2017年 11 月 1 日

ラストライン合同会社

NSS Labs 2017 年の結果から得られた Lastline の優秀な検出能力について

Breach Detection System（以下「セキュリティ違反検出システム」と云う）を選択するとき、TCO (Total Cost of Ownership：総保有コスト)を決めることは重要な課題となっています。今回、NSS Labs は、Lastline を含む著名な7社のセキュリティ違反検出システムのテストを実施し、「2017 NSS Labs Breach Detection Comparative Report」と題したレポートを公開しています。この世界最大のテスト機関からのレポートは、それぞれの組織のために導入するセキュリティ違反検出システムを決定するために有効な情報を提供することを目的にしています。

Lastline の低い TCO と高いセキュリティ対策の有効性で優秀な評価

セキュリティ違反検出システムを選択するとき、バランスのとれた製品の総合的な価値を決定することは難しいですが、非常に重要なことです。導入時の価格または TCO だけで結論づけることは不十分であり、先見性にかけてしまいます。セキュリティ違反検出や防御に必要な能力が欠ける安価な製品を購入して後悔するお客様もいらっしゃいます。製品の価値を判断するには、正確な TCO 算出と、重大な損害が発生する前にセキュリティ違反を検出することがどれだけ効果的かを理解する必要があります。

セキュリティ違反検出システムの場合、NSS Labs はその価値を推測することを止めて定量化しています。

最新の「Breach Detection Systems Group Test」では、NSS Labs は、Lastline を含む 6 社7機種のセキュリティ違反検出システムでテストを実施しました。最も有用なレポートの観点は、NSS Labs が「Security Effectiveness」と提唱している、解析を回避するマルウェアを検知するそれぞれの製品の有効性と、TCO の両方をどのように定量的な評価を行うかです。これら2つの組み合わせた結果は、テストを行ったそれぞれのシステムの価値を完全に把握することが可能となります。

ここに、Lastline がどれだけ低い TCO で且つ高いセキュリティ対策の有効性があり、比類なき価値があるのか、NSS Labs によるテストのハイライトがありますのでご紹介します。

セキュリティ違反検出システムの TCO を正確に計算

NSS Labs は、代表的な企業の購入サイクルを正確に考慮して、購入から複数年間利用することを前提とし、それぞれのシステムに対する TCO の計算を行いました。

NSS Labs は以下の要素を取り入れました。

- センサーと関連する装置の購入費用
- 集中管理用のマネージメントシステムの購入費用
- インストールやメンテナンス、システムの維持に関する費用
- 毎年必要なメンテナンスやサポート、シグネチャアップデートなどのランニングコスト

TCO を計算するために、NSS Labs は、以下レポートから抜粋しているように、3 年以上利用するためのコストをすべて含んでいます。

Value	Description of Calculation
Year 1 Cost	Initial Purchase Price + Maintenance Cost + (Installation x Labor rate $/hr)
Year 2 Cost	Maintenance Cost
Year 3 Cost	Maintenance Cost
3-Year TCO	Year 1 Cost + Year 2 Cost + Year 3 Cost

3-Year Cost Calculation

しかし、テストではセキュリティ対策の有効性や過検知や誤検知、トータルコストの一部であるそれぞれのシステムがもつパフォーマンスを考慮して「Mbps」あたりの TCO を導き出しました。有効性とスループットを含めて考慮することで、それぞれ異なるシステムの「価値」をベースに比較を行うことで、レポートにあるように定量的な結論を導き出すことに成功しました。

TCO per Protected Mbps = 3-Year TCO/((Security Effectiveness x (1-False Positives)) x NSS-Tested Throughput)

