CYLANCE

# ENTERPRISE CAMPAIGN
# CHANNEL SALES PLAYBOOK

# Introduction

MAIN MENU

**Purpose:** Use this Enterprise Campaign Sales Playbook to help qualify and sell prospects for Cylance solutions and security service offerings.

**Who should use it:** Sales professionals who wish to improve their knowledge about the depth and breadth of Cylance solution and service offerings will benefit from reviewing this Playbook. Even seasoned sales professionals will find value, especially by using the Unrecognized Problems section that will help drive immediate customer action.

**How to use this guide:**

**Qualify Customers and Determine Appropriate Service Offerings via:**

- Initial Qualification Questions
- Sales Questions
- Personas / Power / Plan

**Utilize Advanced Resources Specific to Each Solution:**

- Thought Leadership
- Value Propositions
- Sales Questions
- Unrecognized Problems
- Training and Sales Enablement Assets
- Cylance Resources

# Main Menu

MAIN MENU

**Main Menu Button** – Click on the Home Icon to return to the **Main Menu**, where you can move between sections.

**Qualification Questions / Power / Problems** – Start here, especially with a net new customer, to ask initial Qualification Questions to uncover potential Problems related to Cylance Solutions and prospect Power roles within an organization.

**Sales Questions** – This section includes Problem, Value, and Solution questions and information for each persona.

**Unrecognized Problems** – This menu lists several potential Unrecognized Problems to help increase Value and urgency

**Cylance Solutions** – Information related to Cylance Solutions and Services including Value Propositions, Thought Leadership, and more

**Industry Thought Leadership** – Sales Enablement Thought Leadership and Sales Tools to drive action.

**Resources** – Links to Cylance resources to find Collateral, Training Courses, Sales Enablement Assets, and Contacts to help you sell.



CYLANCE

# Campaign Overview & Sales Talking Points

The Enterprise Awareness **Optimize Your Business** Campaign is an adjunct to, and aligns closely with, the Cylance **Think Beyond** campaign. For this campaign, we are targeting three primary roles / personas: Decision Makers, Evaluators, and Influencers. Decision Makers are usually C-Level, VP or Sr. Directors and are involved in specific or final process decisions. They often delegate technical and evaluation tasks to Evaluators and others on their team. DMs are typically more instinctual and strategic in nature and are driven more by risk, cost, and impact avoidance.

**Decision Makers** are typically CISOs or VPs of IS in most organizations. Research shows they are transitioning from Guardians and Technologists to Advisors and Strategists. They are now more interested in strategic thought leadership than details about specific technologies. As such, this campaign provides Thought Leadership content and approaches that should resonate with most Decision Makers.

CISOs and VPs are burdened with a great deal of pressure from other C-Suite executives and Board Members to implement security solutions that will prevent cyber-attacks that could damage the firm's reputation with customers. In fact, they are three times more concerned about this than about applications and technologies. They are also placing unrealistic expectations on CISOs to deploy effective solutions practically overnight. Therefore, discussions with Decision Makers should focus on three things:

1. (Emotional appeal) Optimized business; easing the security skills shortage, simplified management; increased visibility, reduction of complexity and interoperability within their existing security solution; and compact, efficient AI/ML local model
2. (Instinctual appeal) Continuous proactive prevention of malware execution to avoid the need to report publicly and cause brand reputation damage (reactive solutions don't prevent execution)
3. (Logical appeal) Driving predictability; cost-avoidance by mitigating or eliminating the need to reimage/provision systems after a malware compromise; reduction in man-hours of scarce security resources to manually manage existing security solutions, meeting productivity targets through 1) less security interruptions and 2) downtime due to breach recovery and finally, easy integration & metrics reporting

C-Level execs are primarily interested in the prevention of brand and company damage and customer loss due to malicious attacks and security breaches resulting in the loss of trust and Intellectual Property. Campaign messaging and sales enablement tools ire designed to speak to this concern.

# Campaign Overview & Sales Talking Points

**Evaluators** are usually more technical and logical and are involved in the evaluation and/or deployment of solutions. They are often tasked with narrowing down the list of prospective vendors to three or less and then doing POCs and tests to recommend the “final winner.” Partners who engage with these individuals earlier in the Buyer’s Journey can often influence the prospect’s desired capabilities, technical aspects and other RFP “lockout” specs. While most sales pros would prefer to engage latter in the cycle when prospects are almost ready to issue POs, but by this time most Evaluators are leaning heavily toward a partner that engaged earlier in the cycle, fostered a relationship, and influenced the list of requirements. Most Evaluators are interested in saving time, effort, and face—the latter refers to the ability to lower company impacts (e.g; reimaging hundreds of systems) or user disruption (e.g; eliminating daily scans).

**Influencers** have no authority and are not involved in the decision-making or solution evaluation process but should not be ignored or discounted. They can strongly influence the decisions made by Evaluators and Decision Makers. They can also impart valuable information and open doors to others. However, their enthusiasm to help should not be construed as a confirmation of a purchase opportunity. Influencers tend to be more emotional and are motivated by a desire to help their firm and colleagues. They can be an excellent source of company situational information (e.g; recent breach, merger, personnel changes, growth metrics, compliance and audit requirements, user concerns and disruptions, evaluation and purchase processes, etc.).

# LinkedIn Social Selling

**LinkedIn Social Selling with Sales Navigator**

LinkedIn now has almost 500 million contacts and can be one of the most powerful prospecting tools we have in our arsenals. The best way to use Sales Navigator is to follow the directions outlined below and search on appropriate contacts and connect with them, as well as any leads provided by marketing. This allows the use of LinkedIn Messaging rather than relying on expensive and limited InMails. Below are recommended Connect Request and Thank You messages.

**CxO**

**Connect Request Messages:**

- I'd like to Connect so I get connect you with one of our security experts to gain your expert opinion about our next generation security platform
- I'd like to Connect so I can offer you [incentive]
- I'd like to Connect so I can get you a copy of the Gartner Redefining Endpoint Security report [or] Carbonview IT Decision Maker study [or] Forrester Total Economic Impact Security study
- I'd like to Connect so I can send you an invite to a Leadership Forum Event.
- I'd like to Connect so I can invite you to join the LinkedIn Security Leaders Group [Cylance's LinkedIn group]
- I noticed we're both in the LinkedIn [insert] group and thought we should Connect.
- We have several mutual 1st-Level LinkedIn Connects so I thought we should Connect.

**Connect Thank You Messages:**

- Thanks for Connecting, I'd like to offer you [incentive] to schedule a research call with one of our security experts to gain your expert opinion about a next generation security platform. Are you open for a brief call next [day] or [day]?
- Thanks for Connecting, here's a link to the [campaign asset] at this link: [landing page link]
- Thanks for Connecting, here's a link to the Security Leaders Group: https://www.linkedin.com/groups/113049/profile
- Thanks for Connecting, here's a special invite to a Leadership Forum Event [link]
- Thanks for Connecting, if you're concerned about [topic], I recommend this excellent [white paper/video/article/research report].

**Connect Follow-up Messages:**

- I noticed that you downloaded a copy of the [campaign asset] and I'd like to offer you [incentive] and schedule a research call with one of our security experts to gain your expert opinion about our next generation security platform. Are you open for a brief call next [day] or [day]?
- I noticed that you signed up for a Leadership Forum Event and thought you'd like to join us for a special webinar to learn why AI AV is 99% effective against known and unknown threats. [link]
- I noticed that you joined the LinkedIn Security Leaders Group and thought you'd like to know that over 51% of breaches include malware, and the average cost per breach is $4 million. If you'd like to learn how to defeat malware, consider joining our next webinar. [link]
- I noticed that you read the white paper about [topic] and thought you'd like to schedule a solution demo to learn why our AI AV is 99% effective against known and unknown threats. If so, here's the link: [asset link]

# LinkedIn Social Selling


**Non-CxO / Evaluator / Influencer**
**Connect Request Messages:**
• I'd like to Connect so I can offer you [incentive]
• I'd like to Connect so I can get you a copy of the Gartner Redefining Endpoint Security report [or] Carbonview IT Decision Maker study [or] Forrester Total Economic Impact Security study
• I'd like to Connect so I can send you an invite to a Special Security Event and to our LinkedIn Security Leaders Group [Cylance's LinkedIn group]
• I noticed we're both in the LinkedIn [insert] group and thought we should Connect.
• We have several mutual 1st-Level LinkedIn Connects so I thought we should Connect.

**Connect Thank You Messages:**
• Thanks for Connecting, I'd like to offer you [incentive] to schedule a research call with one of our security experts to gain your expert opinion about our next generation security platform. Are you open for a brief call next [day] or [day]?
• Thanks for Connecting, here's a link to the [campaign asset] at this link: [landing page link]
• Thanks for Connecting, here's a link to the Security Leaders Group: https://www.linkedin.com/groups/113049/profile
• Thanks for Connecting, here's a special invite to an upcoming Special Security Event [link]
• Thanks for Connecting, if you're concerned about [topic], I recommend this excellent [white paper/video/article/research report].

**Connect Follow-up Messages**
• I noticed that you downloaded a copy of the [campaign asset] and thought you'd like to schedule a call to learn why legacy anti-malware leaves you vulnerable to early attacks. If so, I'm open on [date] or [date], which is best for you?
• I noticed that you signed up for a Leadership Forum Event and thought you'd like to join us for a special webinar to learn why AI AV is 99% effective against known and unknown threats. [link]
• I noticed that you joined the LinkedIn Security Leaders Group and thought you'd like to know that over 51% of breaches include malware, and the average cost per breach is $4 million. If you'd like to learn how to defeat malware, consider joining our next webinar. [link]
• I noticed that you read the white paper about [topic] and thought you'd like to schedule a solution demo to learn why our AI AV is 99% effective against known and unknown threats. If so, here's the link: [asset link]

# Qualification Questions

**Describe your current role within your organization.**

Start with this question to uncover the prospect's primary role.

**Are you involved in the decision-making process for security solutions or services?**

Ask this to uncover the prospect's decision-making involvement.

**Decision Maker?** NO — YES

**Do you Evaluate, Deploy, or Manage security solutions or services?**

**Evaluator?** NO — YES

**Do you influence security solutions or services decisions?**

**Influencer?** NO — YES

**UNQUALIFIED?**
**This prospect may not be qualified for Cylance.**



CYLANCE

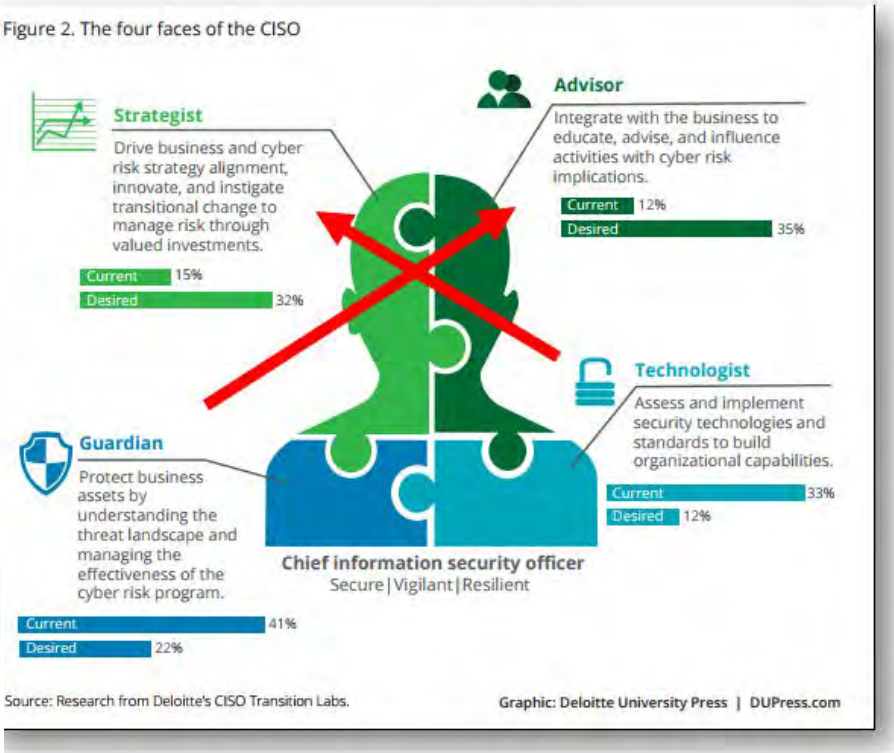
Persona / role-related Sales Questions to uncover specific opportunities.

