

Monitoração de Vulnerabilidades com Telemetria

André Carraretto, CISSP
Security Strategist
Cyber Security Advisor for Rio2016

Conceituação

Telemetria é um processo de comunicação automatizado pelo qual medições e outros dados são coletados em pontos remotos ou inacessíveis e transmitidos para equipamentos de monitoramento.

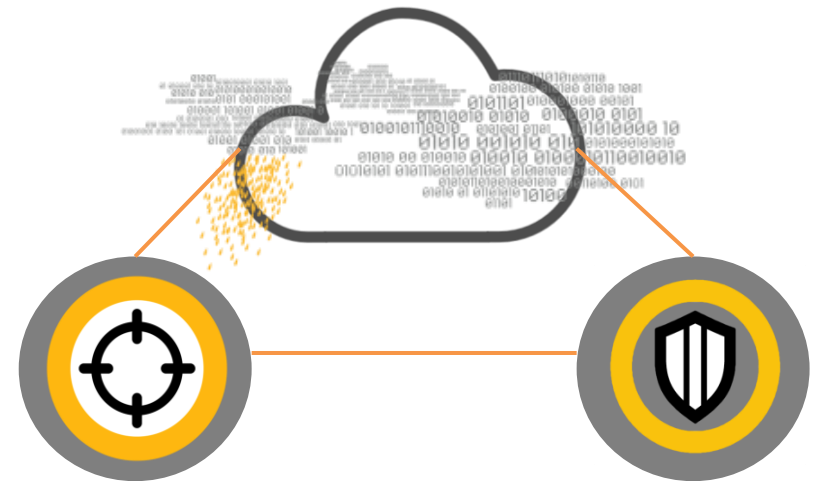
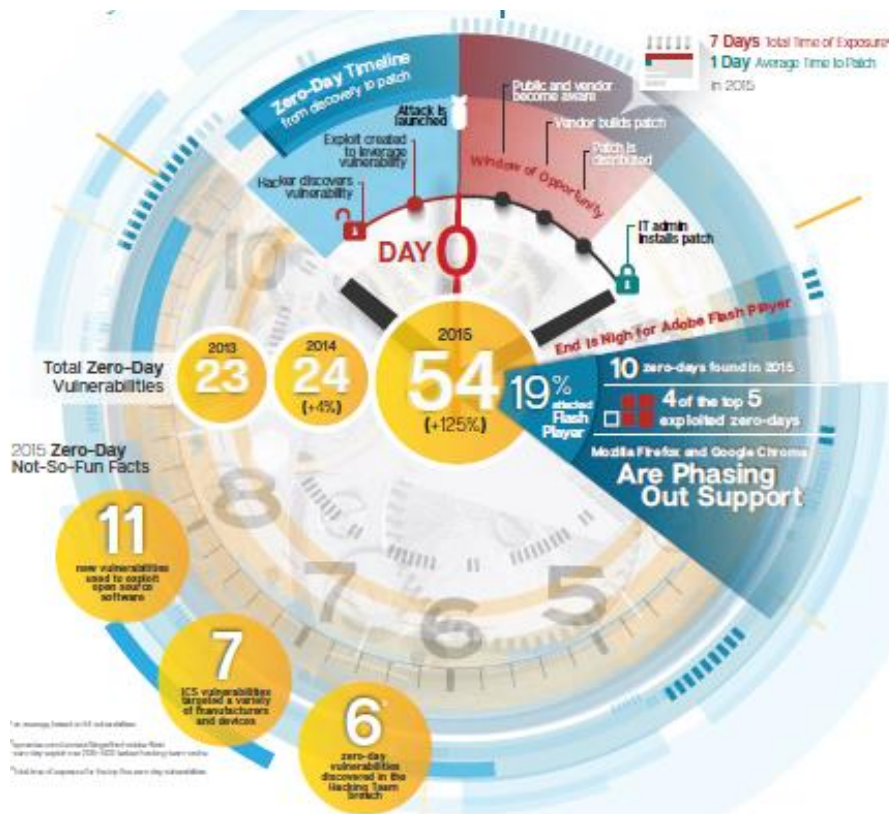
A palavra é derivada de raízes gregas: . Tele = remoto e metron = medida.

Conceito é utilizado nas mais diversas indústrias: óleo/gás, energia, medicina, automobilismo, aeroespacial, agricultura, defesa, varejo, entre muitas outras.

