About This Report

2 Survey and Respondents
Who participated in this survey, and what did we ask them?

3 Executive Summary
tl;dr – Key findings and takeaways

4-6 (In)Security:
IT Pros Don’t See Many Reasons to Be Confident
3 factors causing IT pros to lose faith in their current solutions

7-10 Disconnect Between the Frontlines and C-suite
Why are executives more confident than IT pros, and what else do the two disagree on?

10 Conclusion: What Will It Take to Boost Confidence?
Getting on the same page and moving forward together
Survey and Respondents

Who participated in the survey?
We surveyed 350 IT professionals to get insight into how confident they are when it comes to security, and what their top concerns and priorities are for 2016.

What did we ask them?
- Biggest concerns
- Confidence in current solutions, metrics, and employees
- Number of breaches suffered in 2015
- Time spent on security
- Top priorities
- Biggest downsides to security solutions

Survey and Respondents

Who participated in the survey?
We surveyed 350 IT professionals to get insight into how confident they are when it comes to security, and what their top concerns and priorities are for 2016.

What did we ask them?
- Biggest concerns
- Confidence in current solutions, metrics, and employees
- Number of breaches suffered in 2015
- Time spent on security
- Top priorities
- Biggest downsides to security solutions

Survey and Respondents

Who participated in the survey?
We surveyed 350 IT professionals to get insight into how confident they are when it comes to security, and what their top concerns and priorities are for 2016.

What did we ask them?
- Biggest concerns
- Confidence in current solutions, metrics, and employees
- Number of breaches suffered in 2015
- Time spent on security
- Top priorities
- Biggest downsides to security solutions

Survey and Respondents

Who participated in the survey?
We surveyed 350 IT professionals to get insight into how confident they are when it comes to security, and what their top concerns and priorities are for 2016.

What did we ask them?
- Biggest concerns
- Confidence in current solutions, metrics, and employees
- Number of breaches suffered in 2015
- Time spent on security
- Top priorities
- Biggest downsides to security solutions
Executive Summary

It’s easy for security to feel like an uphill battle. Attacks are becoming increasingly sophisticated, and hundreds of thousands of new malicious programs are being reported every day. Organizations we surveyed reported suffering an average of 2.7 breaches last year alone, but IT pros haven’t given up hope. 82% still believe effective endpoint security is possible.

The problem is half of them aren’t confident in their current solutions, and the majority have difficulty assessing the value solutions provide. Gaining visibility into what’s actually happening in their organizations isn’t easy, and one third of respondents say they even lack the basic ability to tell whether their organization has been breached.

When breaches do happen, respondents are most concerned with the negative impact on productivity. They also aren’t happy sacrificing speed and performance to be more secure.

IT pros and executives often don’t see eye-to-eye when it comes to the best use of time and resources. Execs are generally more confident with their current security and prefer to address issues with new software. IT pros are more skeptical and would rather invest in employee training or hire more help.

Despite these issues, both groups are optimistic they can make improvements and generally feel supported to make the changes they need.
(In)Security: IT Pros Don’t See Many Reasons to Be Confident

Despite widespread increases in IT security spending, half of the IT pros we surveyed aren’t confident their current security products or solutions will actually protect them from an attack. When it comes to securing their endpoints, specifically, one in five don’t even believe effective protection is truly possible.

Confidence levels at a glance:

- 50% aren’t confident in their current security products or solutions
- Nearly 1 in 5 don’t believe effective endpoint security is possible at all
- 54% aren’t confident their organization can measure security ROI
- 3 out of 4 think employees’ cybersecurity awareness is moderate at best

<table>
<thead>
<tr>
<th>How confident are you in your security?</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Believe effective endpoint security is possible</td>
<td>83%</td>
</tr>
<tr>
<td>Are confident in their current security solution</td>
<td>50%</td>
</tr>
<tr>
<td>Are confident in their ability to measure security ROI</td>
<td>46%</td>
</tr>
<tr>
<td>Are confident in employee cybersecurity awareness</td>
<td>25%</td>
</tr>
</tbody>
</table>
What factors are causing IT professionals to give up on their current protection?

