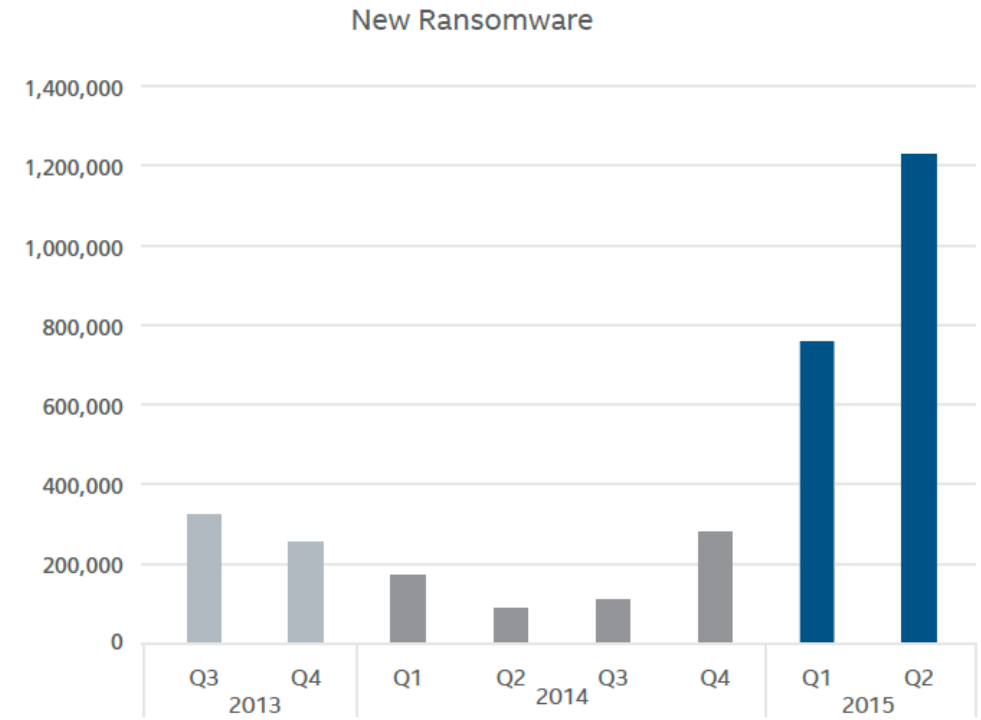
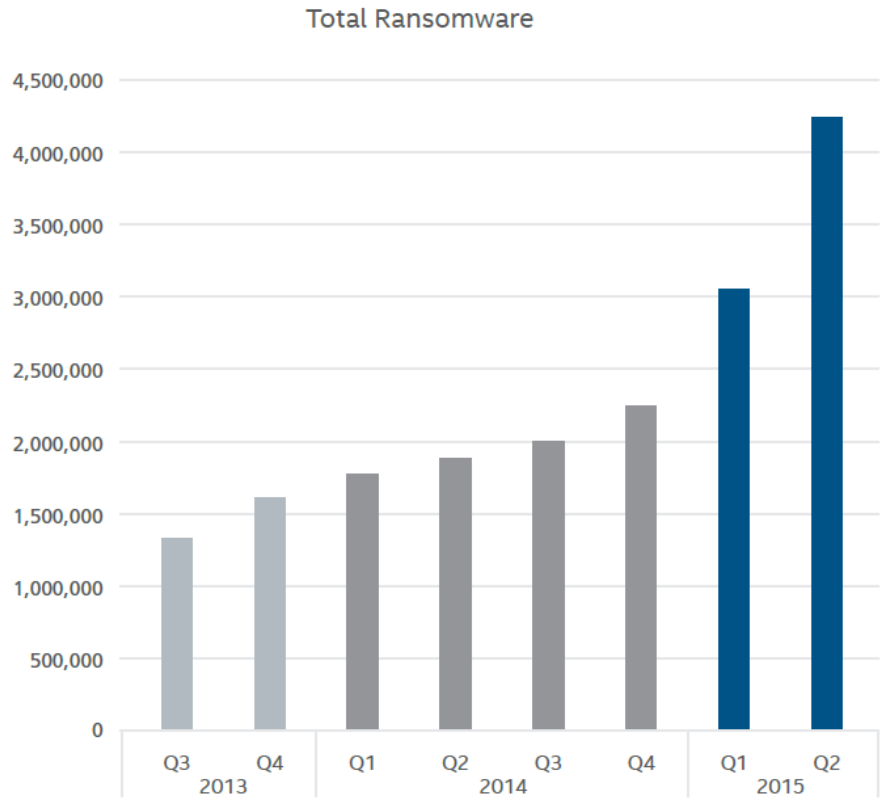
McAfee Labs 2016 Threats Predictions