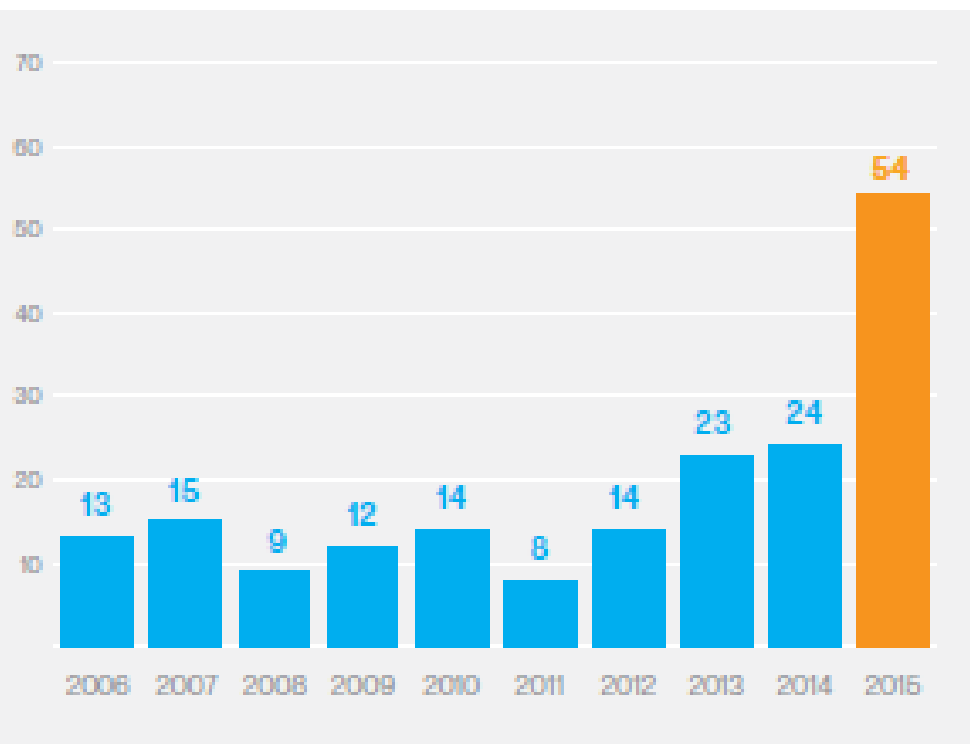


Como a Symantec utiliza Telemetria?

O Security Response e a Global Intelligence Network utilizam a telemetria enviada por mais de 200 milhões de dispositivos para rapidamente formular respostas para novas ameaças, e como estas estão explorando novas e recém descobertas vulnerabilidades.



Importância na rápida identificação e mitigação de vulnerabilidades



125% de aumento de Zero Days identificados em 2015

	2015 Exploit	2015	2014 Exploit	2014
1	Adobe Flash Player CVE-2015-0313	81%	Microsoft ActiveX Control CVE-2013-7331	81%
2	Adobe Flash Player CVE-2015-5119	14%	Microsoft Internet Explorer CVE-2014-0322	10%
3	Adobe Flash Player CVE-2015-5122	5%	Adobe Flash Player CVE-2014-0515	7%
4	Heap-Based Buffer Overflow aka 'Ghost' CVE-2015-0235	<1%	Adobe Flash Player CVE-2014-0497	2%
5	Adobe Flash Player CVE-2015-3113	<1%	Microsoft Windows CVE-2014-4114 OLE	<1%

