



Closing the IT Security Gap with Automation & AI in the Era of IoT: Global

Sponsored by Aruba, a Hewlett Packard Enterprise company

Independently conducted by Ponemon Institute LLC

Publication Date: September 2018

Closing the IT Security Gap with Automation & AI in the Era of IoT: Global

Prepared by Ponemon Institute, September 2018

Part 1. Introduction

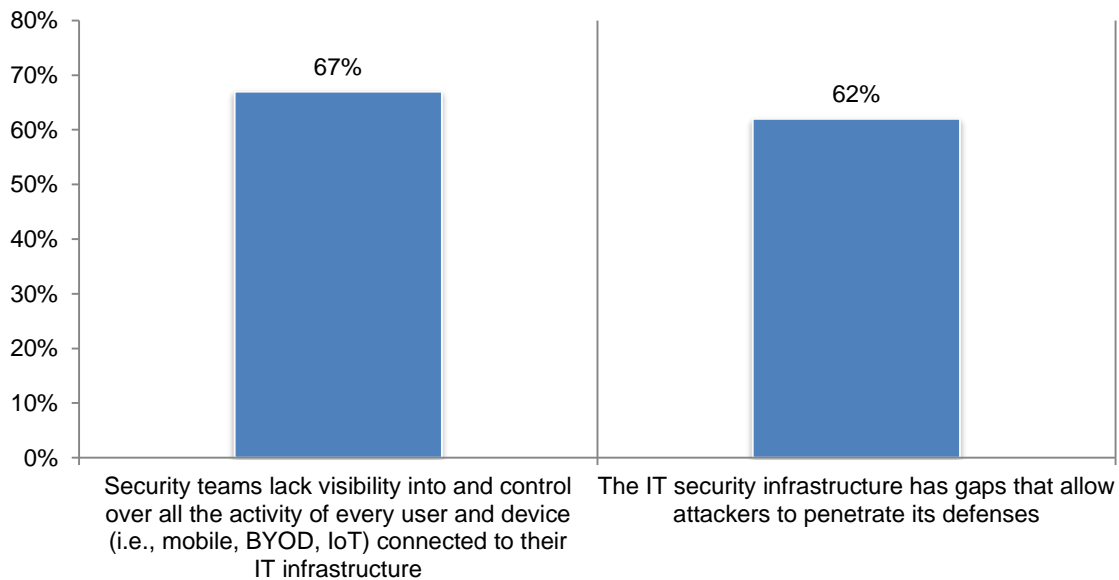
The purpose of this research, sponsored by Aruba, is to understand the reasons for the dangerous gap in modern IT security programs and strategies, a gap that is diminishing the ability of organizations to identify, detect, contain and resolve data breaches and other security incidents. The consequences of the gap can include financial losses, diminishment in reputation and the inability to comply with privacy regulations such as the EU's General Data Protection Regulation (GDPR).

Ponemon Institute surveyed 3,866 IT and IT security practitioners in the following three regions and eight countries: Asia-Pacific, EMEA, North America, Australia, Brazil, Germany, India, Japan, Mexico, Singapore and the United Kingdom. In this report, we provide the global findings.

The IT security gap allows attackers to penetrate companies' defenses. In the context of this research, the IT security gap is defined as the inability of an organization's people, processes and technologies to keep up with a constantly changing threat landscape. As shown in Figure 1, 62 percent of respondents believe that this gap in the IT infrastructure makes it easier for attackers to penetrate companies' defenses. The gap is caused by a lack of visibility into and control over all the activity of every user and device (i.e., mobile, BYOD, IoT) connected to their organization's IT infrastructure, according to 67 percent of respondents.

Figure 1. Consequences of an IT security gap

Strongly agree and Agree responses combined



The following findings illustrate the reasons behind and the problems created by the IT security gap.

The expanding and blurring of the IT perimeter is the main reason companies have an IT security gap. Fifty-five percent of respondents say it is hard to protect the expanding and blurring IT perimeter in light of IoT, BYOD, mobile and cloud. Other reasons for the IT security gap are shortages in skilled staff and the lack of visibility into what every user and device is doing while connected to the IT infrastructure (both 49 percent of respondents).

Compromised legitimate users are considered the greatest risk. Compromised and negligent users who have legitimate access inside the organization pose the greatest threat.

The IT security gap leaves the IT infrastructure vulnerable to attack. Only 38 percent of respondents are confident that attacks inside the IT infrastructure can be detected before they cause a cybersecurity breach, resulting in data stolen, modified or viewed by unauthorized entities. Fifty-one percent of respondents say attacks that have reached inside the network have the potential to do the greatest damage.

Despite all the investments in cybersecurity programs, breaches are still happening. As a result of the IT security gap, companies are unable to stop many data breaches. Almost half (49 percent of respondents) say it is difficult to protect complex and dynamically changing attack surfaces such as mobile, BYOD, cloud and IoT. Additionally, 48 percent of respondents said the lack of security staff with the necessary expertise is another key problem. A third reason is that today's attackers are persistent, sophisticated, well-trained and well-financed (46 percent of respondents).

The inability to secure IoT devices and apps is a primary driver behind the IT security gap. Sixty-six percent of respondents say their organizations are unable to, or have just a low ability, to secure their IoT devices and apps. More than half of respondents (51 percent) say IoT visibility is important for detecting attacks.

To achieve a strong level of IoT security, 52 percent of respondents say continuous monitoring of network traffic for each IoT device is required to spot anomalies early and achieve a strong level of security. NAC is also important for addressing IoT risks, according to 41 percent of respondents.

Why IoT devices are widening the IT security gap. Only 23 percent of respondents believe that IoT devices that simply monitor or perform minor tasks pose little threat to their organization's overall security. Seventy-one percent of respondents agree that legacy IoT technologies are difficult to secure. As a consequence, only 24 percent of respondents say their organization's IoT devices are appropriately secured with a proper security strategy in place.

The following findings describe the solutions for closing the IT security gap.

New technologies are needed to close the IT security gap. Sixty-four percent of respondents say new technologies, such as machine learning (ML), are needed to discover and understand threats that are active in the IT infrastructure. Currently, only 45 percent of respondents say their organizations are getting the full value from their current security investments. Steps that respondents believe are important to minimize the dangers of stealthy and hidden threats within the IT infrastructure include monitoring privileged users (53 percent), Security Information and Event Management systems (SIEM) (47 percent), and User and Entity Behavior Analytics (40 percent), which is increasingly seen as a way to monitor high value assets while "turbocharging" existing SIEM installations.