1. Solutions aren’t reliably stopping breaches

When asked how many breaches (if any) their company had experienced in the past year, a third of respondents admitted they didn’t know. Putting that problem aside for the moment, those who were aware reported suffering an average of 2.7 breaches. It’s understandably difficult to be confident in your protection when your company is suffering nearly three breaches a year.

2. Solutions have downsides

Not only are today’s security solutions failing to inspire confidence in their effectiveness, survey findings also indicate they’re putting a significant strain on business operations.

How many breaches has your company experienced in the last year?

<table>
<thead>
<tr>
<th>Avg. by company size:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- 1K employees</td>
<td>2.0</td>
</tr>
<tr>
<td>1K-9K employees</td>
<td>3.5</td>
</tr>
<tr>
<td>+ 10K employees</td>
<td>2.7</td>
</tr>
<tr>
<td>Don’t know</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1-5</td>
<td></td>
</tr>
<tr>
<td>6-10</td>
<td></td>
</tr>
<tr>
<td>10+</td>
<td></td>
</tr>
</tbody>
</table>
3. It’s difficult to measure the value solutions provide

The majority of the respondents we surveyed struggle to determine the direct effect solutions have on their organization’s security posture, and how that effect translates into measurable return on investment (ROI).

The fact that a third of respondents did not have the ability to tell whether their company had been breached in the past year suggests the lack of visibility isn’t confined to ROI. Many companies still don’t have proper insight into what’s happening in their organization from a security perspective. Therefore, they can’t be sure whether the solutions they’re paying for are working or not.

Despite all these issues, 52% of IT execs would still jump at the chance to purchase new, improved security software, and one in four say there is no limit to what they would pay for something more effective and reliable.

That’s a far cry from the position the majority of IT professionals in non-executive roles take – and the differences of opinion do not stop there. In the next section we’ll look closely at how gaps between IT pros on the front lines and executives in management positions may point to a potentially damaging misalignment between concerns, priorities, and roles.
Disconnect Between the Front Lines & C-Suite

When our survey results came in, we quickly noticed a striking difference in attitudes among IT professionals in non-management positions and their counterparts in executive roles. These two groups responded differently to nearly every question we asked, from time spent on security to the most problematic effect of a data breach. Stepping back and looking at the survey as a whole, one particular theme emerged:

When it comes to security, executives are much more confident than their IT teams.

Why the discrepancy, and who has it right? Should IT pros be more confident, or are executives being unrealistic? For more insight, let’s look at some of the key differences in each group’s roles, top concerns, and immediate priorities.
Who has the time for security?

For 40% of IT pros, improving security is an essential priority that they unfortunately seldom have time to focus on. On average, they spend 76% of their day being pulled in other directions. Executives, on the other hand, spend nearly twice the amount of time on security that IT pros do, despite the fact only 26% of them view it as an essential priority.

Average time spent on security (min. per hr.):

<table>
<thead>
<tr>
<th></th>
<th>IT pros</th>
<th>Executives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>14 mins</td>
<td>25 mins</td>
</tr>
</tbody>
</table>

Security is an essential priority:

<table>
<thead>
<tr>
<th></th>
<th>IT pros</th>
<th>Executives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>40%</td>
<td>26%</td>
</tr>
</tbody>
</table>

This discrepancy in the amount of time each group has to spend on security may be one factor that plays into executives being more confident and IT pros less so.

Top 5 security concerns:

<table>
<thead>
<tr>
<th>IT pros</th>
<th>Executives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. External breaches</td>
<td>Insider threats</td>
</tr>
<tr>
<td>2. Uninformed employees</td>
<td>External breaches</td>
</tr>
<tr>
<td>3. Cloud security</td>
<td>Uninformed employees</td>
</tr>
<tr>
<td>4. Insider threats</td>
<td>Cloud security</td>
</tr>
<tr>
<td>5. BYOD management</td>
<td>BYOD management</td>
</tr>
</tbody>
</table>

What could possibly go wrong?