Adobe Flash Player no Top 5 dos exploits mais utilizados

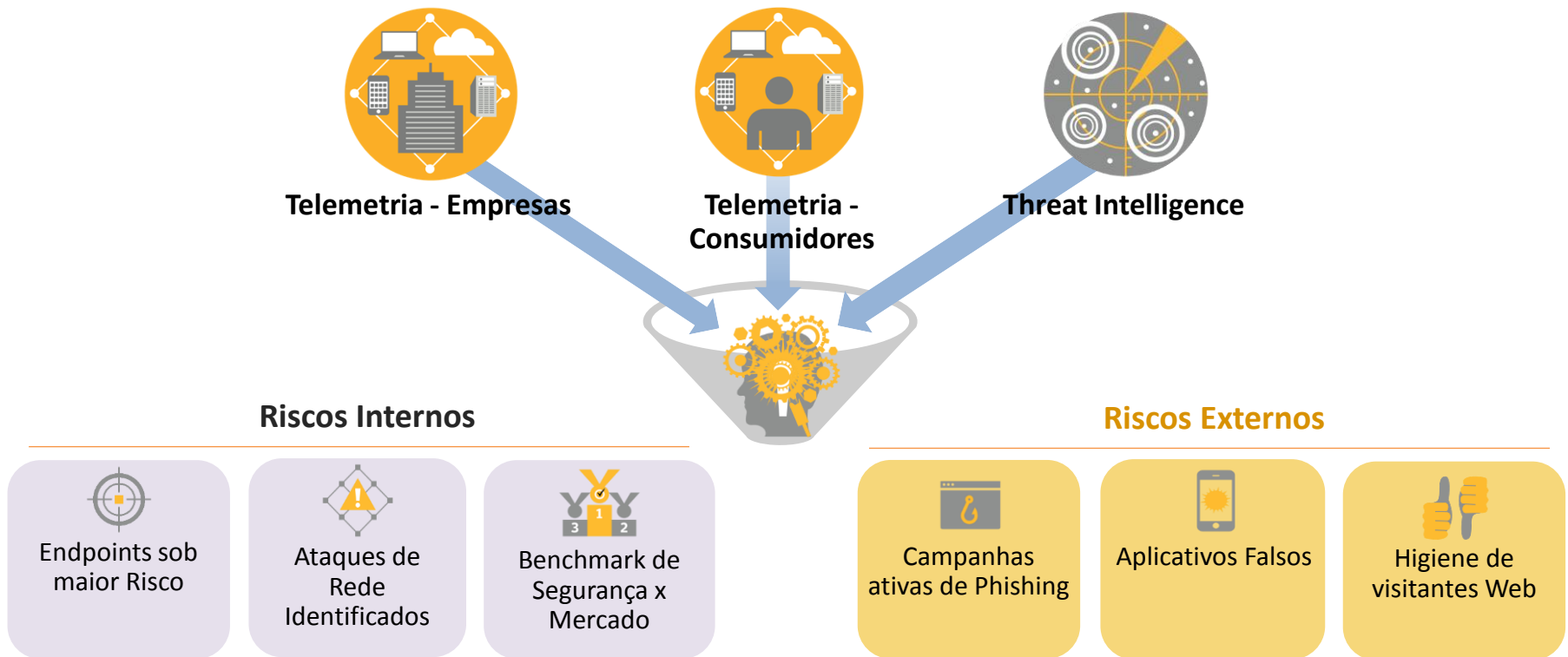
Disclaimer

Any information regarding pre-release Symantec offerings, future updates or other planned modifications is subject to ongoing evaluation by Symantec and therefore subject to change.

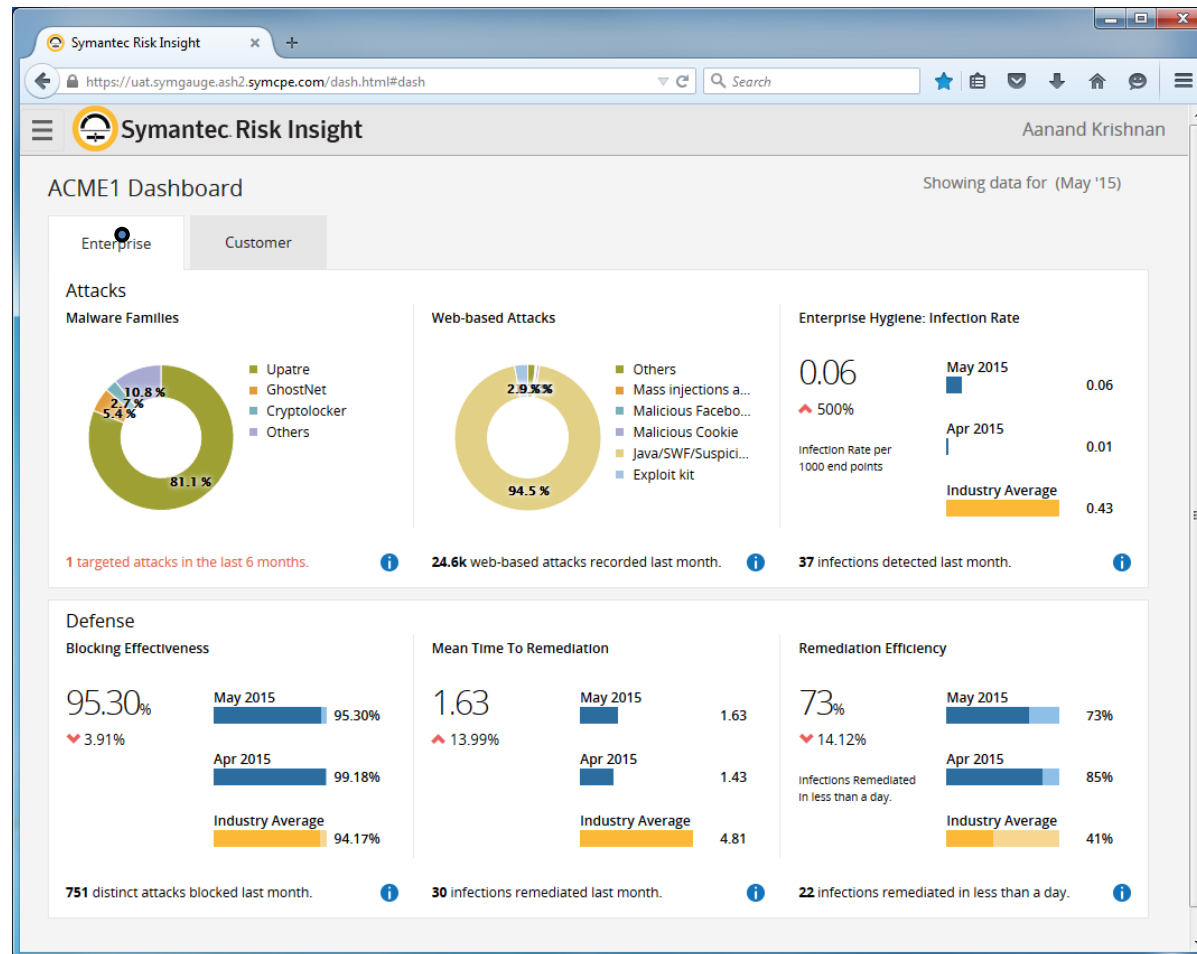
This information is provided without warranty of any kind, express or implied.