Ransomware

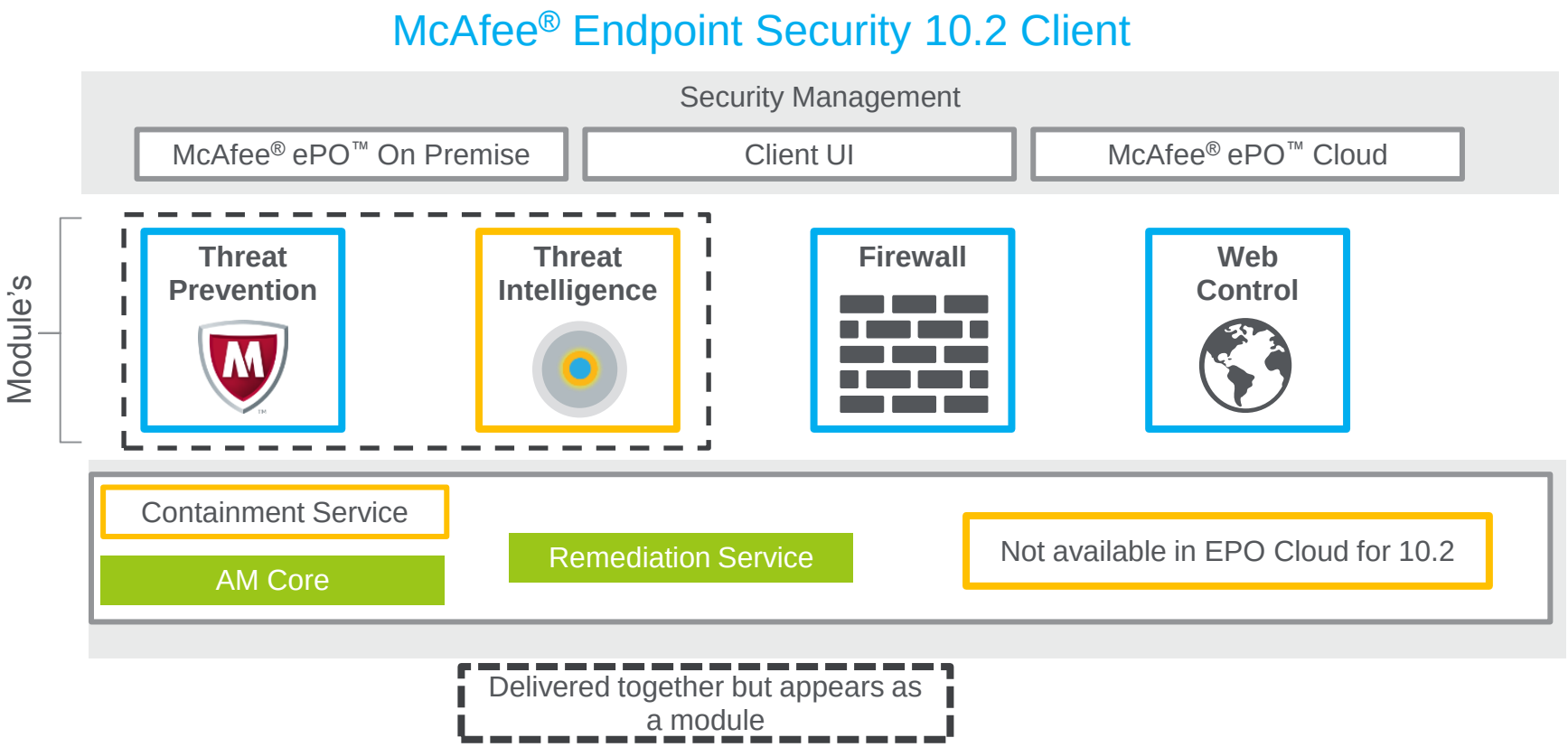
Ransomware zůstává hlavní a rychle rostoucí hrozbou v roce 2016, využívající anonymitu sítě a nových platebních metod – bitcoin.