Industry Thought Leadership information to deliver compelling reasons to take action.

Value Propositions for Cylance solutions to help entice and motivate prospects.

Resources page for Cylance solutions with links to assets for Industry Thought Leadership, Customer Collateral, Training, Sales Enablement, and Cylance Contacts.

# Persona
# Decision Maker


| Type | More instinctual |
|---|---|
| Titles | Chief security officer, CISO, VP/Dir Security |
| Job Focus | Managing security ops, selecting tactical security products, responding to audit & compliance mandates, minimizing bad publicity and security costs |
| Pain Points | Sea of alerting and reports, evolving threats, siloed, limited legacy security architecture, data breaches |
| Info Sources | Peers, analysts, trade shows, industry associations, |
| Preferred Assets | Keynotes, demos, POCs, research & analyst reports, white papers |
| Triggers | Strategic, proven, reliable, industry accolades, risk aversion, compliant, high value, superior |

# Decision Maker Sales Questions

## Business Issues:

**Decision Makers are concerned with organizational risk and all the countermeasures associated with managing it. They dictate the need for security-related controls, training, process, programs and personnel.**

## Unrecognized Problems:

U

After uncovering Concerns & Problems by asking the below questions, click on the U to select Unrecognized Problems.

## What concerns do you have about…

- Undiscovered breaches and preventing APT or malware attacks?
- Increased risks of public exposure & lawsuits due to a security breach?
- Months of downtime & high costs due to a serious malware attack?

## How would it impact you if…

- Your current solution kept your staff from working on other projects?
- Your team was burdened with frequent and significant updates?
- Zero-day malware was not discovered prior to execution?

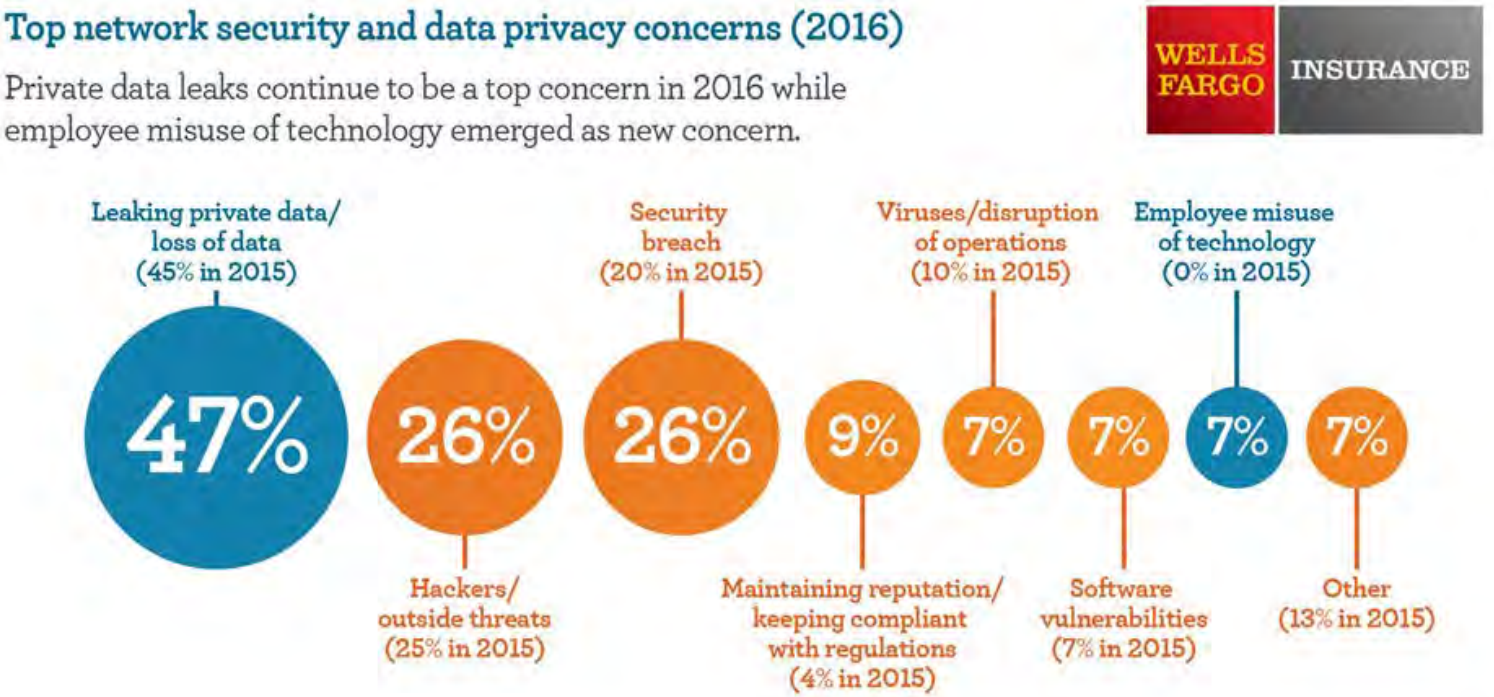
## What if you could…

- Realize 30% more system performance and avoid continuous scans?
- Avoid reacting with signature updates to stop tomorrow's threats?
- Avoid spending up to $4M to clean up a malicious malware attack?



CYLANCE

# Persona
# Evaluator




| Type | More logical |
|---|---|
| Titles | Security center ops director, manager, sr. manager, security admin/manager/director/engineer |
| Job Focus | Managing SOC, staffing, issues, desktop/laptop infrastructure, user uptime & experience |
| Pain Points | Staff retention, incident numbers, security levels, outages, complexities, patch cycles, user-experience |
| Info Sources | Google, peers, analysts, trade shows, industry associations, |
| Preferred Assets | Demos, customer references, POCs, white papers, research & analyst reports, trade shows, |
| Triggers | Tactical, pragmatic, proven, reliable, percentages, graphs, charts, numbers, statistics, next generation, technical |



CYLANCE

# Evaluator
# Sales Questions

## Business Issue:

**Evaluators are concerned with evolving threats, solution silos, limited legacy security architectures, too many alerts & false positives, ease of management and reporting, lack of visibility, constantly putting out fires, incidents & outages, patch cycles, and complexities**

## Unrecognized Problems:

U

After uncovering Concerns & Problems by asking the below questions, click on the U to select Unrecognized Problems.

## What concerns do you have about…

- Keeping the IR team caught up on malware-related caseloads?
- Increased risks due to expanding attack surfaces such as flash & cloud?
- Using reactive EPP that could could take 120 days to detect & resolve?

## How would it impact you if you had…

- Complex solutions that are difficult to manage and disruptive to users?
- Reactive security that did not prevent malware from executing?
- Inefficient security that did not block over 99% of malware attacks?

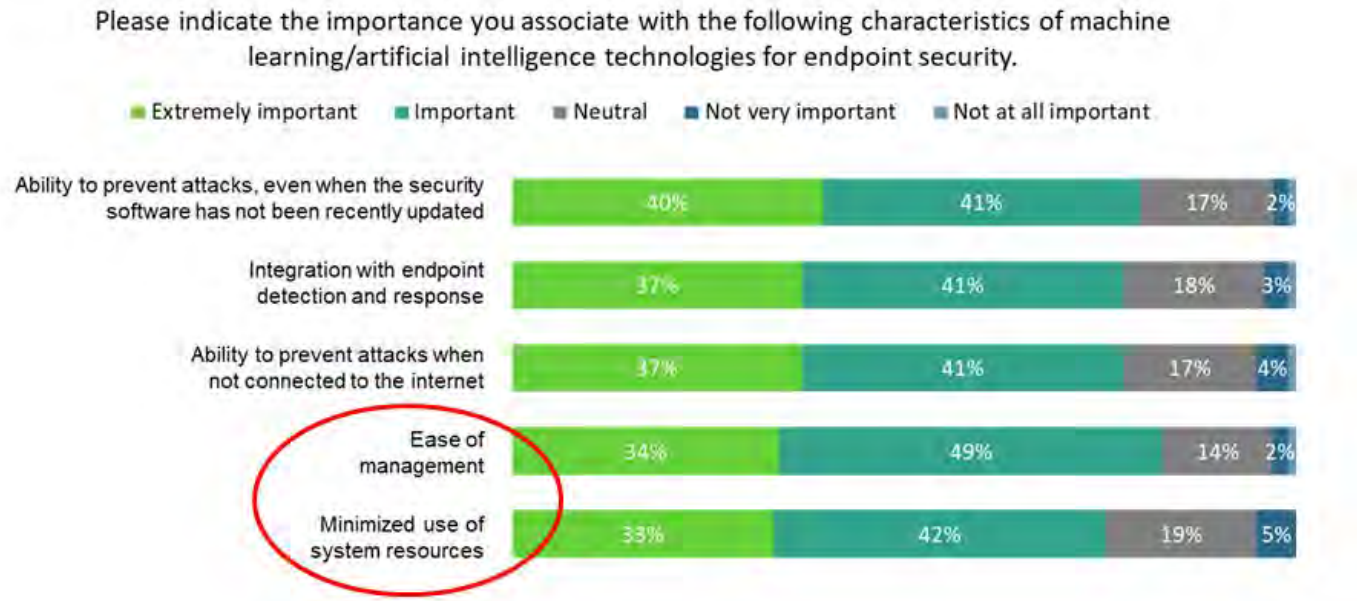
## What if you could…

- Avoid urgent patch cycles to stop publicly sensationalized
- threats?Avoid complex configurations or lengthy exception lists?
- Manage all OSs including VDI with the same solution?



CYLANCE

# Persona
# Influencer




Source: Enterprise Strategy Group 2017 Survey, 300 IT security professionals

| Type | More emotional |
|---|---|
| Titles | Security operations, analyst, architect, engineer, SOC security analyst |
| Job Focus | Monitoring, detecting, and preventing attacks and data leaks, staying compliant, helping the CISO understand how all the parts fit together, investigating security incidents, taking incident response actions |
| Pain Points | Evolving threats, siloed, limited legacy security architecture, sea of alerting and reports, data breaches, lack of visibility, constantly putting out fires |
| Info Sources | Analysts, peers, industry associations, trade shows, Google |
| Preferred Assets | White papers, research and analyst reports, trade shows, Google, demos, POCs, white papers |
| Triggers | Helpful, simple, easy, proven, customer success stories, industry accolades, analyst opinions, cutting edge, recommended |



CYLANCE

# Influencer Sales Questions

## Business Issue:

**Influencers are often concerned with evolving threats, compliance audits, productivity disruptions due to daily scans or performance issues, and customer loss or brand damage due to data breaches.**

## Unrecognized Problems:

U

After uncovering Concerns & Problems by asking the below questions, click on the U to select Unrecognized Problems.