Customers who purchase Symantec offerings should make their purchase decision based upon features that are currently available.

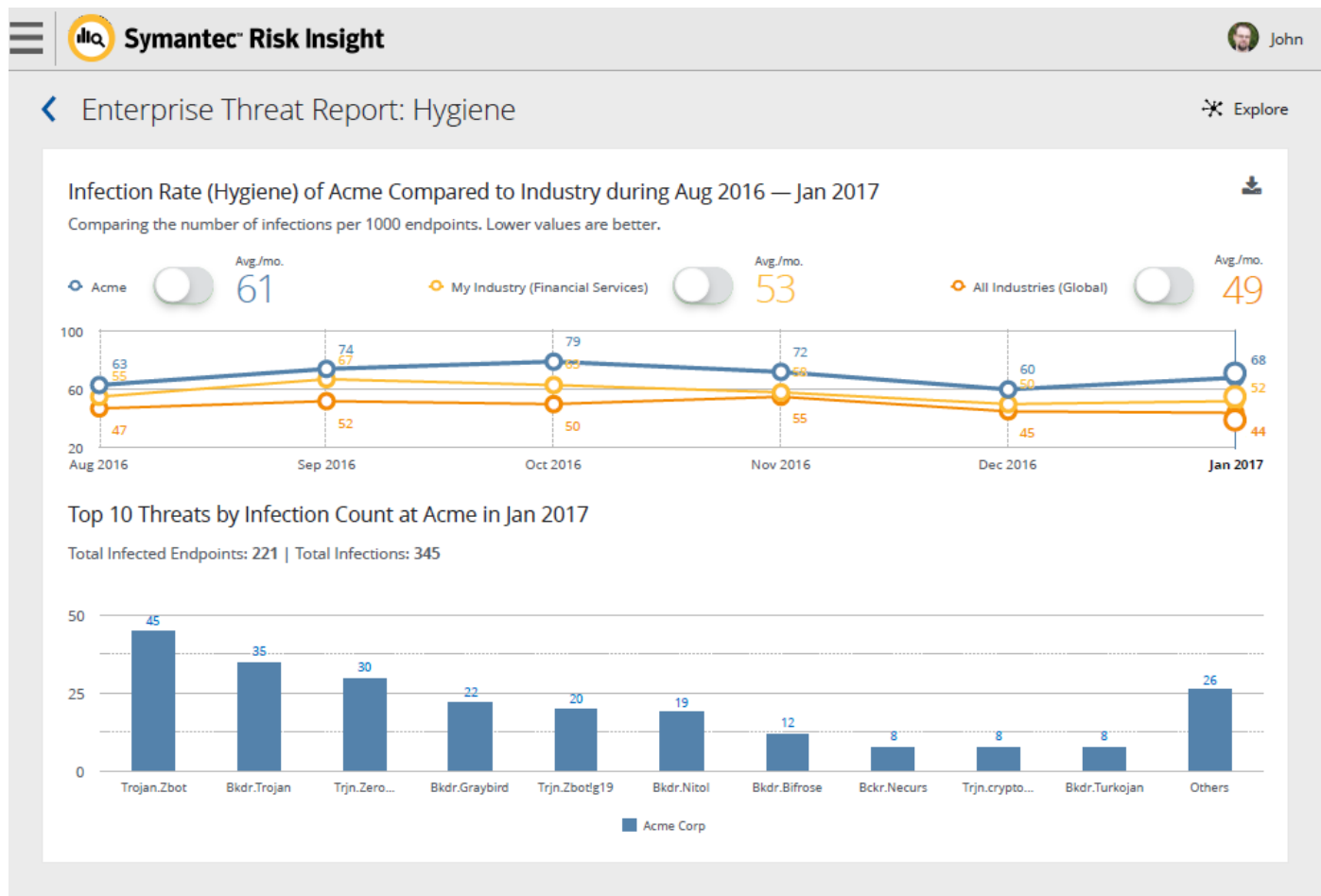
Utilizando Telemetria para avaliação de Risco e exposição à Vulnerabilidades