Application and endpoint visibility is critical to detecting attacks from the inside. Seventy-one percent of respondents say application visibility is critical to detecting attacks and 69 percent

of respondents believe endpoint visibility is important. Also important are cloud and network traffic visibility (64 percent and 63 percent, respectively).

Is AI-based ML hype or reality? More than half of respondents (51 percent) agree that AI technologies such as ML and behavioral analytics are essential to detecting attacks on the inside before they do damage. The top three security benefits of using these technologies are an increase in effectiveness of security teams, more efficient investigations and the ability to find stealthy threats that have evaded standard security defenses (63 percent, 60 percent and 56 percent of respondents respectively).

Most organizations are planning to use ML for security purposes. Currently 29 percent of respondents say ML is implemented extensively throughout their IT infrastructure (12 percent) or partially (17 percent). Forty-six percent of respondents say they will have ML in the next 12 months (26 percent) or in more than a year (20 percent).

The most beneficial aspect of automation is reducing the amount of time and effort required to investigate an alert. Respondents believe the most important benefit of automation technology is the ability to reduce the amount of time and effort required to investigate an alert (71 percent respondents), followed by a reduction in the number of false positives that analysts must investigate (68 percent of respondents).

This is especially important in complying with the recently enacted EU GDPR privacy standard. A key requirement is in the event of a personal data breach, the data controllers must notify the supervisory authority within 72 hours. Such notification should include detailed information about who was affected, the overall impact of the breach and actions taken to remediate the breach.

NAC is considered important to providing visibility to what is on networks. Respondents believe their NAC products provide visibility into what is on the network (53 percent) or that it is a key component of their overall security strategy (52 percent). However, more than half (51 percent) say NAC products are difficult to set up and administer.

Part 2. Key findings

In this section of the report, we provide a deeper dive into the findings of the research. The complete audited findings are presented in the Appendix of this report.

We have organized the findings according to the following topics:

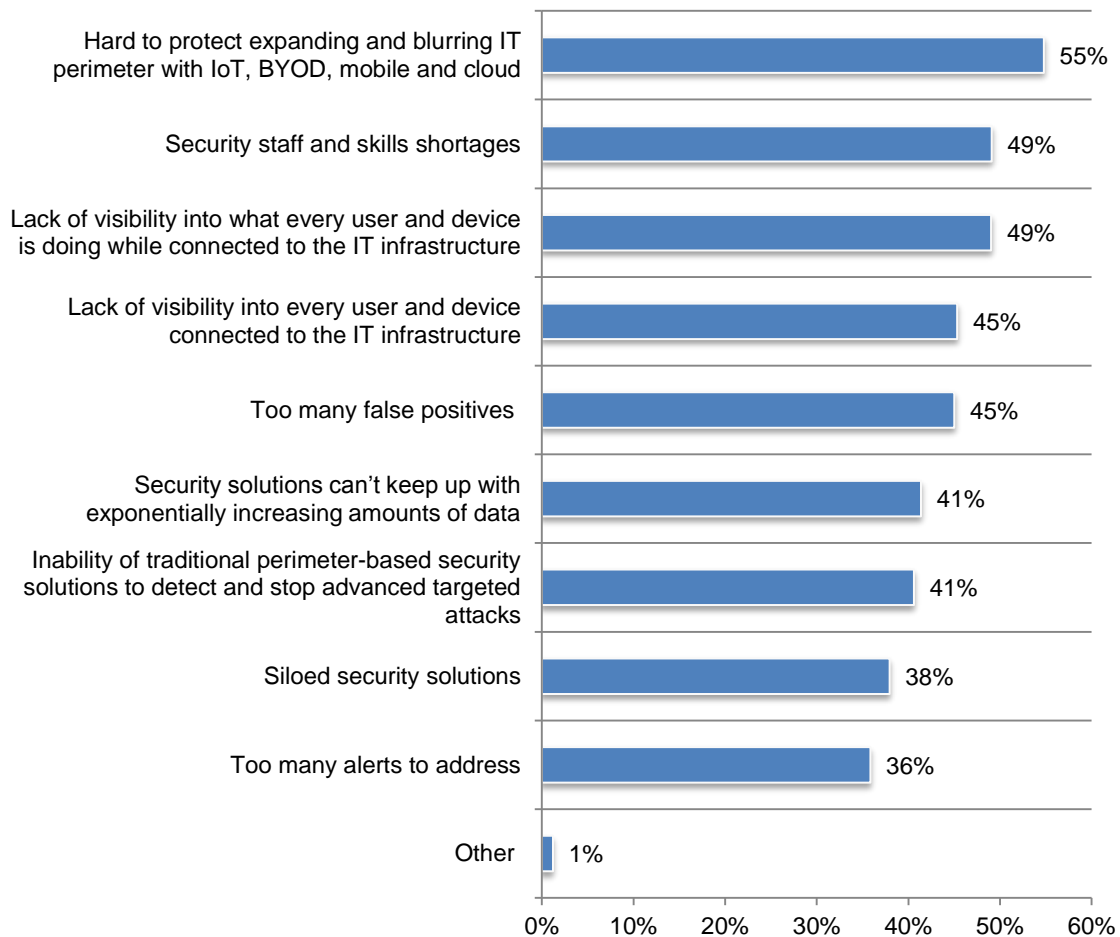
- The IT security gap
- The risk of noncompliance with GDPR and other privacy regulations
- Is the IoT widening the IT security gap?
- Solutions for closing the IT security gap

The IT security gap

The expanding and blurring of the IT perimeter is the main reason companies have an IT security gap. According to Figure 2, 55 percent of respondents say it is hard to protect the expanding and blurring IT perimeter with IoT, BYOD, mobile and cloud. Other reasons for the IT security gap are shortages in staffing and the lack of visibility into what every user and device is doing while connected to the IT infrastructure (both 49 percent of respondents).