## What concerns do you have about…

- Eliminating less effective security controls to recapture budget?
- The inability to expand the use of flash and cloud due to attack risks?
- The impact of technical controls on users and server infrastructures?

## How would it impact you if…

- Users had disruptions and dramatic decreases in system performance?
- You could not scale up the number of managed endpoints quickly?
- Users were not protected against the latest threats both off & online?

## What if you could…

- Rollout and upgrade without disruption and avoid migrating data?
- Avoid costly process of ripping & replacing your current solution?
- Have confidence in your ability to prevent patient zero infections?



CYLANCE

# Unrecognized Problems




## U Problems

- Breach Concerns
- Complexities or Siloes
- Compliance Concerns
- Cost or Budget Concerns
- Detection & Response Issues
- Email or Phishing Attacks
- Expertise & Staff Constraints
- False Positive Alerts
- Outages or Downtime
- Performance Concerns
- Reimaging Issues
- Setup or Deployment Needs
- Unknown Malware
- Visibility Concerns

## S Solutions

- CylancePROTECT
- CylanceOPTICS

*Click on a Problem for Sales Questions*
*Click on a Cylance Solution for Details*

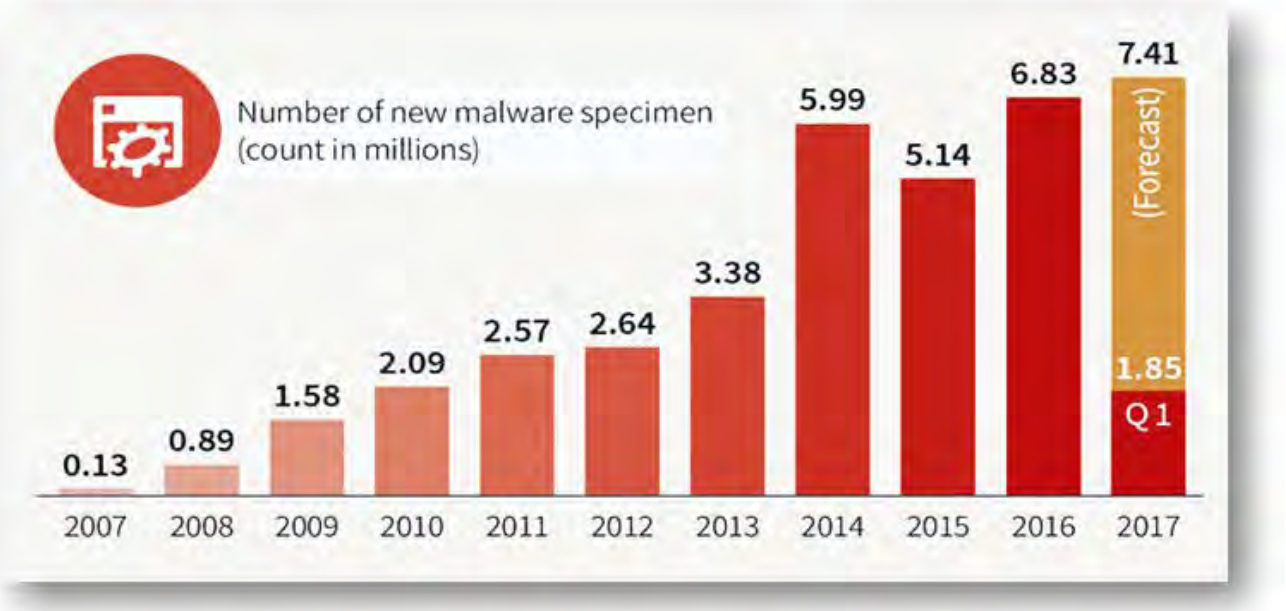


CYLANCE

# Breach Concerns: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem





Sources: AV-Test, Q1 2017; Ponemon Institute

## Thought Leadership Information

- ✓ Emotional: A recent Gartner report says that legacy EPP is obsolete and more difficult to manage.
- ✓ Instinctual: An AV-Test report shows that the number of malware specimens has doubled in the past four years to over 7 million.
- ✓ Logical: Ponemon Institute calculated that it can take over 120 days to detect and resolve an attack at a cost of almost $4M.

# Breach Concerns: Customer Unrecognized Risks

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

**Problem** (Open)

**What concerns do you have about your current endpoint protection platform being outdated? Or that it's reactive in that it is not activated until after malware has executed?**

Use this question to setup the Unrecognized Problem

**Solution** (Probe)

**What if your current EPP / AV solution proactively employed artificial intelligence and machine learning to prevent 99% of malware attacks before they execute?**

Use this question to setup the Unrecognized Problem

**Thought Leadership** (Open)

**The 2017 U.S. State of Cybercrime Survey shows that the average time for intrusion discovery is growing and it's now over 90 days. Ponemon Institute discovered that it then takes over 30 days to resolve the incident, which can cost more than $32,000 per day. Combined, that's over 120 days at a total cost of almost $4 million. That's why Gartner says that reactive EPP is now obsolete.**

**Unrecognized Risks** (Confirm)

**How would it impact you to have newer technologies, such as artificial intelligence and machine learning, that proactively prevented over 99% of malware attacks before they executed?**

**Action** (Open)

**Cylance is committed to helping firms like yours avoid the costly consequences of using legacy reactive EPP by considering more modern proactive AI solutions. Let's talk about a plan to do this…**

S

CLICK to go to the Cylance Soutions information section

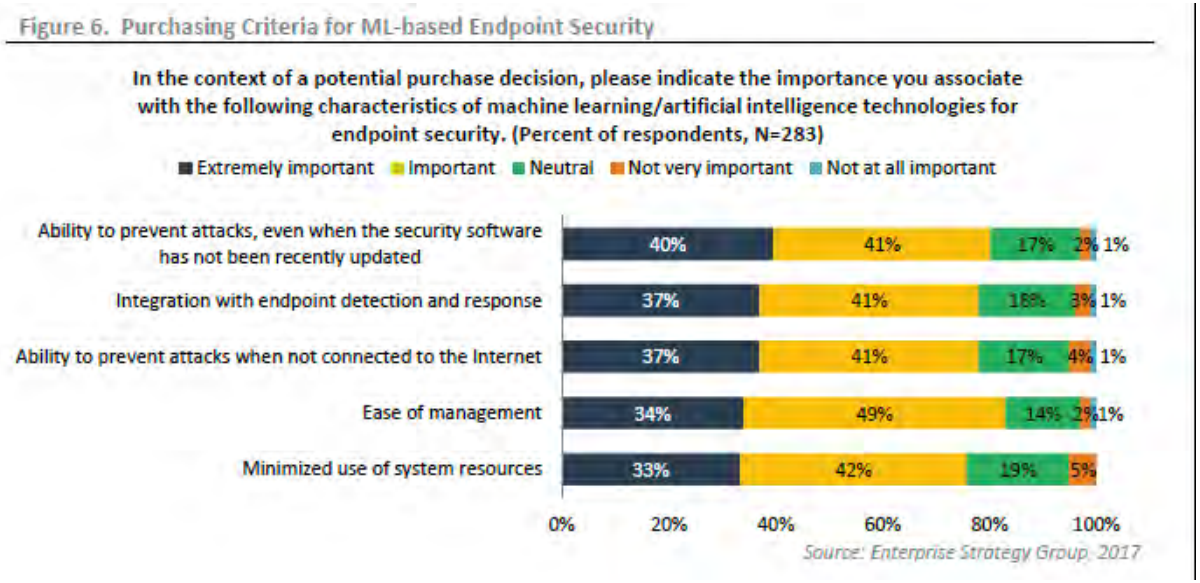


CYLANCE

# Complexities or Silos: Thought Leadership

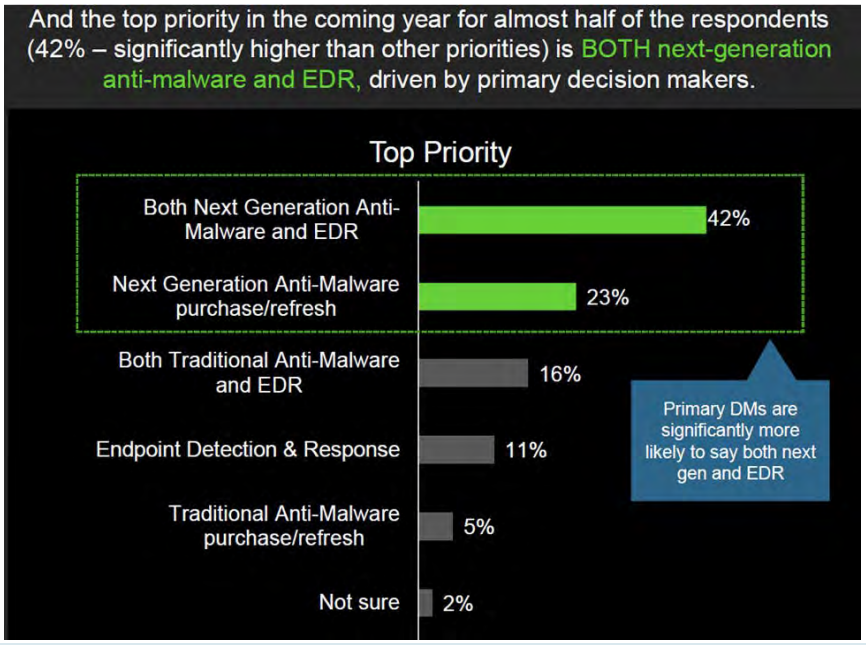
**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem




## Thought Leadership Information

- ✓ Emotional: Ease of management & minimized resource use are two of the most important solution criteria.
- ✓ Instinctual: The Gartner Redefining Endpoint Protection report says that legacy EPP is no longer effective.
- ✓ Logical: Decision-Makers are significantly motivated to eliminate silos and combine EPP & EDR.




Source: Carbonview Study 2017

# Complexities or Silos: Customer Unrecognized Problem

Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.

**Problem** (Open)

What concerns do you have about maintaining complex security solution silos? Or not having more effective endpoint protection combined with endpoint detection and response?

Use this question to setup the Unrecognized Problem

**Solution** (Probe)

What if you could combine next generation EPP with EDR and use artificial intelligence and machine learning to prevent over 99% of malware attacks before they execute?

Use this question to setup the Unrecognized Problem

**Thought Leadership** (Open)

The Gartner Redefining Endpoint Protection report says that legacy EPP is no longer effective and organizations should consider combining next generation EPP with EDR. A 2017 ESG reports shows that ease of management and minimized resource use are two of the most important capabilities for EPP and EDR as this can reduce security silos and complexities.

**Unrecognized Risks** (Confirm)

How would it impact you to combine next generation EPP and EDR with artificial intelligence and machine learning to proactively prevent over 99% of malware attacks before they execute?