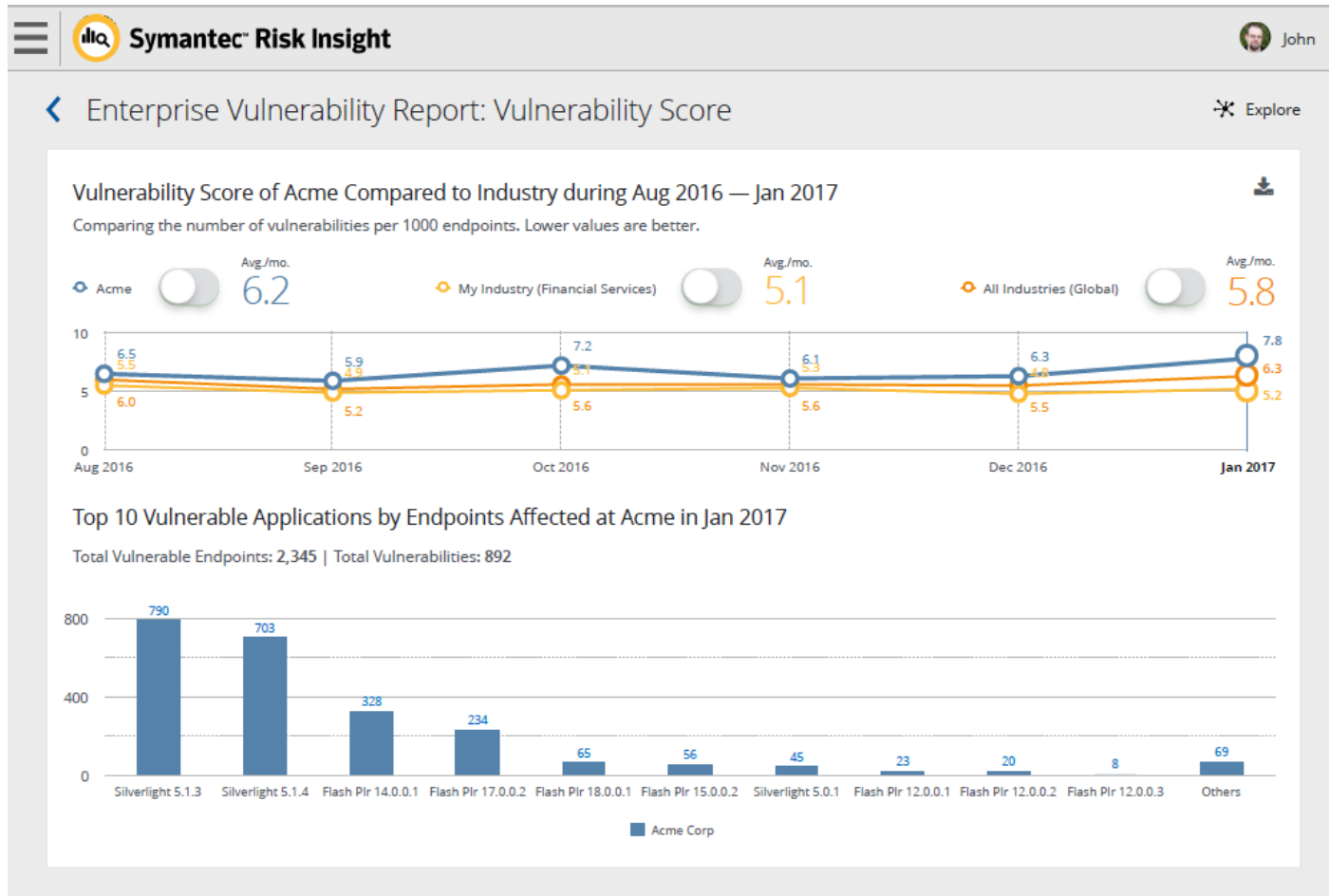
Risk Insight - Visão consolidada sobre risco em TI