Figure 2. Why the IT security gap exists

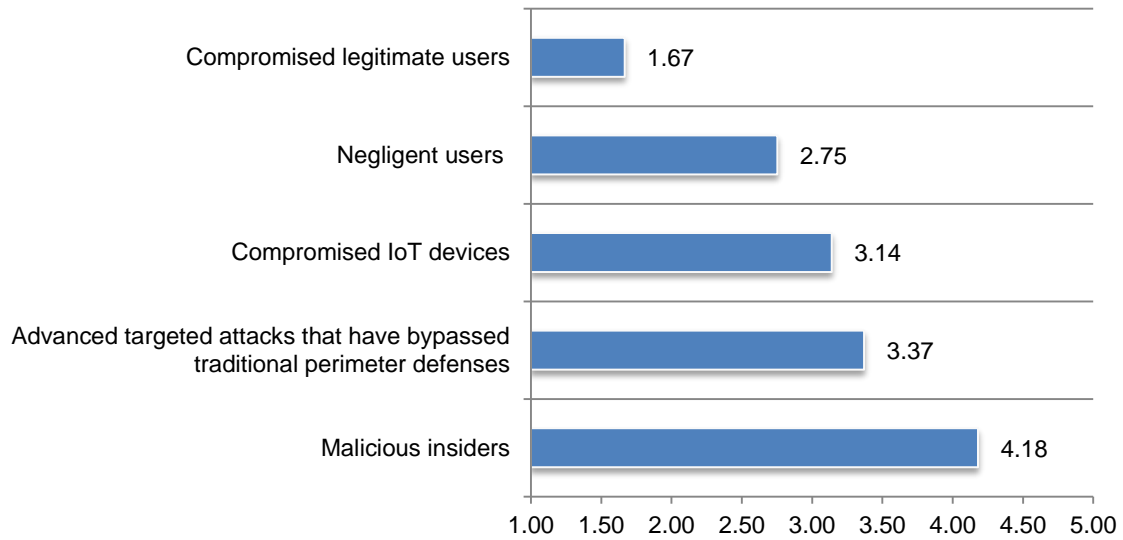
Four responses permitted



Compromised legitimate users are considered the greatest risk. Respondents were asked to rate five factors that pose the greatest inside threat from 1 = highest threat to 5 = lowest threat. As shown in Figure 3, individuals who have legitimate access inside the organization pose the greatest threat. These are compromised legitimate users as well as negligent users. The inability to see and detect compromised IoT devices is also creating a significant risk for organizations.

Figure 3. Where are the greatest threats from the inside?

1 = highest threat to 5 = lowest threat



The risk of noncompliance with GDPR and other privacy regulations

IT security gaps exacerbate the risk of noncompliance with certain GDPR obligations.

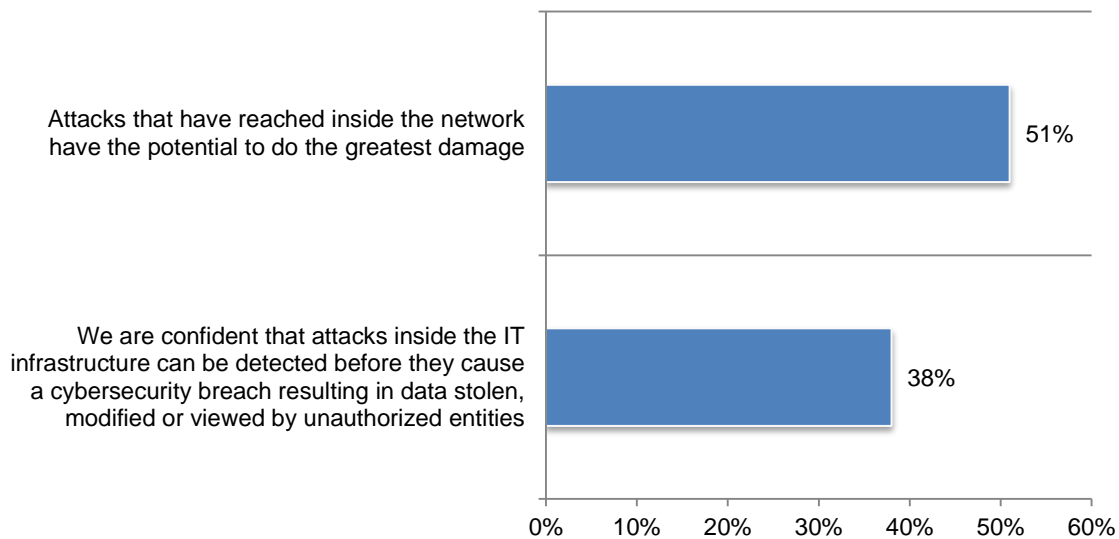
According to another recent Ponemon Institute study,¹ many companies believe their organizations are at a high risk if they fail to comply with specific GDPR obligations. Participants in this study believe that the greatest risk is for fines and regulatory action. Other cited risks include notification obligations, including operationalizing the right to be forgotten, conducting data inventory/mapping activities, obtaining/managing user consent, and establishing legitimate interest for data processing.

The IT security gap leaves the IT infrastructure vulnerable to attack. As shown in Figure 4, only 38 percent of respondents are confident that attacks inside the IT infrastructure can be detected before they cause a cybersecurity breach that results in data being stolen, modified, or viewed by unauthorized entities.

Fifty-one percent of respondents say attacks that have reached inside the network have the potential to do the greatest damage. According to the GDPR, in the event of a personal data breach, the companies must notify authorities within 72 hours. If there is a delay, companies must provide a “reasoned justification”.