**Action** (Open)

Cylance is committed to helping firms like yours avoid the costly consequences of maintaining complex and costly security silos. Let's talk about a plan to do this…

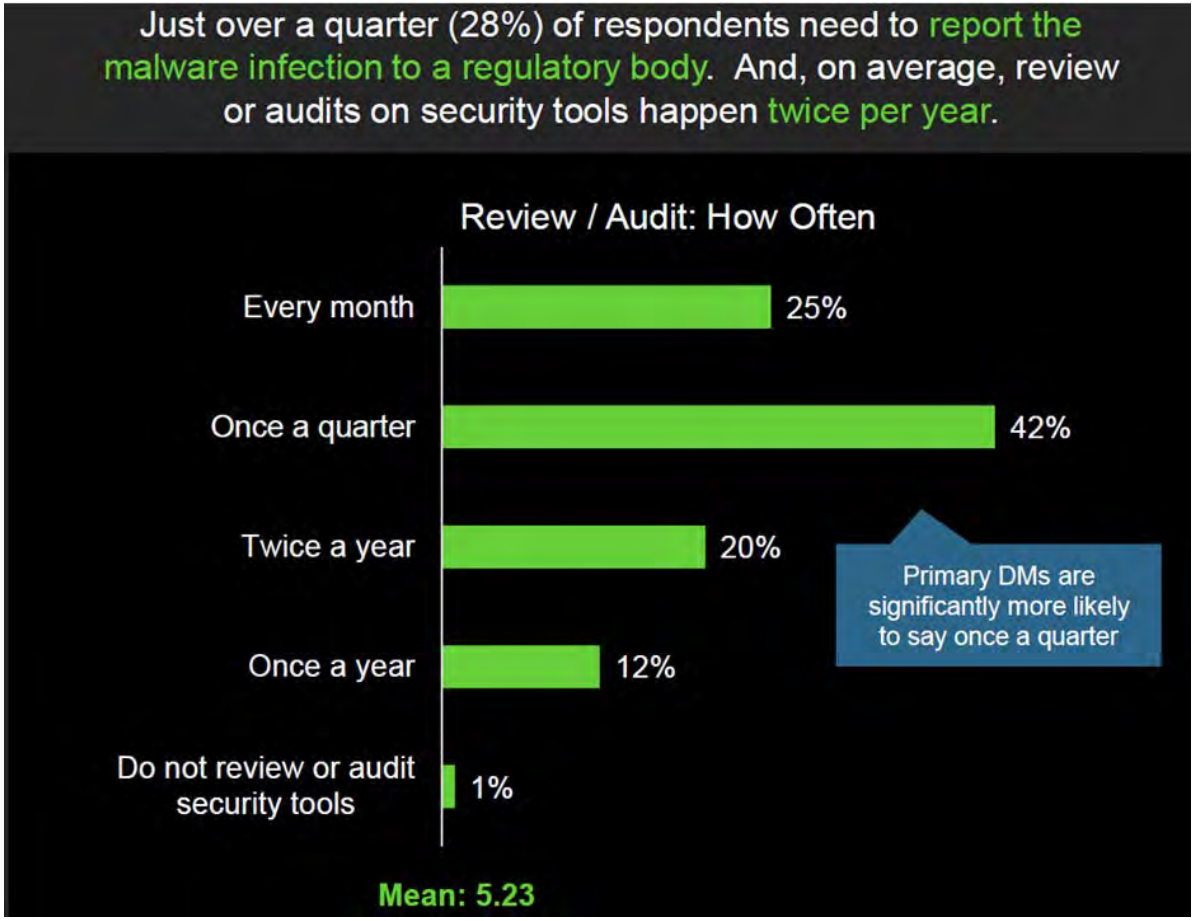
S

CLICK to go to the Cylance Soutions information section

# Compliance Concerns: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem




Source: Carbonview Study 2017

## Thought Leadership Information

- ✓ Emotional: Many organizations are regulated and need to simplify compliance processes.
- ✓ Instinctual: Firms are frequently audited and the cost of failing audits or non-compliance can be high.
- ✓ Logical: Audits on security tools are usually quarterly and the cost to avoid audit failure is also high.

# Compliance Concerns: Customer Unrecognized Problem

Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.

**Problem** (Open)

**What compliance mandates are you regulated by, how often are you audited, and what concerns do you have about failing your security solution audits?**

Use this question to setup the Unrecognized Problem

**Solution** (Probe)

**What if you could simplify your ability to pass regulatory security solution audits while lower costs and complexities?**

Use this question to setup the Unrecognized Problem

**Thought Leadership** (Open)

**Every U.S. State now has serious mandates that require the protection of the Personal Information (PI) of every resident. Regulatory bodies have increased the fines for security breaches, mandated that breaches are disclosed publicly, and many have made it easier for citizens to file costly lawsuits. The consequences for inadequate security are now higher than ever.**

**Unrecognized Risks** (Confirm)

**How would it impact you to combine next generation EPP and EDR with artificial intelligence and machine learning to proactively prevent attacks and ensure regulatory compliance?**

**Action** (Open)

**Cylance is committed to helping firms like yours avoid the costly consequences of failing regulatory compliance audits. Let's talk about a plan to do this…**

S

CLICK to go to the Cylance Soutions information section

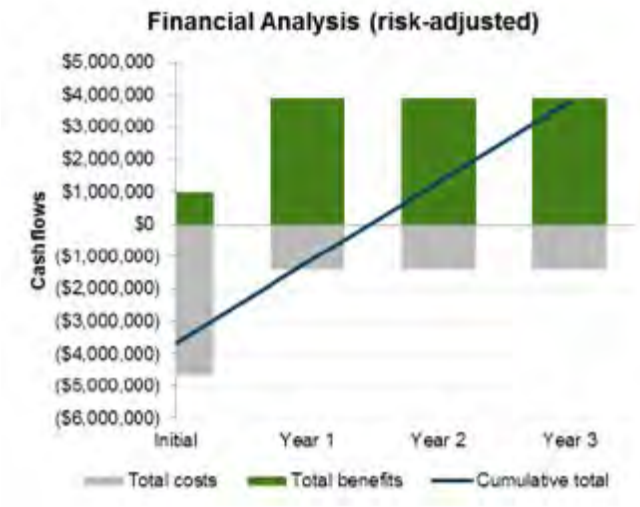


CYLANCE

# Cost or Budget Concerns: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem





## Thought Leadership Information

- ✓ Emotional: $260,000 in cost savings related to reducing the need to remediate/reimage systems.
- ✓ Instinctual: A yearly cost savings of $2.3 million due to reduced incidence of zero-day threats & data breaches.
- ✓ Logical: Improved productivity for IT, network, and security FTEs of three–year present value of $1.8 million.

**Benefits**
**$7.7 million**

**Forrester completed a study in 2017 on a State County and verified a dramatic economic benefit for deploying Cylance endpoint security solutions.**

Source: Forrester Study 2017



CYLANCE

# Cost or Budget Concerns: Customer Unrecognized Problem

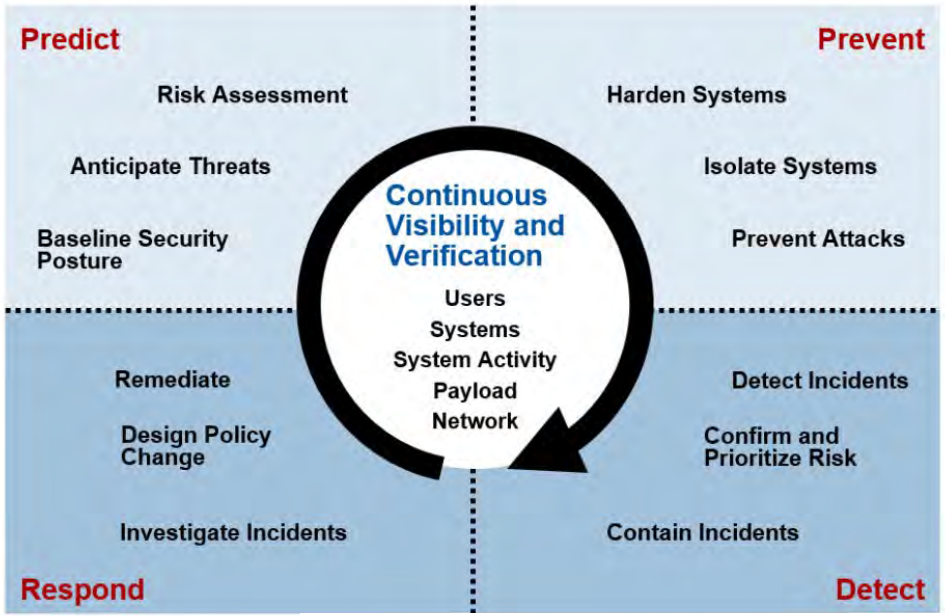
**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

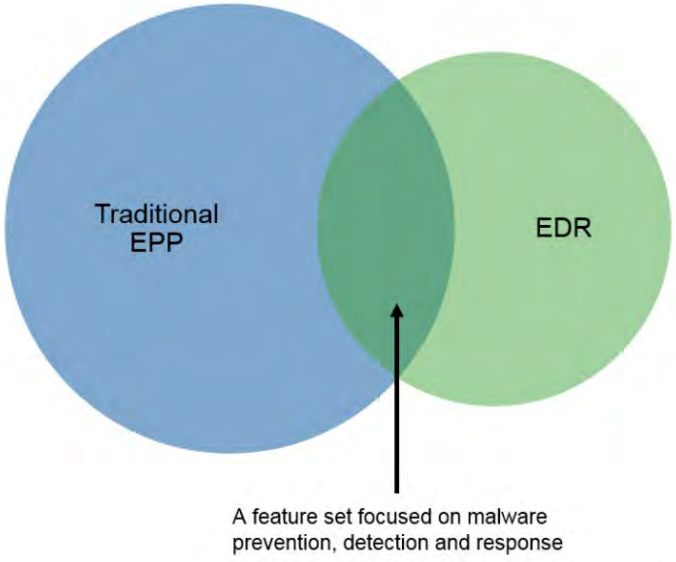
| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about the effectiveness of your current endpoint protection solutions and increased costs for management, reimaging or remediation, and daily scan disruptions??** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if you could lower costs and meet budgets by eliminating daily scans, reimaging or remediation, and reducing security staff efforts and costs?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **Forrester completed a study in 2017 on a State County and verified a dramatic economic benefit for deploying the right endpoint security solutions. They saved $260,000 by reducing the need to remediate or reimage systems, $2.3 million by reducing the incidence of zero-day threats & data breaches, and improved productivity resulting in a three–year present value of $1.8 million.** | |
| Unrecognized Risks (Confirm) | **How would it impact you to enjoy $7.7M in economic benefits by reducing complexities and successful attacks while improving your team's productivity?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the consequences of using inadequate legacy security solutions. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |

# Detection & Response Issues: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem






## Thought Leadership Information

- ✓ Emotional: A recent Gartner report says that legacy EPP that does not include EDR is obsolete & ineffective.
- ✓ Instinctual: The Gartner report states that organizations need the ability to detect, investigate, and respond.
- ✓ Logical: EDR should be a glove-fit with EPP and include Threat Hunting, incident investigation, and analysis.