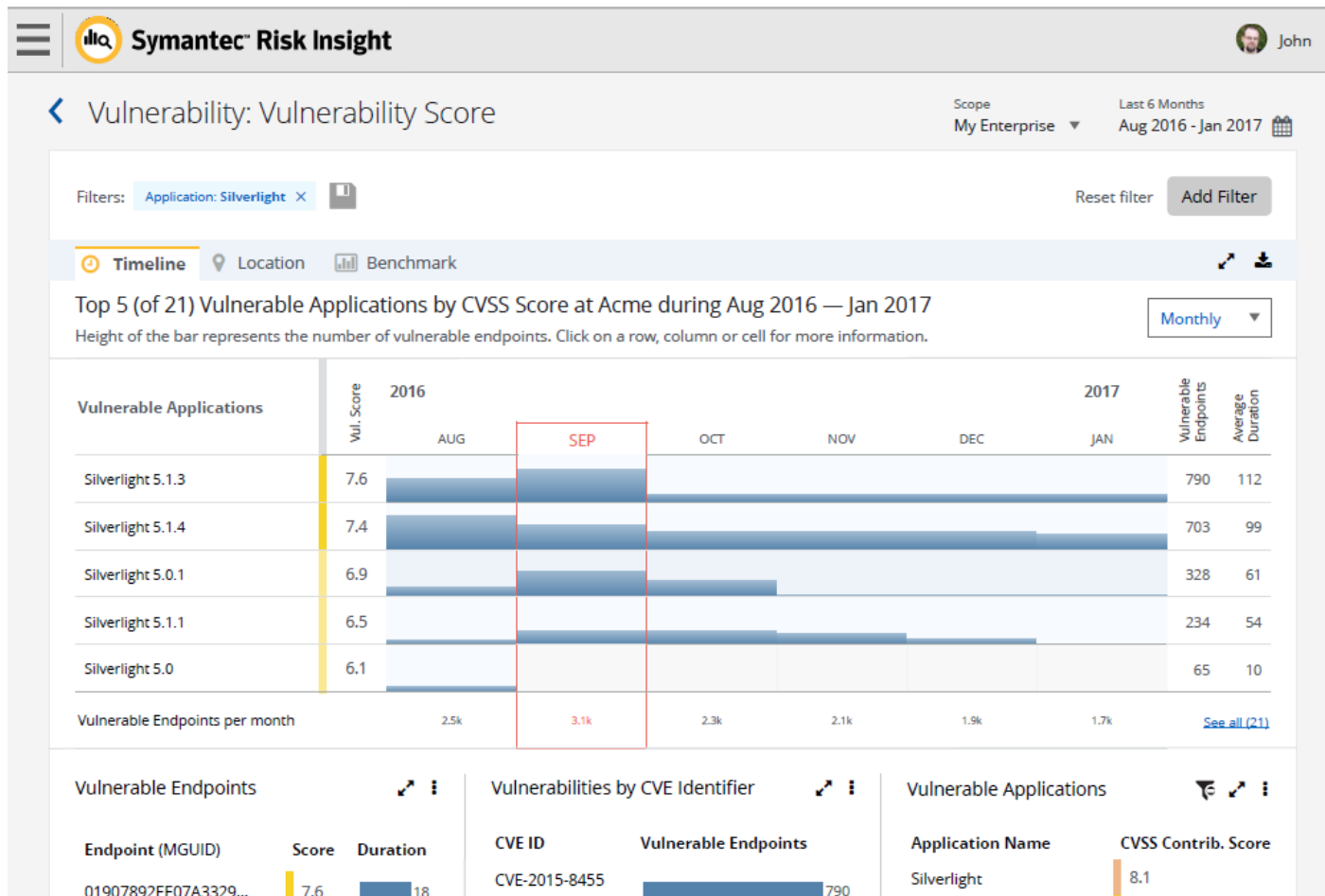
Risk Insight - Informações sobre grau de higiene