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





McAfee Endpoint Security 10.x



McAfee Endpoint Security 10.2 klient

Inteligentní a rychlé skenování

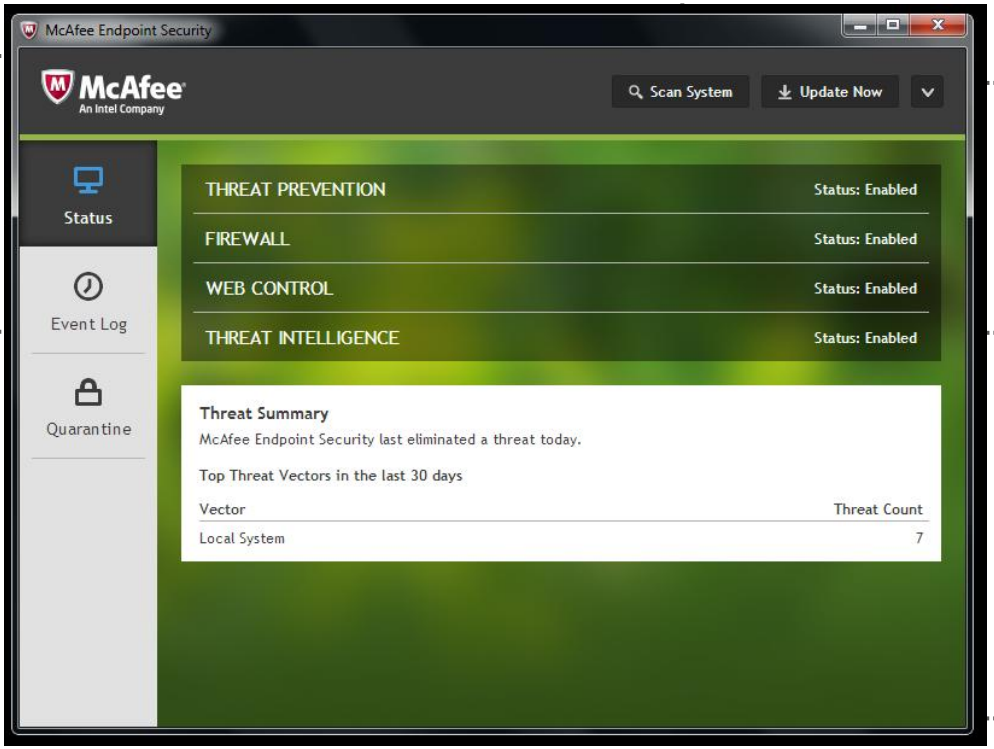