Figure 4. The IT security gap in the IT infrastructure

Strongly Agree and Agree responses combined

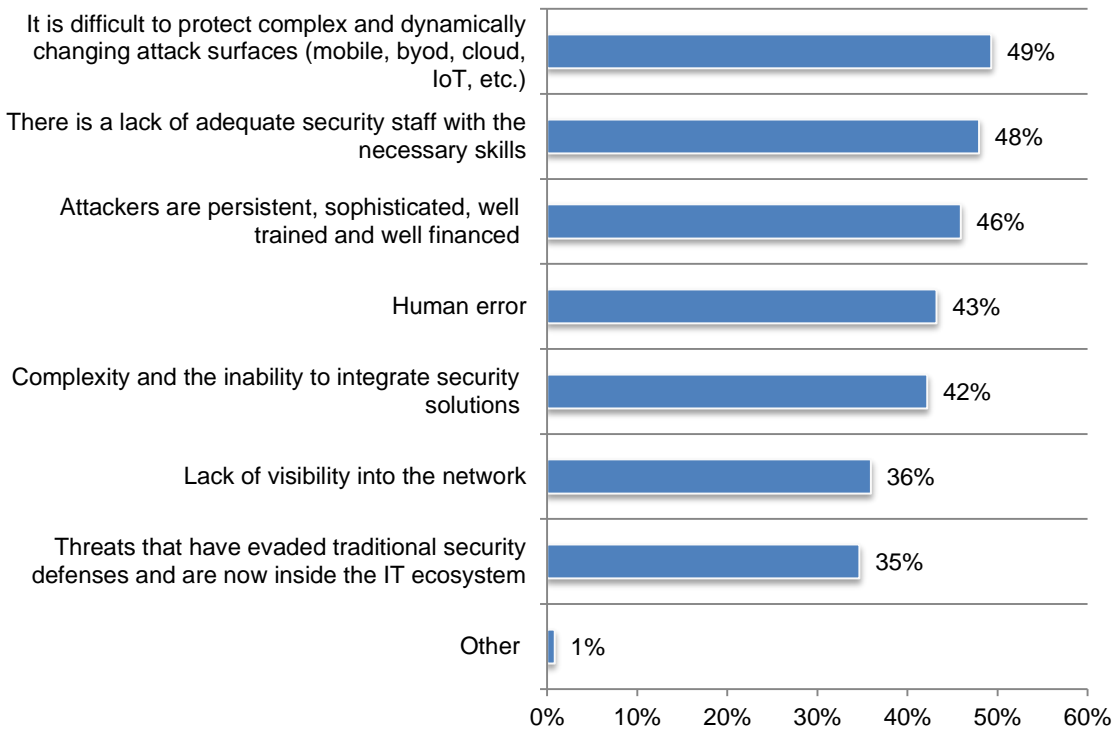


¹ *The Race to GDPR: A Study of Companies in the United States & Europe*, conducted by Ponemon Institute and sponsored by McDermott, Will & Emery, LLP, April 2018

Despite all the investments in cybersecurity programs, breaches are still happening. As a result of the IT security gap, companies are unable to stop all data breaches. According to Figure 5, almost half (49 percent of respondents) say it is difficult to protect complex and dynamically changing attack surfaces such as mobile, BYOD, cloud and IoT and 48 percent say there is a skills gap because of the lack of adequate security staff with the necessary expertise. Another reason is that today's attackers are persistent, sophisticated, well-trained and well-financed (46 percent).

Figure 5. Why data breaches still happen

Three responses permitted



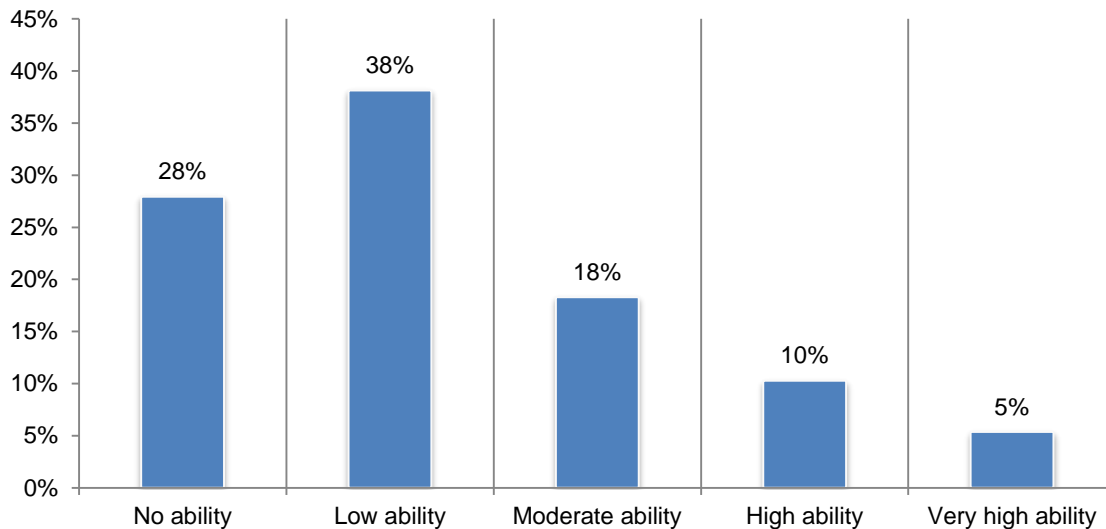
Is the IoT widening the IT security gap?

The inability to secure IoT devices and apps is exacerbating the IT security gap.

Respondents were asked to rate their organization's ability to secure IoT devices and apps from 1 = no ability to 5 = very high ability. As shown in Figure 6, 66 percent of respondents say their organization has no, or a low ability, to secure their IoT devices and apps. More than half of respondents (51 percent) say IoT visibility is important to detecting attacks.

Figure 6. The ability to secure IoT devices and apps

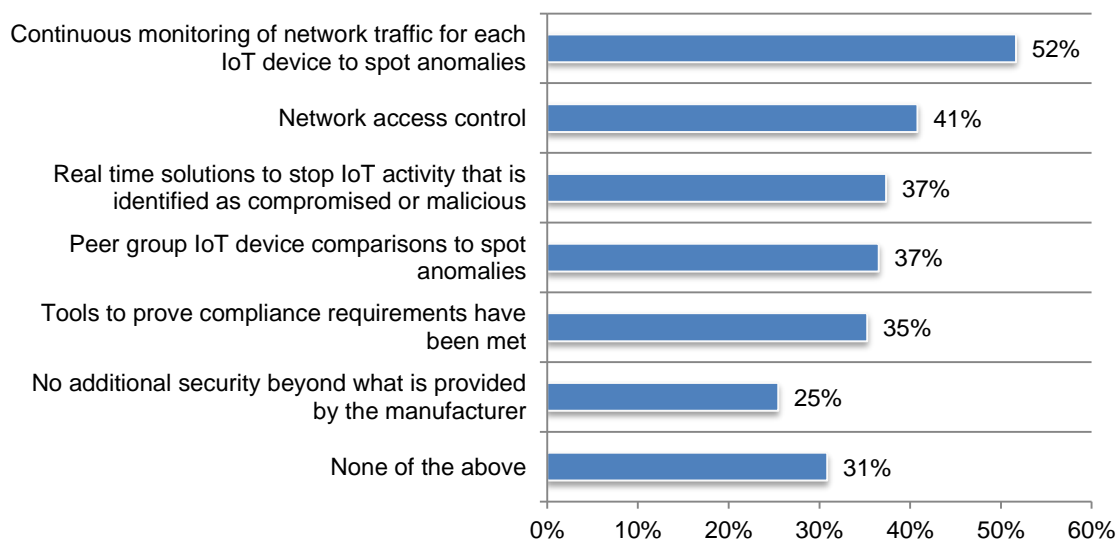
1 = no ability to 5 = very high ability



As presented in Figure 7, 52 percent of respondents say continuous monitoring of network traffic for each IoT device is required to spot anomalies and achieve a strong level of security. NAC is also important to addressing IoT risks according to 41 percent of respondents.