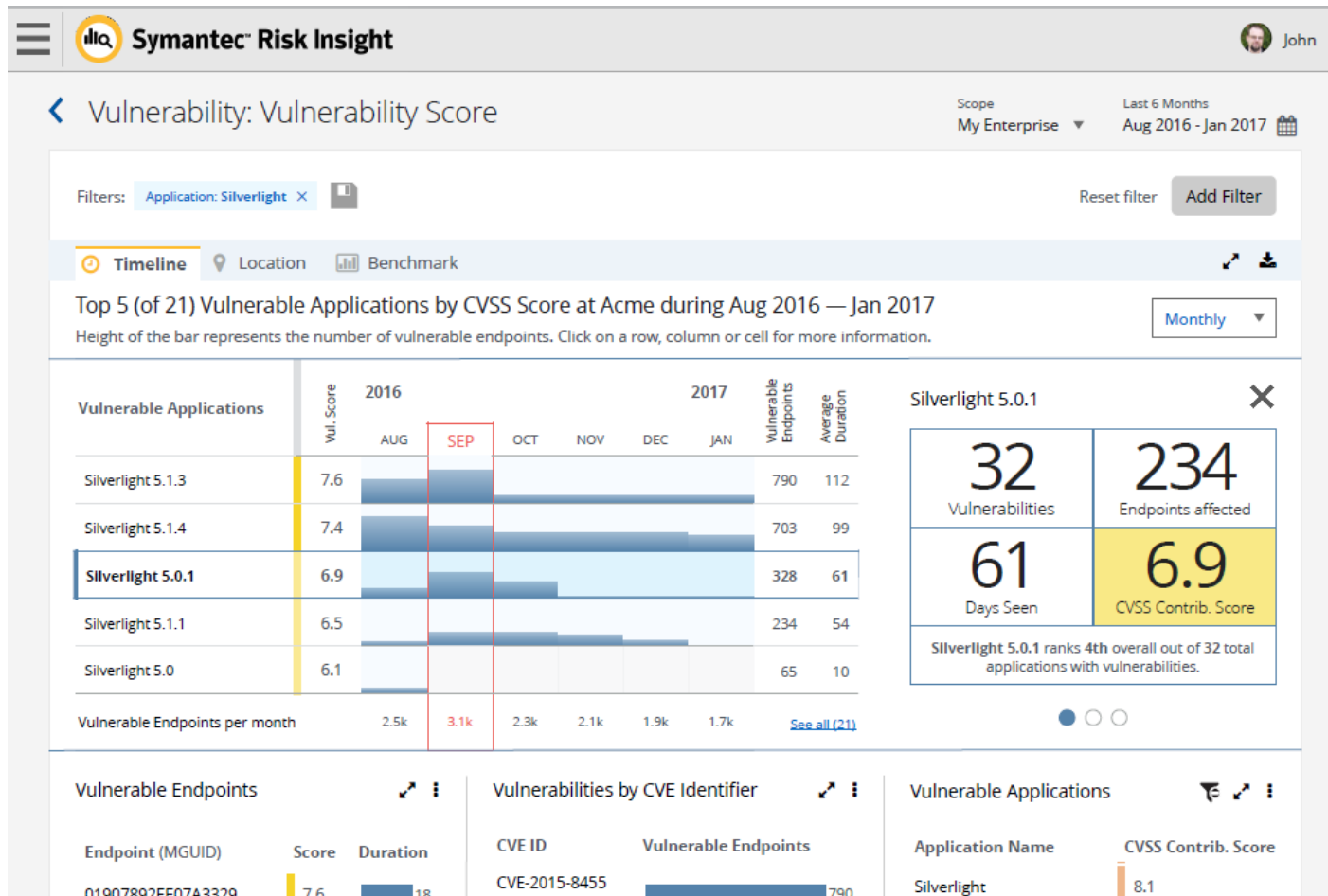
Risk Insight - Vulnerabilidades



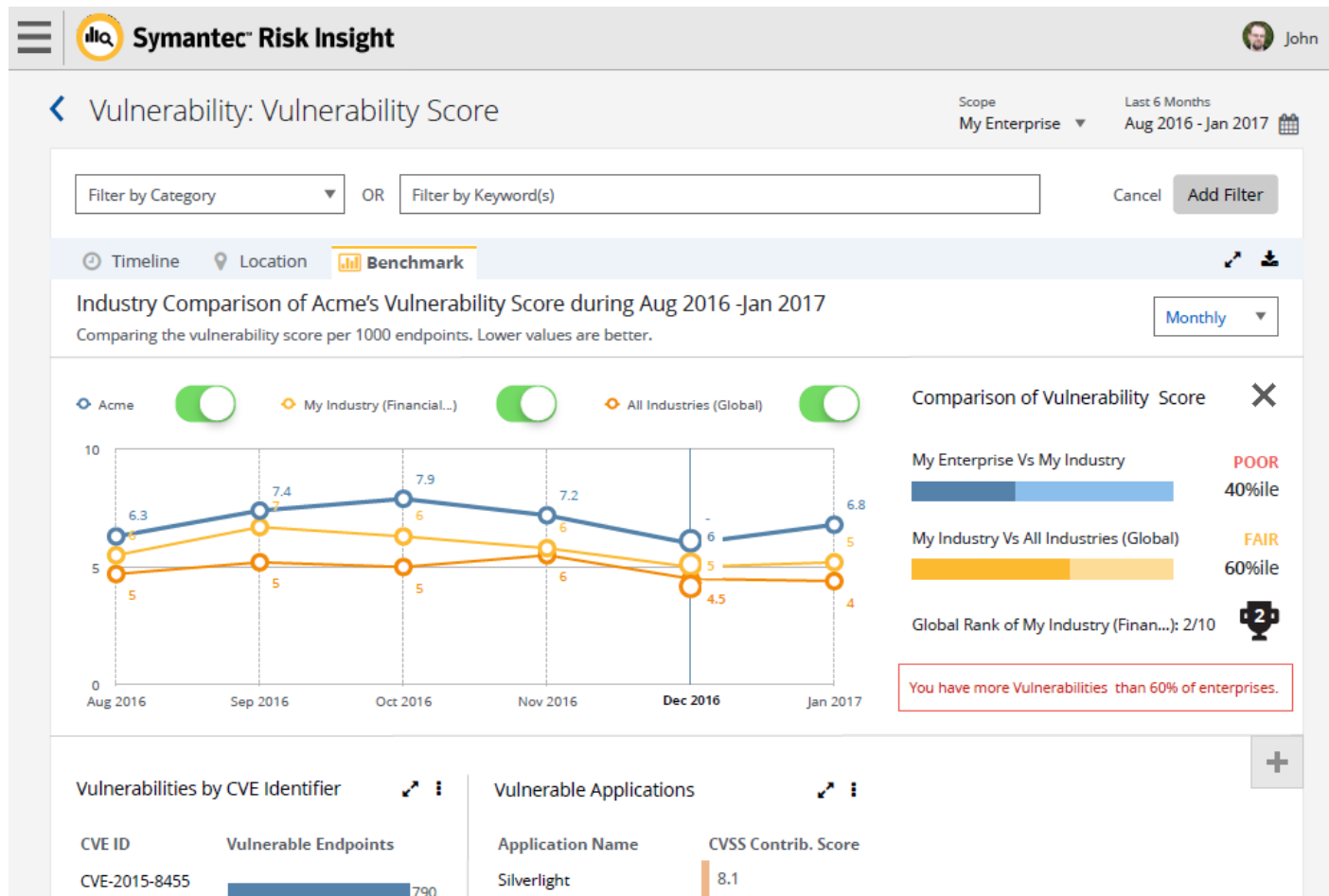
Risk Insight - Vulnerabilidades x CVSS Score