CYLANCE

# Detection & Response Issues: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

**Problem** (Open)

**What concerns do you have about your inability to respond quickly and take decisive action when a security incident is identified or a threat needs to be mitigated?**

Use this question to setup the Unrecognized Problem

**Solution** (Probe)

**What if your EPP included EDR that could, with a few simple clicks, download and quarantine files and take aggressive containment actions by isolating harmful network endpoints?**

Use this question to setup the Unrecognized Problem

**Thought Leadership** (Open)

**The 2017 U.S. State of Cybercrime Survey shows that the average time for intrusion discovery is growing and it's now over 90 days. Ponemon Institute discovered that it then takes over 30 days to resolve the incident, which can cost more than $32,000 per day. Combined, that's over 120 days at a total cost of almost $4 million. That's why Gartner says that EPP without effective EDR is obsolete.**

**Unrecognized Risks** (Confirm)

**How would it impact you to have EDR that could offer a root cause analysis on any blocked threat or artifact, proactively "threat hunt" endpoints and take decisive action to prevent incidents?**

**Action** (Open)

**Cylance is committed to helping firms like yours avoid the costly consequences of using legacy EDR solutions by considering more modern proactive AI solutions. Let's talk about a plan to do this…**

S

CLICK to go to the Cylance Soutions information section



CYLANCE

# Email or Phishing Attacks: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem

Figure 1. Attack Vectors Experienced in the Past Two Years

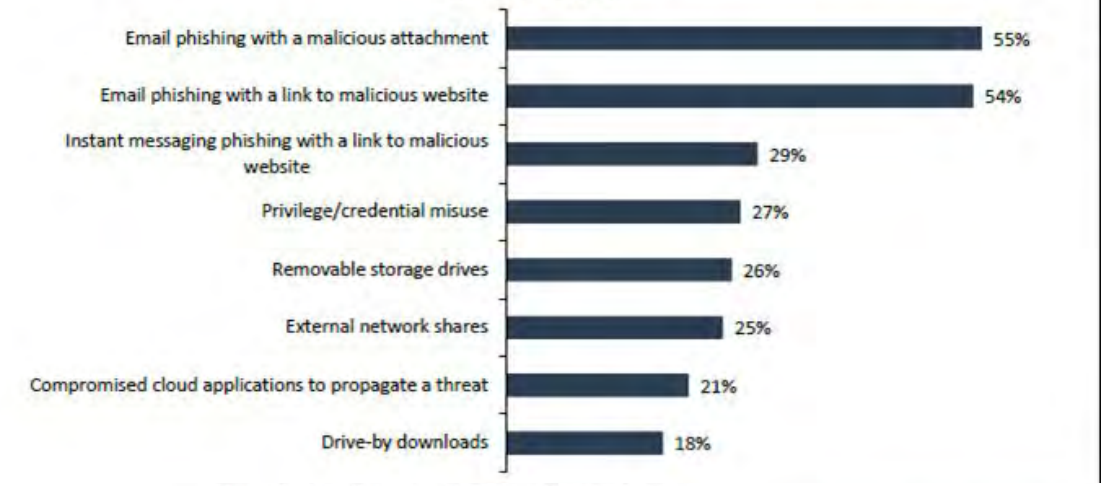
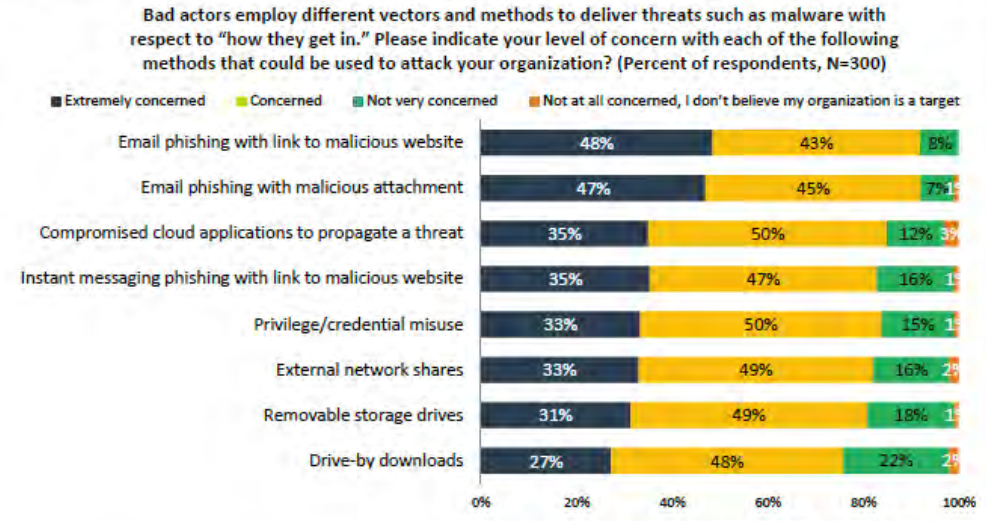



Figure 2. Attack Vectors of Concern in the Future




## Thought Leadership Information

- ✓ Emotional: Most firms agree that employee training helps but is not very effective against phishing.
- ✓ Instinctual: A majority of security professionals rate email phishing as their highest security concern.
- ✓ Logical: Phishing can cost firms millions as it can lead to ransomware, downtime, or lost assets.

# Email or Phishing Attacks: Customer Unrecognized Problem

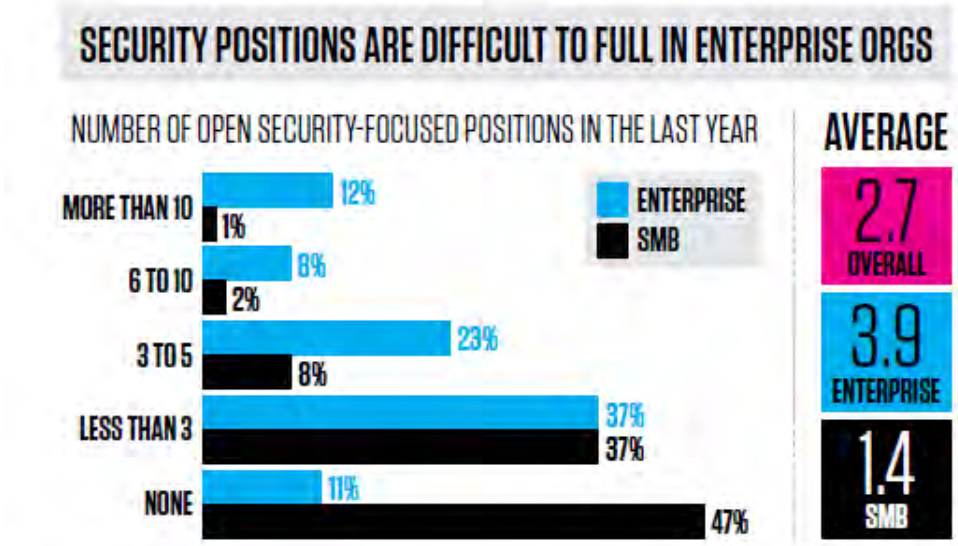
**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about email phishing attacks that can lead to ransomware, downtime, lost intellectual property, or lost customers due to public exposure?** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if your endpoint protection platform could prevent over 99% of malicious attacks before they execute and thereby reduce the impact of email phishing attacks?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **Most firms agree that employee training helps but is not very effective against phishing. A majority of security professionals rate email phishing as their highest security concern. Phishing can cost firms millions as it can lead to ransomware, downtime, or lost assets. The best way to mitigate the impact of email phishing is to employ security solutions that prevent attacks before they execute.** | |
| Unrecognized Risks (Confirm) | **How would it impact you to have proactive endpoint protection that prevented successful email phishing attacks by ensuring that malicious payloads did not execute even if a bad link was clicked?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the costly consequences of email phishing attacks by using next generation proactive AI solutions. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |

# Expertise & Staff Constraints: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem




Source: Security Priorities, IDG, 2017

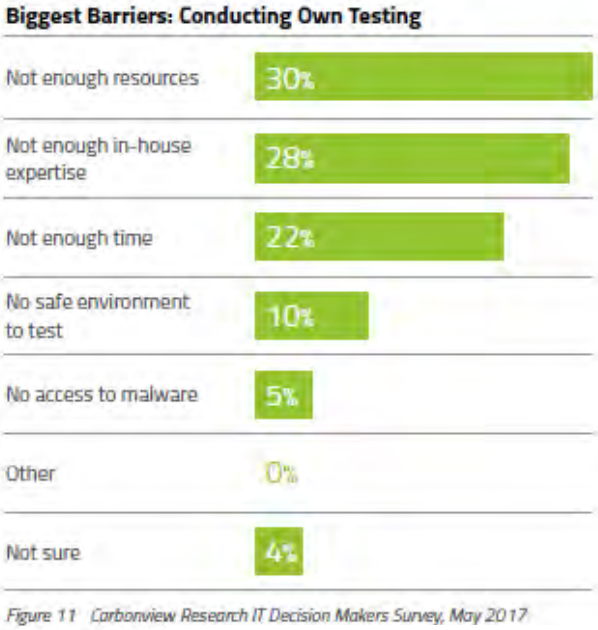



*Figure 11 Carbonview Research IT Decision Makers Survey, May 2017*

## Thought Leadership Information

- ✓ Emotional: Around 20% of enterprises average more than six open positions for security professionals.
- ✓ Instinctual: Enterprise IT security executives are often competing for scarce security talent.
- ✓ Logical: One of the largest barriers to conducting internal security testing is not having enough in-house expertise.



CYLANCE

# Expertise & Staff Constraints: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

**Problem** (Open)

**What concerns do you have about needing to recruit more IT security professionals in an environment where talent is becoming more scarce on a daily basis?**

Use this question to setup the Unrecognized Problem

**Solution** (Probe)

**What if you could augment your security team within days by leveraging readily available top security services expertise?**

Use this question to setup the Unrecognized Problem

**Thought Leadership** (Open)

**According to recent research conducting by leading firms such as IDG, 20% of enterprise organizations have six open requisitions for IT security professionals at any one time. Given the demand for these individuals, they are competing for scarce talent. In many cases these requisitions go unfilled for long months at a time. This is causing serious initiative delays and resource contraints.**

**Unrecognized Risks** (Confirm)

**How would it impact you to have one or more of your IT security professionals leave for another opportunity and only give you a two-week notice? How fast could you fill that void?**

**Action** (Open)

**Cylance is committed to helping firms like yours avoid the costly consequences of not having the expert talent needed by offering on-call security service expertise. Let's talk about a plan to do this…**