Figure 7. How to achieve a strong level of IoT security

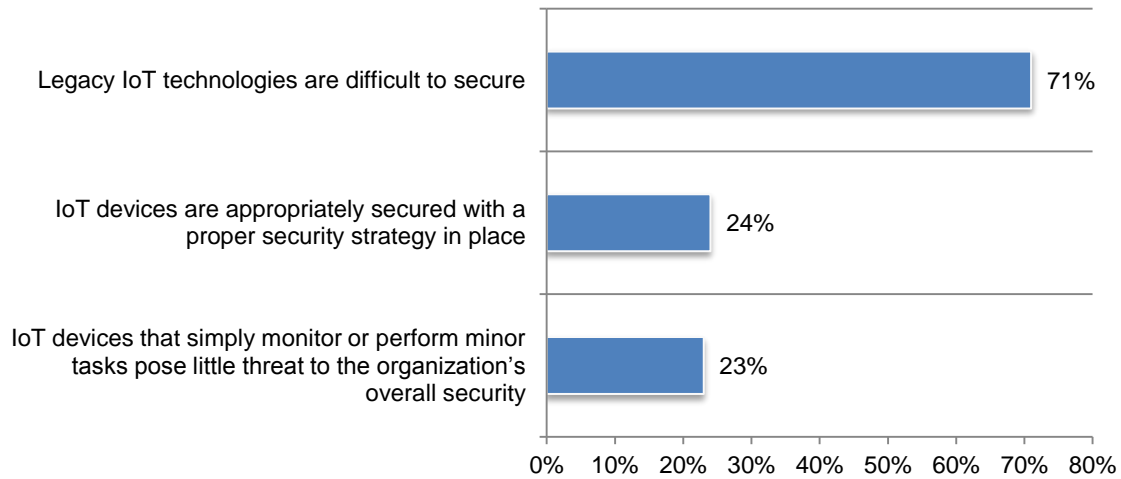
More than one response permitted



Why IoT devices are widening the IT security gap. As described in Figure 8, 23 percent of respondents believe that even IoT devices that simply monitor or perform minor tasks pose little threat to their organization’s security. Seventy-one percent of respondents agree that legacy IoT technologies are difficult to secure. As a consequence, only 24 percent of respondents say their organization’s IoT devices are appropriately secured with a proper security strategy in place.

Figure 8. Perceptions about IoT security

Strongly agree and Agree responses combined

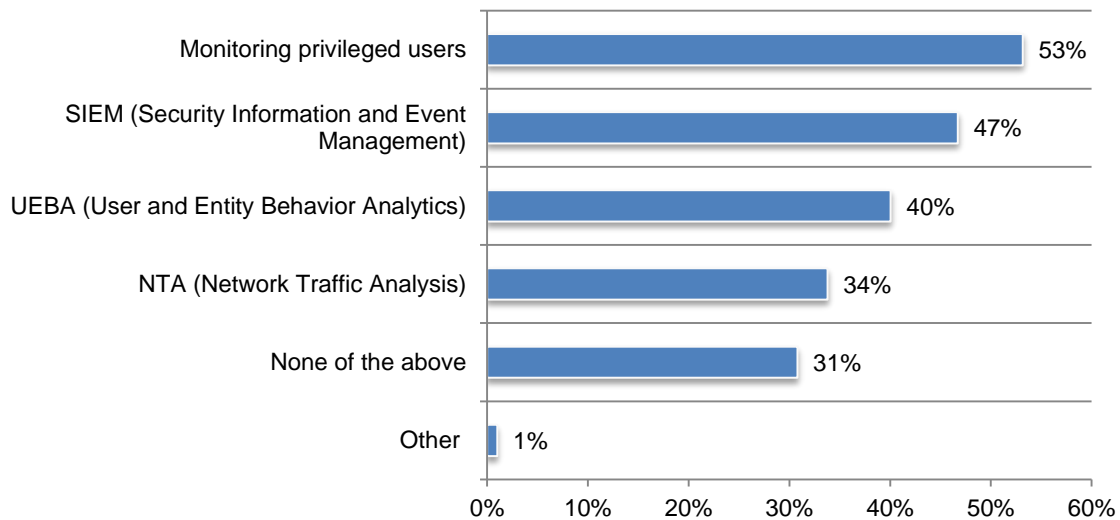


Solutions to closing the IT security gap

New technologies are needed to close the IT security gap. Sixty-four percent of respondents say new technologies such as ML are needed to discover, understand and neutralize threats that are active in the IT infrastructure. Currently, only 45 percent of respondents say their organizations are getting the full value from their current security investments.

Figure 9 describes steps that respondents believe are important for minimizing stealthy and hidden threats within the IT infrastructure include monitoring privileged users (53 percent), SIEM (47 percent) and User and Entity Behavior Analytics (40 percent), which is increasingly seen as a way to monitor high value assets while “turbocharging” existing SIEM installations.

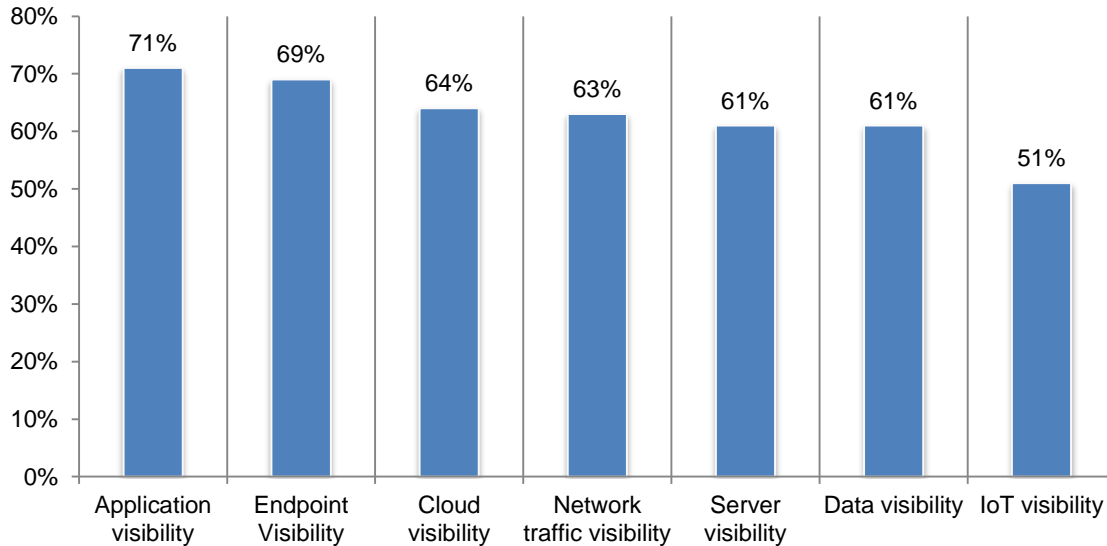
Figure 9. What steps can minimize stealthy, hidden threats within the IT infrastructure
More than one response permitted



Application and endpoint visibility is most important to detecting attacks from the inside. Respondents were asked to rate the various types of visibility in terms of detecting attacks on the inside from 1 = not important to 5 = very high importance. Figure 10 shows that, 71 percent of respondents say application visibility is critical to detecting attacks and 69 percent of respondents believe endpoint visibility is important. Also important is cloud and network traffic visibility (64 percent and 63 percent, respectively).