Dotykové ovládání

Ochrana heslem

Politiky nabízí

Základní / Rozšířené

klientské nastavení

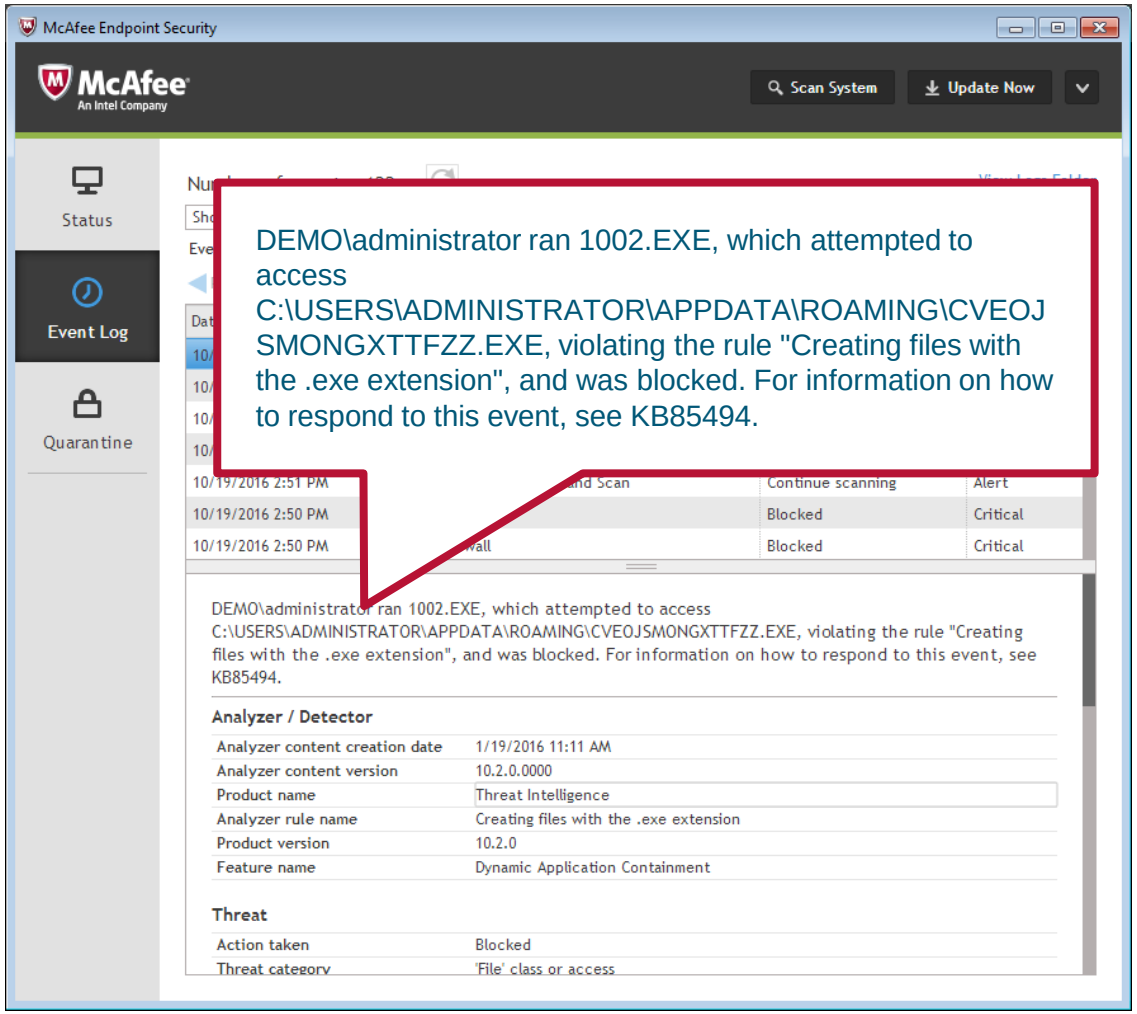


Srozumitelné zobrazení událostí

Integrované bezpečnostní moduly

Modulární a rozšiřitelný design