S

CLICK to go to the Cylance Soutions information section



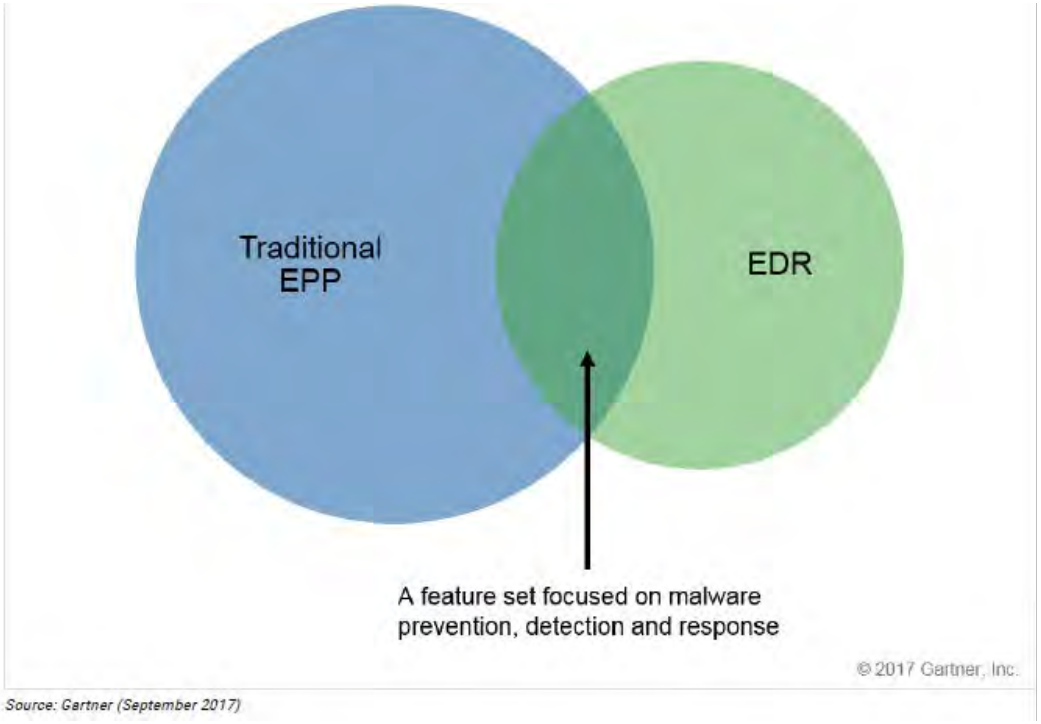
CYLANCE

# False Positive Alerts: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem


Source: Forrester Total Economic Impact Study, February 2018




Source: Gartner (September 2017)

## Thought Leadership Information

- ✓ Emotional: According to Forrester, security teams are buried under a massive amount of security alerts.
- ✓ Instinctual: These alerts, many false positive, prevent teams from focusing on critical security issues.
- ✓ Logical: Reactive firefighting creates inefficiencies and does not solve the critical problem of threat prevention.

# False Positive Alerts: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about a high number of false positive alerts that can disrupt business operations, overburden your staff, and delay important initiatives?** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if you could mitigate or even eliminate a most or all of your false positive alerts while converging endpoint protection with endpoint detection and response?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **Most IT executives agree that real incidents are disruptive enough. Adding a large number of false positive is like having constant "cry wolf" fire drills that can anger users, overburden security teams, and cause serious project delays. Gartner's Redefining Endpoint Protection study discuss how legacy EPP and EDR solutions need to converge to empower efficiency and reduce false positives.** | |
| Unrecognized Risks (Confirm) | **How would it impact you if your false positive alert rate escalated and your team started spending tens of hours per week chasing ghosts that did not exist?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the costly impact of constant false positive alerts by offering the best combination of EPP and EDR. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |



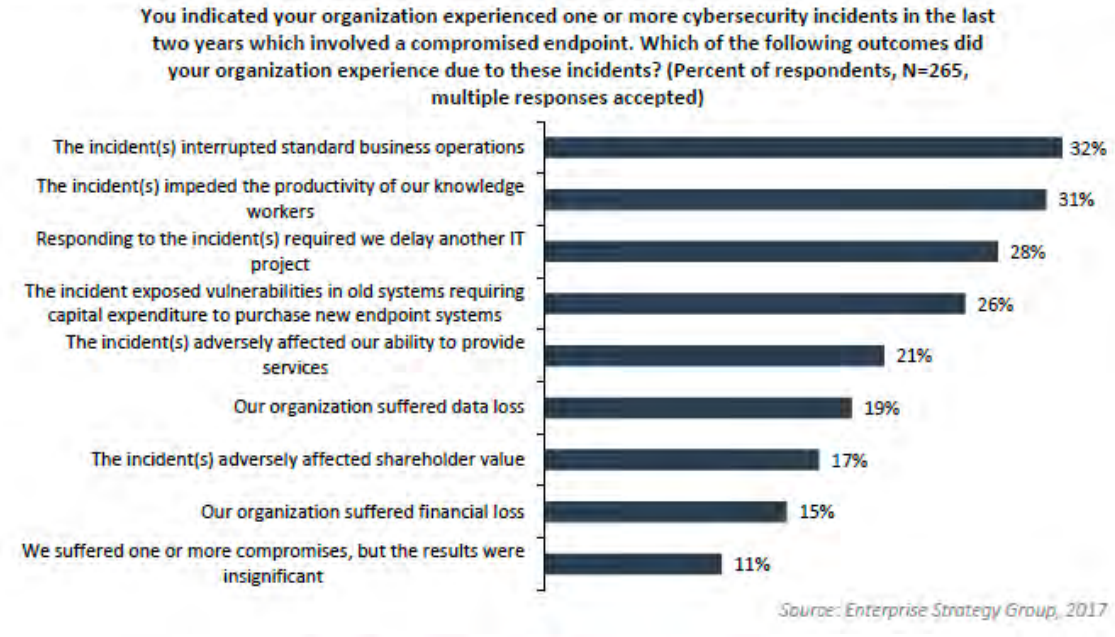
CYLANCE

# Outages or Downtime: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem

Figure 4. Impact of Compromised Endpoints



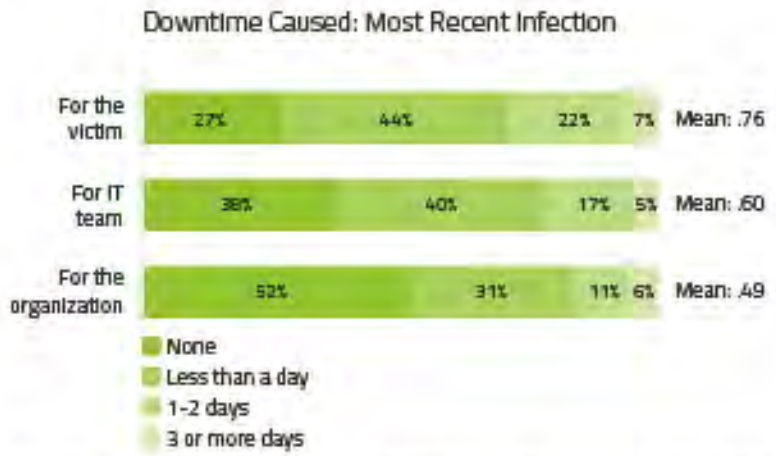




*Figure 5* *Carbonview Research IT Decision Makers Survey, May 2017*

## Thought Leadership Information

- ✓ Emotional: Incidents are disruptive to standard business operations and impede productivity.
- ✓ Instinctual: Incidents can delay other projects and adversely affect the ability to provide other IT services.
- ✓ Logical: Downtime due to re-imaging occurs 70% of the time and 31% of occurrences involve 3+ systems.

# Outages or Downtime: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about security incidents causing costly user downtime and productivity interruptions, as well as significant IT team downtime to re-image systems?** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if you could mitigate or even eliminate most user outages and productivity disruptions, as well as IT team downtime to re-image systems?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **A recent ESG reports notes that security incidents are highly disruptive to standard business operations and impede productivity. Incidents can delay other projects and adversely affect the ability to provide other IT services. A Carbonview study shows that downtime due to system re-imaging occurs 70% of the time, and 31% of those occurrences involve three or more systems.** | |
| Unrecognized Risks (Confirm) | **How would it negatively impact you if unknown malware successfully executed and caused extensive user disruption and IT team downtime to re-image systems?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the costly impact of user disruption and IT downtime by offering the proactive endpoint security solutions. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |

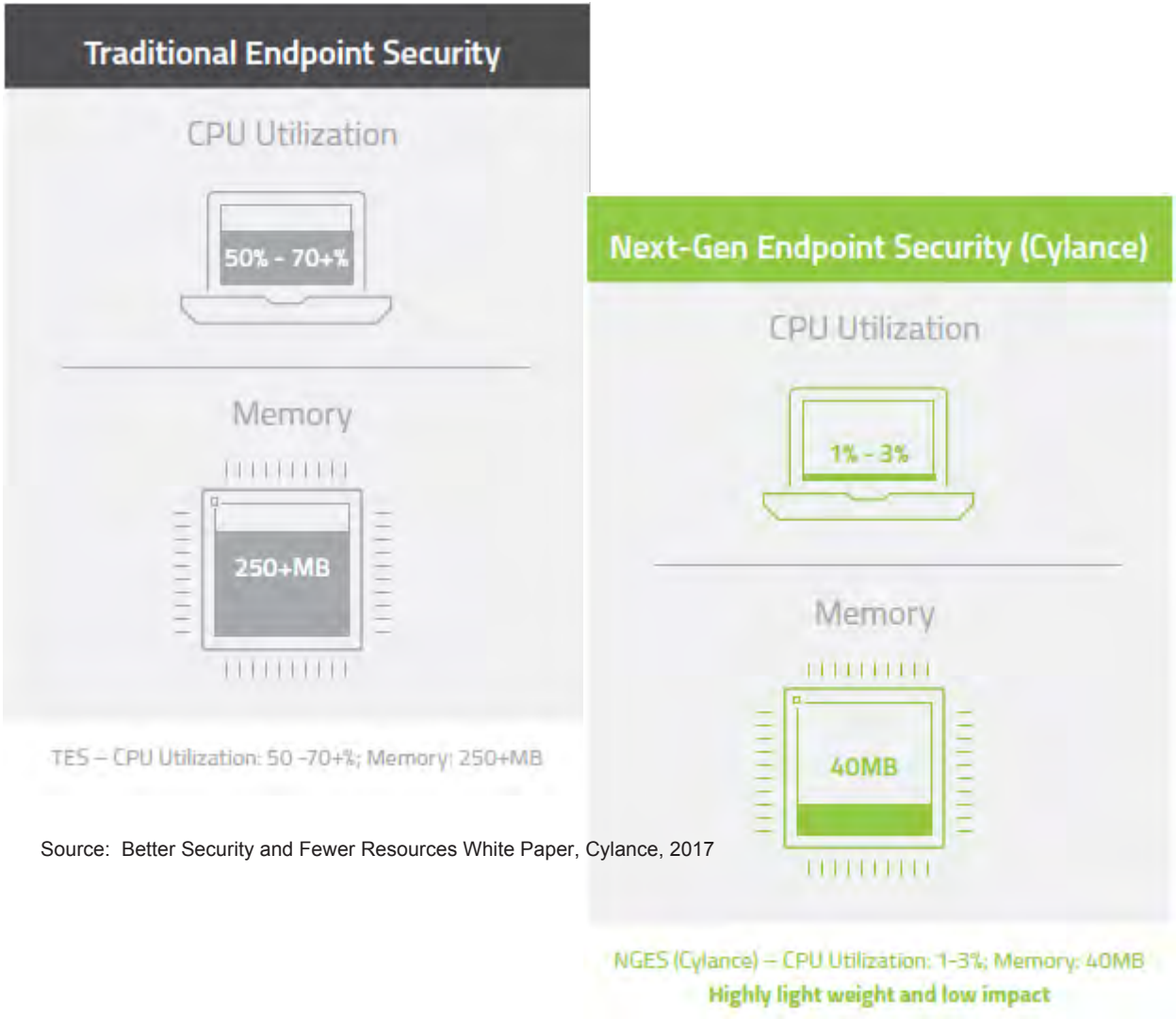


CYLANCE

# Performance Concerns: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem




Source: Better Security and Fewer Resources White Paper, Cylance, 2017

## Thought Leadership Information

- ✓ Emotional: Traditional EPP slows performance and overtaxes system memory, causing user disruptions.
- ✓ Instinctual: High CPU and memory utilization can result in productivity loss and higher costs.
- ✓ Logical: Traditional EPP can use 70X more CPU and over 6X more memory than next generation EPP.