Figure 10. The importance of visibility in detecting attacks on the inside

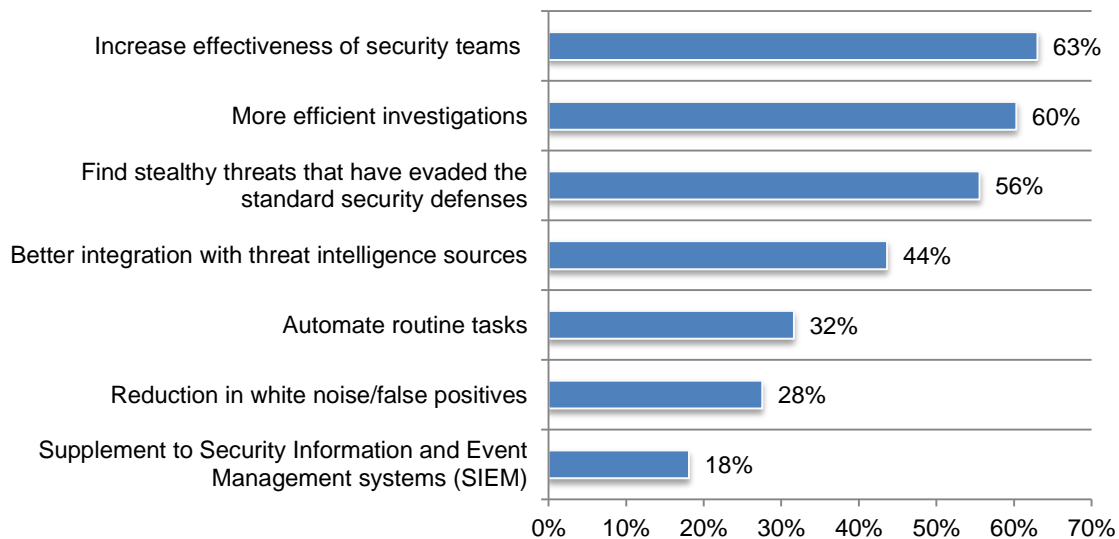
Very high importance and High importance combined



Is AI-based ML hype or reality? More than half of respondents (51 percent) agree that AI technologies such as ML and behavioral analytics are essential for detecting attacks on the inside before they can do damage. As shown in Figure 11, the top three benefits of using these technologies are an increase in effectiveness of security teams, more efficient investigations and the ability to find stealthy threats that have evaded standard security defenses (63 percent, 60 percent and 56 percent of respondents respectively).

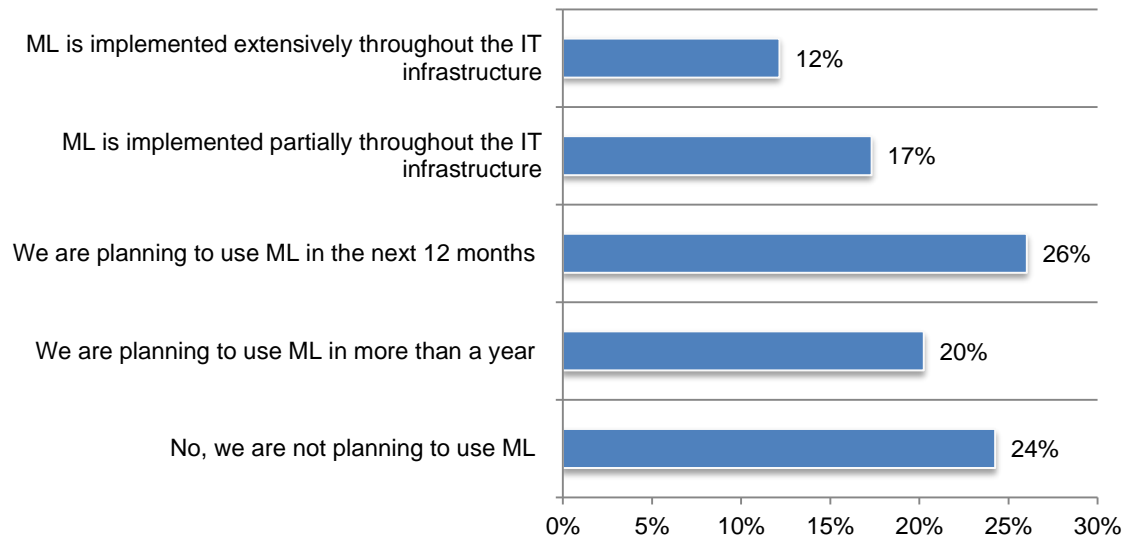
Figure 11. The top security benefits from ML and advanced analytics

Three responses permitted



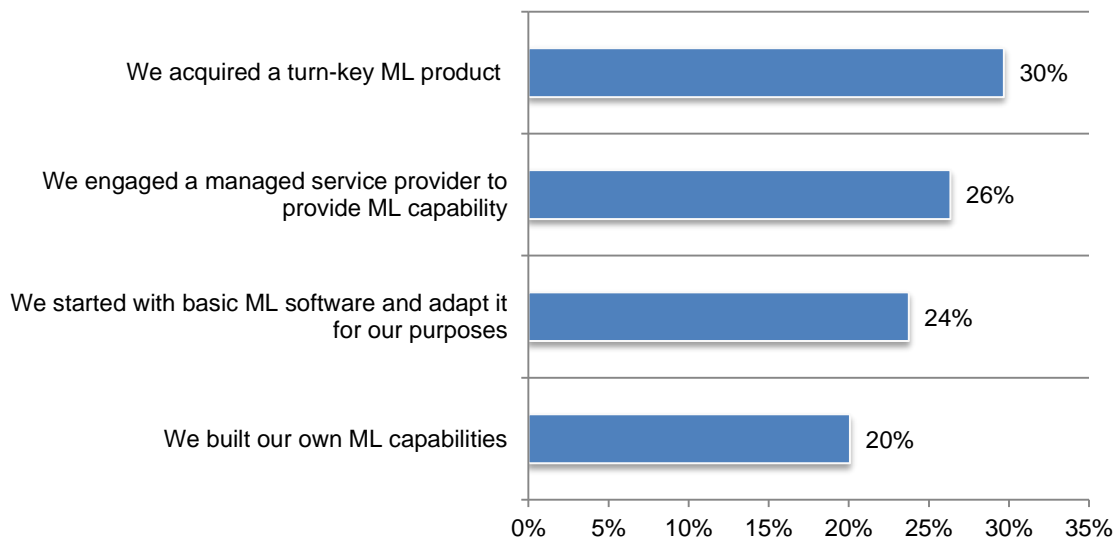
Most organizations are planning to use ML for security purposes. As shown in Figure 12, currently 29 percent of respondents say ML is implemented extensively throughout their IT infrastructure (12 percent) or partially (17 percent). Forty-six percent of respondents say they will have ML in the next 12 months (26 percent) or in more than a year (20 percent).