Detailní pohled na detekované události

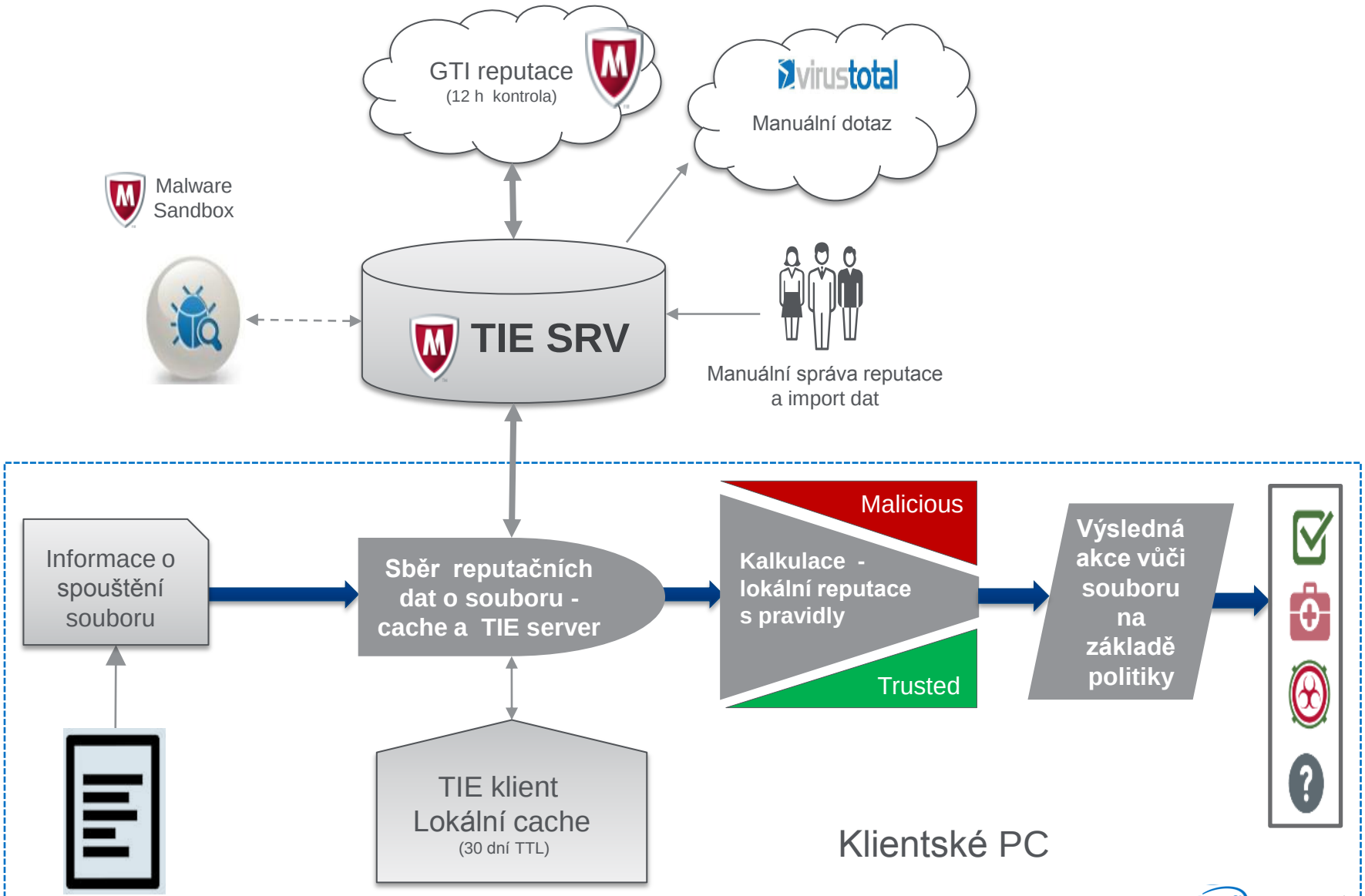


Integrovaná inteligence, která okamžitě informuje o hrozbě

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