# Performance Concerns: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about using legacy endpoint protection solutions that can overtax your system CPU and memory and cause user disruptions and high costs?** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if you could reduce your CPU utilization by 70X and memory usage by 6X and eliminate the risk of user and IT disruption and higher system costs?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **Traditional EPP slows performance and overtaxes system memory, causing serious user disruptions and complaints. High CPU and memory utilization can result in productivity loss and higher costs. Traditional endpoint protection solutions can often use 70X more CPU and over 6X more memory than next generation endpoint protection systems.** | |
| Unrecognized Risks (Confirm) | **How would it impact your firm if user productivity decreased and complaints increased due to CPU and memory over-utilization caused by your legacy EPP solution?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the cost and performance hits caused by inefficient EPP solutions by offering next generation technology. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |



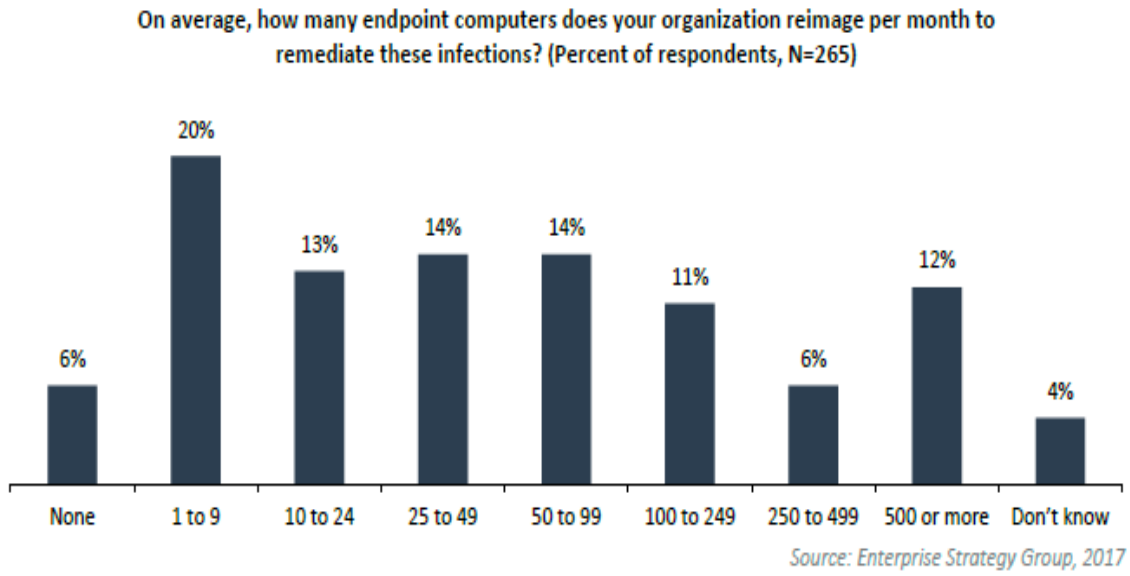
CYLANCE

# Re-imaging Issues: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem

Figure 5. Extent of Reimaging as Remediation for Infections




## Thought Leadership Information

- ✓ Emotional: It's difficult and time-consuming for IT teams to re-image systems to remediate infections.
- ✓ Instinctual: Re-imaging risks missing a bad file or deleting a good one, thus compromising the endpoint.
- ✓ Logical: Remediating infections takes hours or days and interrupts business productivity.


Source: ESG Survey, 2017

# Re-imaging Issues: Customer Unrecognized Problem

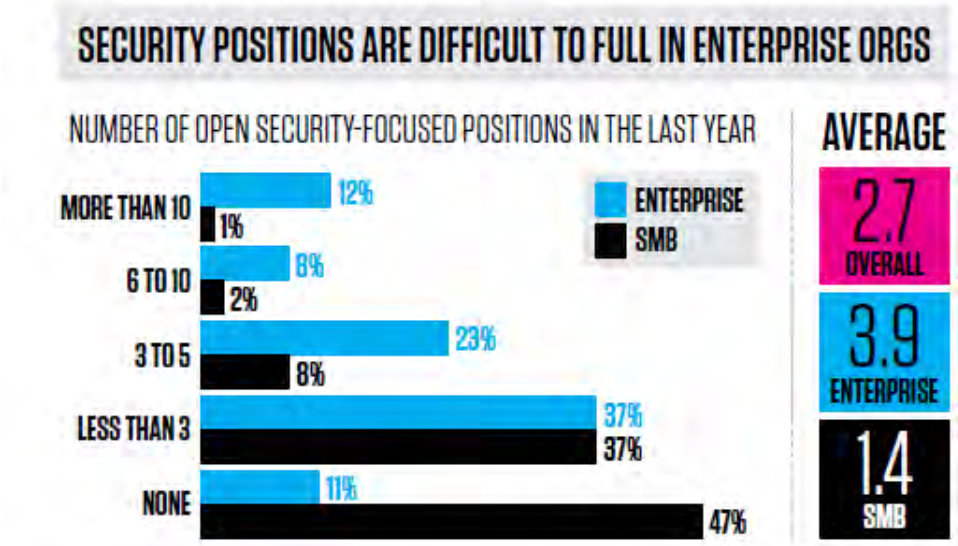
**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about using legacy endpoint protection solutions that require frequent remediation and system re-imaging that cause user and IT team disruptions?** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if you could reduce or eliminate the need to frequently remediate infections or re-image systems?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **If malware successfully executes, it can be difficult and time-consuming for IT teams to re-image systems to remediate infections. Re-imaging systems risks missing a bad file or deleting a good one, which could compromise your endpoints. Remediating these infections usually takes hours or even days, which shuts downs endpoints and interrupts business productivity.** | |
| Unrecognized Risks (Confirm) | **How would it impact your firm if user productivity decreased and complaints increased due to extensive remediation and re-imaging caused by your legacy EPP solution?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the cost and performance hits caused by re-imaging and remediation by offering next generation EPP. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |

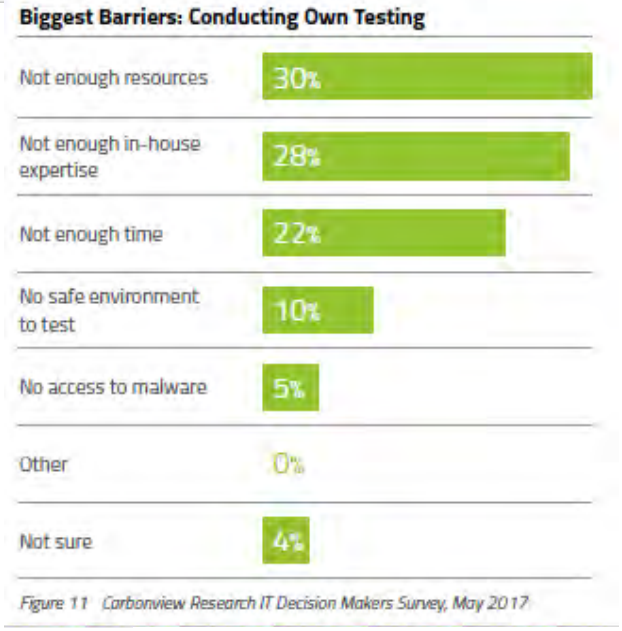
# Setup or Deployment Needs: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem




Source: Security Priorities, IDG, 2017




## Thought Leadership Information

- ✓ Emotional: Around 20% of enterprises average more than six open positions for security professionals.
- ✓ Instinctual: Enterprises risk malicious attacks when solution deployment is delayed due to resource constraints.
- ✓ Logical: One of the largest barriers to conducting internal setup & testing is not having enough in-house expertise.



CYLANCE

# Setup or Deployment Needs: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

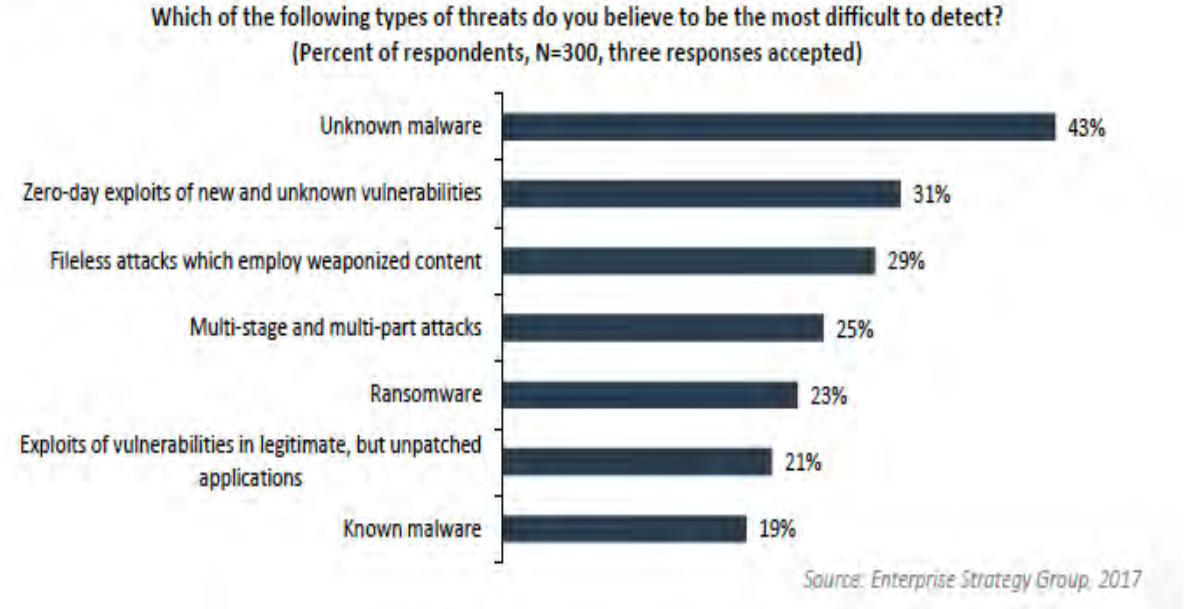
| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about not having enough IT or IS team bandwidth to properly and quickly setup or deploy new security solutions?** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if you could quickly augment your staff with certified expert security professionals that could setup and deploy your security solutions or updates?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **According to recent research conducting by leading firms such as IDG, 20% of enterprise organizations have six open requisitions for IT security professionals at any one time. This creates a burden on current staff to quickly and properly deploy critical security solutions. This is causing serious initiative delays and places organizations at risk for malcious attacks.** | |
| Unrecognized Risks (Confirm) | **How would it impact you if a new malware strain successfully executed and caused serious consequences such as ransomware, downtime, lost data, or brand and customer loss?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the costly impact of not setting up or deploying solutions by offering on-call security service expertise. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |

# Unknown Malware: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem

Figure 3. Types of Threats that Are Most Difficult to Detect




## Thought Leadership Information

- ✓ Emotional: A majority of survey ESG respondents say unknown malware is hardest to detect.
- ✓ Instinctual: Almost half of respondents were victims of a ransomware attack in the last year.
- ✓ Logical: Over half restored data from a backup but it was proven ineffective due to recurrances.