Figure 12. How ML is used



Of those organizations that have ML, 30 percent say they acquired a turnkey ML product or engaged a managed service provider (26 percent). Only 20 percent of respondents say they built their own ML capabilities.

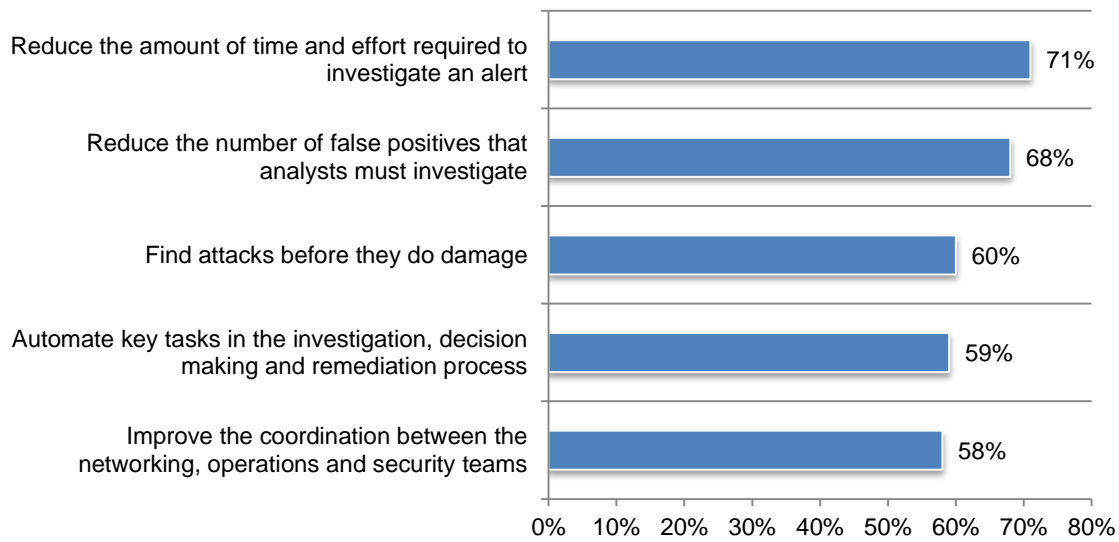
Figure 13. How ML is deployed for attack detection



The biggest benefit of automation is considered to be reducing the amount of time and effort required to investigate an alert. Respondents were asked to rate the importance of specific benefits of automation to achieving a more efficient and effective security posture from 1 = not important to 5 = very high importance. Figure 14 shows the most important benefit of this technology is the ability to reduce the amount of time and effort required to investigate an alert (71 percent respondents), followed by a reduction in the number of false positives that analysts must investigate (68 percent of respondents).

Figure 14. Importance of benefits from automation

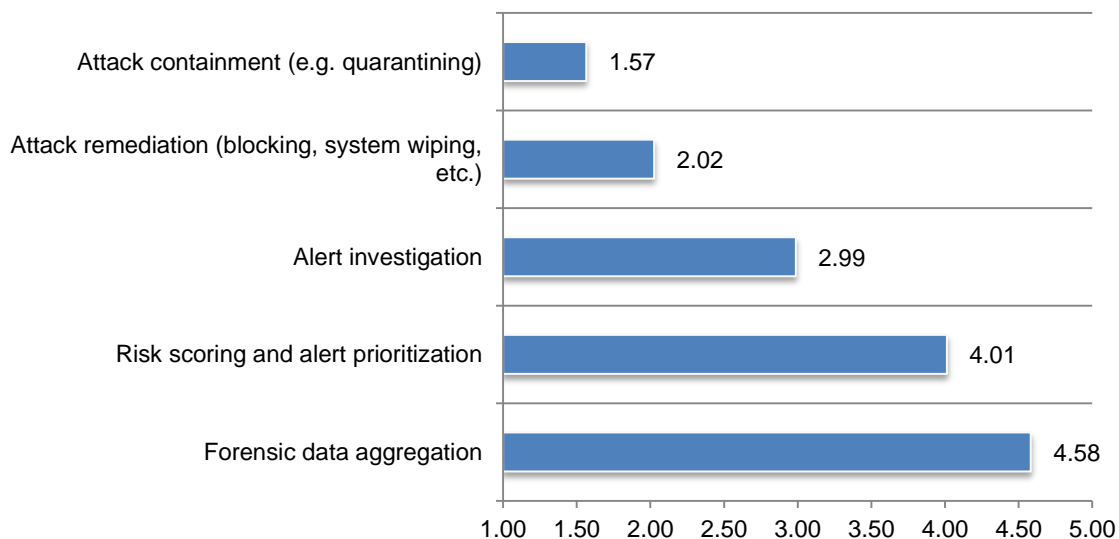
Very high importance and High importance combined



Respondents were asked to rate the following processes most likely to be automated by their organization from 1 = most likely to 5 = least likely. As shown in Figure 15, the processes that will most likely be automated are attack containment and attack remediation.