Another potential key to understanding each group’s confidence levels is identifying what they are most concerned about and what they are trying to prevent.

The threat of external breaches keeps both executives and IT pros up at night, but for C-level respondents insider threats are an even bigger concern. Both groups are worried about employees clicking things they shouldn’t, which should be no surprise considering their low confidence in employee cybersecurity awareness.
Should the worst case happen and their organization suffer a data breach, IT pros tend to worry more about downtime while executives worry more about remediation costs. Both, however, agree the biggest downside of a breach is that it can hamper their ability to get stuff done.

It’s interesting to note loss of productivity (in the form of a slow-running system) is also the #1 issue IT pros and execs have with current security solutions. That doesn’t exactly bode well for confidence, as it leaves them feeling like they’re stuck between a rock and a hard place – suffer a breach and be unproductive, or purchase security and be less productive, too.

**Most damaging impact of a data breach:**

<table>
<thead>
<tr>
<th>IT pros</th>
<th>Executives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Loss of employee productivity</td>
<td>Loss of employee productivity</td>
</tr>
<tr>
<td>2. End user downtime</td>
<td>Recovery costs</td>
</tr>
<tr>
<td>3. Loss of customer trust</td>
<td>End user downtime</td>
</tr>
<tr>
<td>4. Recovery costs</td>
<td>Legal expenses</td>
</tr>
<tr>
<td>5. Legal expenses</td>
<td>Loss of customer trust</td>
</tr>
</tbody>
</table>

**Different priorities**

For executives, the potential for security to hamper workflow is also top-of-mind when it comes to evaluating new solutions. When asked what they wanted most out of a security product, nearly 40% indicated ease of deployment, ranking it higher than price or even efficacy.

As the more likely everyday users of security solutions, IT pros are perhaps naturally more concerned with how well the solution actually works, and whether or not they will have support to help them use it.

**Most wanted from a security solution:**

<table>
<thead>
<tr>
<th>IT pros</th>
<th>Executives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Efficacy</td>
<td>Ease of deployment</td>
</tr>
<tr>
<td>2. Affordable</td>
<td>Affordable</td>
</tr>
<tr>
<td>3. Ease of deployment</td>
<td>Efficacy</td>
</tr>
<tr>
<td>4. Client support</td>
<td>Client support</td>
</tr>
<tr>
<td>5. Ease of use</td>
<td>Ease of use</td>
</tr>
</tbody>
</table>
Conclusion:  
Keys to Boosting Confidence

So what are IT pros and execs confident in?

83% believe  
effective endpoint security is possible

3 out of 4 believe their leadership team  
places a high or essential priority on security

The majority are confident  
they have the support to choose the best security option available

That’s a good foundation to build from. But to move forward, companies need to eliminate internal disconnects and get on the same page in terms of priorities. Not only will that allow them to focus on addressing their most pressing needs, it will also give them clear guideposts for measuring their performance and progress.

The majority of IT pros and executives are optimistic improvements can be made. The next step is learning to row together in the right direction.

Given free rein to make any improvements they saw fit, the majority of execs would jump at the chance to purchase new, improved security software. IT pros, on the other hand, would rather hold more educational events and training sessions, despite (or perhaps due to) their low confidence in employee security awareness.

In an ideal scenario, first thing you would do/change:

- Increase employee training
- Hire a dedicated security professional
- Purchase new, improved software

In short, execs would prefer to solve their security problem with technology. IT pros want to enlist allies to help shoulder the burden.

In short, execs would prefer to solve their security problem with technology. IT pros want to enlist allies to help shoulder the burden.
At Barkly, we believe security shouldn’t be difficult to use or understand. That’s why we're building strong endpoint protection that's fast, affordable, and easy to use.