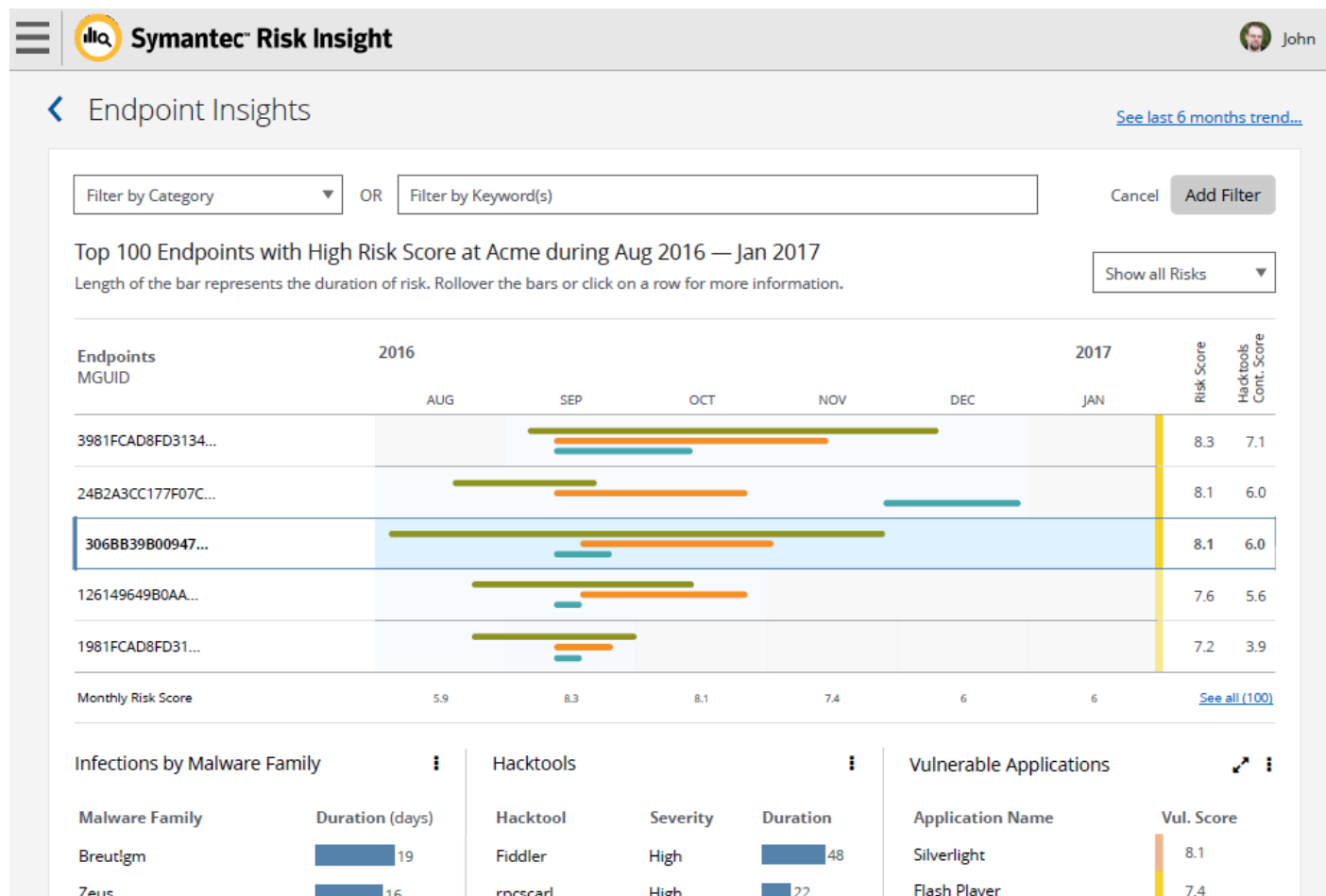
Risk Insight - Vulnerabilidades x CVSS Score



Risk Insight - Benchmark com Indústrias



Risk Insight in action - Endpoints com maior risco



Obrigado!

André Carraretto, CISSP
andre_carraretto@symantec.com