NSS Labs TCO テストの結果

レポートから抜粋した以下の表は、評価検証を行った 7 製品の TCO の結果です。

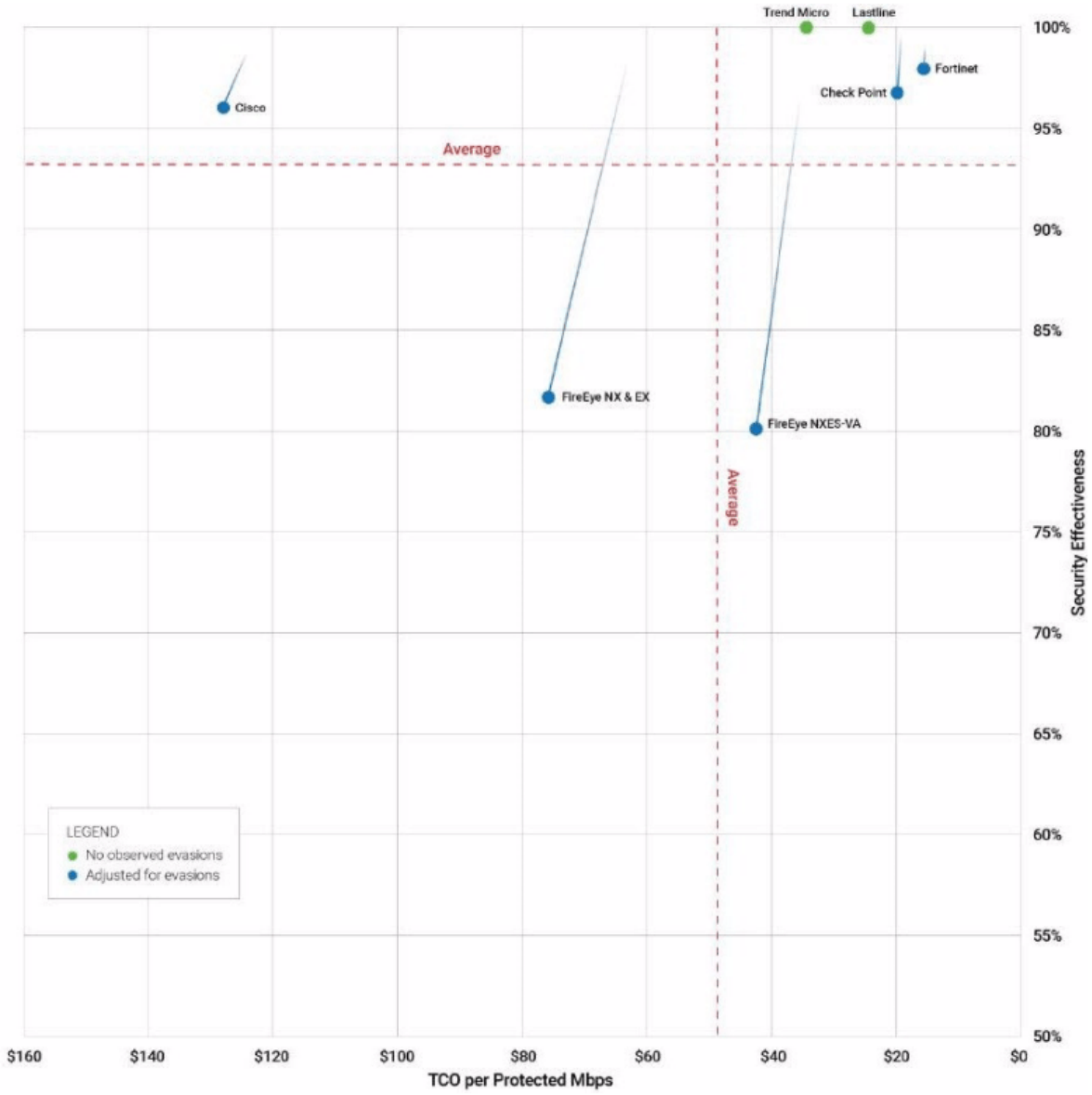
注目すべき項目は、「TCO per Protected Mbps（低いコストが高評価）」と「Security Effectiveness（高いパーセンテージが高評価）」の2列です。

Product	NSS-Tested Throughput (Mbps)	3-Year TCO (USS) (four devices + CMS)	Security Effectiveness	TCO per Protected Mbps
Check Point	5,667	$435,521	96.7%	$20
Cisco	750	$368,356	96.0%	$128
FireEye NX & EX	5,000	$1,240,156	81.7%	$76
FireEye NXES-VA	1,667	$228,424	80.2%	$43
Fortinet	8,667	$533,211	98.0%	$16
Lastline	3,000	$294,900	100.0%	$25
Trend Micro	8,667	$1,197,600	100.0%	$35