CYLANCE

# Unknown Malware: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

**Problem** (Open)

**What concerns do you have about using legacy endpoint protection solutions that are ineffective at detecting or remediating unknown malcious malware?**

Use this question to setup the Unrecognized Problem

**Solution** (Probe)

**What if you could prevent successful malware execution even if the malware is an unknown type?**

Use this question to setup the Unrecognized Problem

**Thought Leadership** (Open)

**A majority of respondents to a 2017 ESG security survey reported that unknown malware was the most difficult to detect using legacy endpoint security solutions. Almost half of respondents said they were victims of a ransomware attack in the last year. Also, Over half restored data from a backup but it was proven ineffective due to subsequent recurrances.**

**Unrecognized Risks** (Confirm)

**How would it impact your firm if your current endpoint protection solution failed to detect an unknown strain of malware and it caused serious consequences for your users and organization?**

**Action** (Open)

**Cylance is committed to helping firms like yours avoid the devastating impact of not detecting new unknown malware strains hits caused by offering next generation endpoint protection. Let's talk about a plan to do this…**

S

CLICK to go to the Cylance Soutions information section

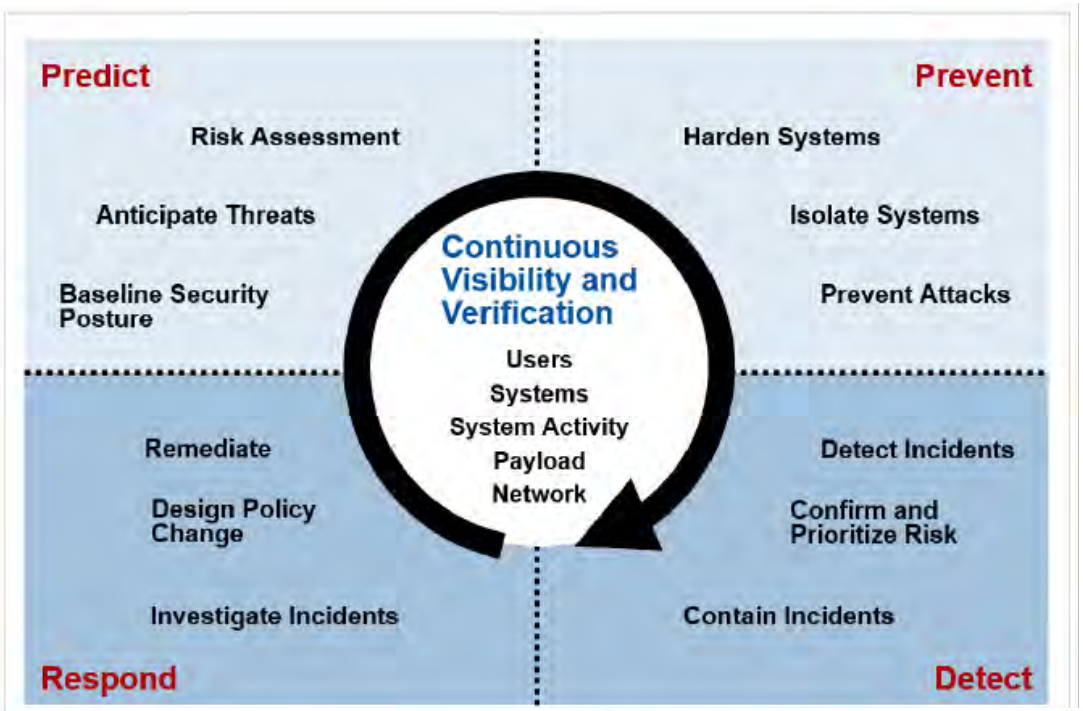


CYLANCE

# Visibility Concerns: Thought Leadership

**Leverage this Thought Leadership information to teach prospects about an Unrecognized Problem, increase credibility, and motivate them to take immediate action.**

CLICK to the next page for Thought Leadership information for the Unrecognized Problem




*Source: Gartner (September 2017)*

## Thought Leadership Information

- ✓ Emotional: Gartner says traditional endpoint protection misses many adaptive security architecture tasks.
- ✓ Instinctual: Malware is evolving faster than the visibility delivered by traditional platforms.
- ✓ Logical: Smart IT pros use next gen EDR with advanced threat hunting / detection & automated response.

# Visibility Concerns: Customer Unrecognized Problem

**Use this to teach prospects about an Unrecognized Problem, increase credibility via Thought Leadership information, and increase Value to motivate them to take immediate action.**

| | | |
|---|---|---|
| Problem (Open) | **What concerns do you have about traditional endpoint protection platforms that lack visibility for unknown malware and advanced threat detection and automated response?** | Use this question to setup the Unrecognized Problem |
| Solution (Probe) | **What if you could dramatically improve your visibility across all endpoints and increase threat detection and response capabilities?** | Use this question to setup the Unrecognized Problem |
| Thought Leadership (Open) | **The Gartner Redefining Endpoint Protection for 2017 & 2018 report notes that traditional endpoint protection platforms miss many critical adaptive security architecture requirements. The report also says that malware is evolving faster than the visibility and capability delivered by traditional platforms. Smart IT pros use next gen EDR with advanced threat detection & automated response.** | |
| Unrecognized Risks (Confirm) | **How would it impact your firm if your current endpoint protection solution failed to detect and automatically respond to a new strain of malware that reeked havoc on your organization?** | |
| Action (Open) | **Cylance is committed to helping firms like yours avoid the serious costs of not having next generation advanced endpoint detection and response. Let's talk about a plan to do this…** | S — CLICK to go to the Cylance Soutions information section |

# Prospect Power

## Power:

Decision Makers own the strategy to improve overall risk to the organization. In some cases, they have no or limited access to the BoD. Decision and purchasing power may exist elsewhere. Greater executive presense may be required to validate the strategic solution value to other leaders in the organization.

## Plan:

Is a PoC required to make this decision? Determine how security solutions are procured and which stakeholders are involved in the decision process. Clarify PoC requirements up front and make sure the team presents an outbrief to prove how Cylance resolves the Business Issue and answers the Anxiety Question.

### Influencers

- Architect
- Auditor
- BoD
- CEO
- CFO
- Committee
- COO
- Finance
- IS Director / Manager
- IS Team
- Line of Business
- Others
- Users

### Evaluators

- Architect
- Committee
- IS Director
- IS Manager
- IS Team
- Line of Business
- Others
- Users

### Decision Makers

- BoD
- CEO
- CFO
- Committee
- COO
- Finance
- IS Director
- IS Director / Manager
- IS Team
- IS VP
- Line of Business
- Others

NOTE: Hold down CTRL key to make multiple selections



CYLANCE

# CylancePROTECT

CylancePROTECT leverages the power of machines, not humans, to dissect malware's DNA. Artificial intelligence then determines if the code is safe to run.

Microsoft

Mac

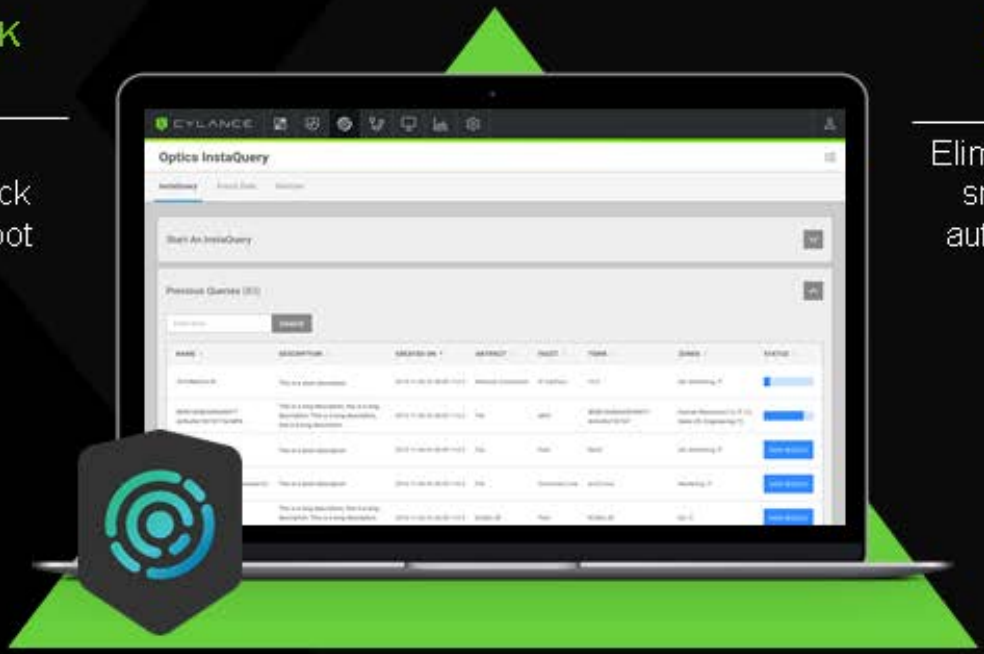
CYLANCE

# CylanceOPTICS

## CylanceOPTICS: ENDPOINT DETECTION AND RESPONSE

### REDUCE ATTACK SURFACE

Identify and mitigate previously exploited attack vectors with AI driven Root Cause Analysis




### CONSISTENT VISIBILITY

Eliminate hidden threats with smart threat hunting and automated threat detection

### INTEGRATED INCIDENT RESPONSE

Streamline incident response and containment to reduce dwell time, improve efficiency, and decrease business impact of any security risk

CYLANCE

# Plan Letter

[Prospect Name]
[Prospect Title]
[Prospect Company]

Dear [Prospect First Name,]

Thank you for your for your interest in Partner/Cylance, and for your time to discuss how we might work together to reduce your security risks, efforts, and costs. I have outlined below the key points of our recent discussion, please let me know if any of these need corrections or modifications.

I recall that your most pressing challenge is: [Business Issue]

The resolve this challenge, we need to address these three concerns:

1. [Problem 1: Unrecognized Problem]
2. [Problem 2]
3. [Problem 3]

The solutions we reviewed that may help us to resolve these concerns include:

1. [Solution 1]
2. [Solution 2]
3. [Solution 3]

If we can successfully address these concerns, the value-benefits might include:

1. [Value 1]
2. [Value 2]
3. [Value 3]

We agreed that our next action steps should be:

1. [Customer/Partner Action 1]
2. [Customer/Partner Action 2]
3. [Customer/Partner Action 3]

Again, please let me know if any of the above items need corrections or modifications. I will commit to completing my action steps and will follow-up with you on [date and time]. Thank you again for your time, and I look forward to partnering with you to ensure success.

Sincerely,
[Your Name]

# Cylance Resources

| | |
|---|---|
| THOUGHT LEADERSHIP<br>Information Links | Links to information TBD |
| SOLUTION COLLATERAL<br>Resource Links | Links to information TBD |
| PARTNER ASSETS / TRAINING<br>Resource Links | Links to information TBD |
| ENABLEMENT ASSETS<br>Resource Links | Links to information TBD |
| SALES TRAINING<br>Resource Links | Links to information TBD |
| CONTACTS / REQUESTS<br>Cylance Contacts | Links to information TBD |