TCO per Protected Mbps

結果は、Lastline が、TCO per Protected Mbps を考慮したセキュリティ対策の有効性でパーフェクトな結果を得ることができました。

- Lastline は毎年のメンテナンス費用が不必要な唯一のシステムで、Lastline の TCO そのものを下げる結果でした。 3 年間以上の TCO で計算した場合は、テストを行った他のどのシステムと比べても、最も低い TCO となりました。
- Lastline の TCO per Protected Mbps は、テストを行った他のシステムと比較して約半分となりました。3 年間以上の TCO は、全 7 製品の平均が 49 米ドル（2017 年11月 1 日の為替レート 1 米ドル 113.67 円で 5,570 円） per Protected Mbps に対して、Lastline ではたったの 25 米ドル（同レートで 2,842 円）となりました。
- Lastline の 2017 年の結果は昨年に続き、100%のパーフェクトな結果となり、低い TCO と高いセキュリティ対策の有効性を証明したもので、3 年連続して NSS Labs の推奨システムとなりました。



NSS Labs 2017 Security Value Map (SVM) for Breach Detection Systems (BDS)

レポートは Lastline の総合的な価値を証明

NSS Labs のレポートは、更にセキュリティ対策の有効性が含まれています。レポートでは、「セキュリティ対策の有効性が購入価格よりも高いシステムは、適切な価値があると見なされる」と記述されています。

以下のレポートの中の購入価格とセキュリティ対策の有効性の表では、Lastline は総合的なセキュリティ対策の有効性は最も高く、712,323 米ドル（同レートで 80,969,755 円）となっており、システム購入価格よりも 144% 高くなっており、他のシステムの約半分となっています。

Product	Purchase Price	Security Effectiveness Value	Delta	% Delta
Check Point	$205,060	$413,489	$208,429	102%
Cisco	$211,652	$136,747	($74,905)	-35%
FireEye NX & EX	$613,600	$465,573	($148,027)	-24%
FireEye NXES-VA	$114,232	$114,232	$0	0%
Fortinet	$214,998	$558,268	$343,270	160%
Lastline	$292,500	$712,323	$419,823	144%
Trend Micro	$664,000	$569,858	($94,142)	-14%

Purchase Price vs. Security Effectiveness Value

「NSS Labs 2017 年 セキュリティ違反検出システム結果レポート」のダウンロード

NSS Labs 2017 BDS Group Test results は、こちらからダウンロード可能です。

NSS Labs の結果に関する Lastline のブログも併せてご覧ください。

- Lastline Ranks Highest in Security Effectiveness in NSS Labs Breach Detection Systems Group Test - Again
- How Lastline Enterprise Keeps Earning NSS Labs Highest Score in Breach Detection

Lastline, Inc.について https://www.lastline.com

米国 Lastline 社は、多くのセキュリティ研究機関やセキュリティベンダーに利用されているバイナリファイル分析「Anubis（アヌビス）」、Web サイト脅威分析「Wepawet（ウェパウェット）」の開発者により、2011 年に設立されました。設立メンバーは、世界的に優れたサイバーセキュリティ学術研究者、エンギン・カーダ(Engin Kirda：ノースイースタン大学)、クリストファー・クルーゲル(Christopher Kruegel：カリフォルニア大学サンタバーバラ校)、ジョバンニ・ヴィーニャ(Giovanni Vigna：カリフォルニア大学サンタバーバラ校)の 3 名で、15 年以上の研究開発成果を基に次世代サンドボックス技術を製品化し、APT（Advanced Persistent Threat）を含む高度なサイバー攻撃とゼロデイ攻撃に特化した、比類ない検知能力と低誤検知のマルウェア防御ソリューションを提供しており、OEM 提供も含めて世界で 3 万社以上の導入実績があります。

本記事の連絡先：

ラストライン合同会社

〒100-0005

東京都千代田区丸の内 1-8-3 丸の内トラストタワー本館 20F

TEL：03-5288-5386　FAX：03-5288-5686

Email：info.Japan@lastline.com