Figure 15. Processes most likely to be automated

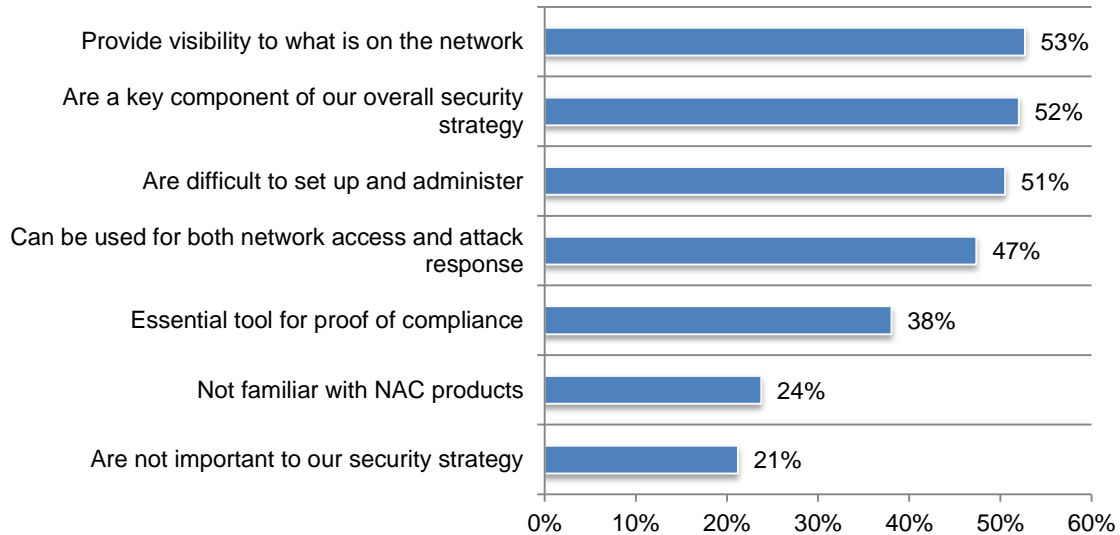
1 = most likely to 5 = least likely



NAC is considered important for providing visibility into what is on networks. Respondents believe their NAC products provide visibility into what is on the network (53 percent) or it is a key component of their overall security strategy (52 percent). However, more than half (51 percent) say NAC products are difficult to set up and administer, according to Figure 16.

Figure 16. How NAC products are deployed

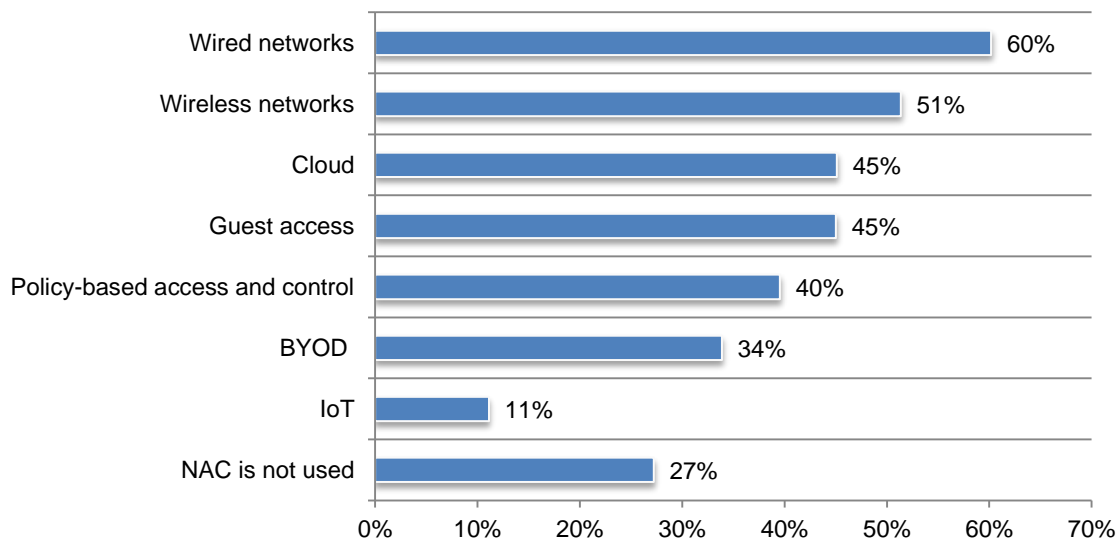
More than one response permitted



Seventy-three percent of respondents say their organizations deploy NAC. Most of them are deployed for wired networks (60 percent of respondents) or wireless networks (51 percent of respondents). However, only 18 percent of respondents are very confident or confident that they know all the users and devices connected to their network all the time.

Figure 17. Purposes for NAC products

More than one response permitted



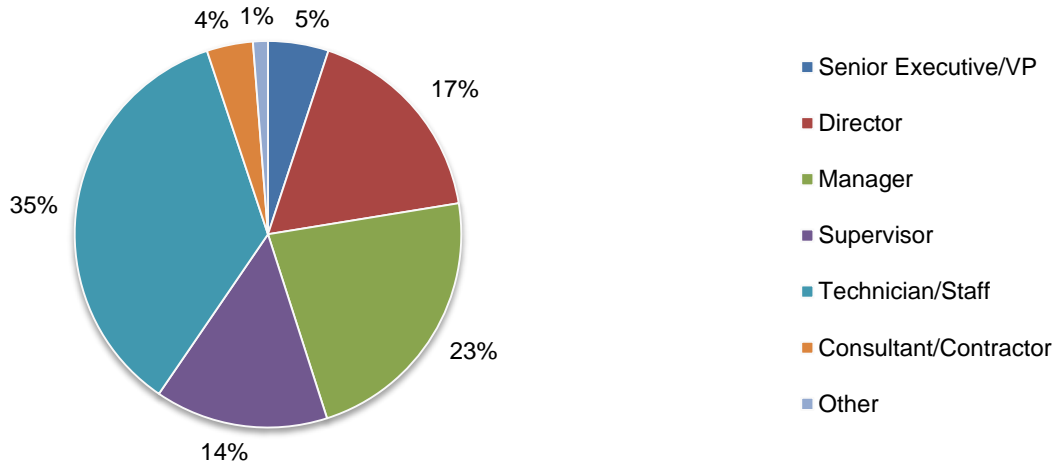
Part 3. Methods

The sampling frame is composed of 115,471 IT and IT security practitioners in the following three regions and eight countries: Asia-Pacific, EMEA, North America, Australia, Brazil, Germany, India, Japan, Mexico, Singapore and the United Kingdom. As shown in Table 1, 4,385 respondents completed the survey. Screening removed 519 surveys. The final sample was 3,866 surveys (or a 3.3 percent response rate).

| Table 1. Sample response | Freq | Pct% |
|---------------------------------|-------------|-------------|
| Total sampling frame | 115,471 | 100.0% |
| Total returns | 4,385 | 3.8% |
| Rejected or screened surveys | 519 | 0.4% |
| Final sample | 3,866 | 3.3% |

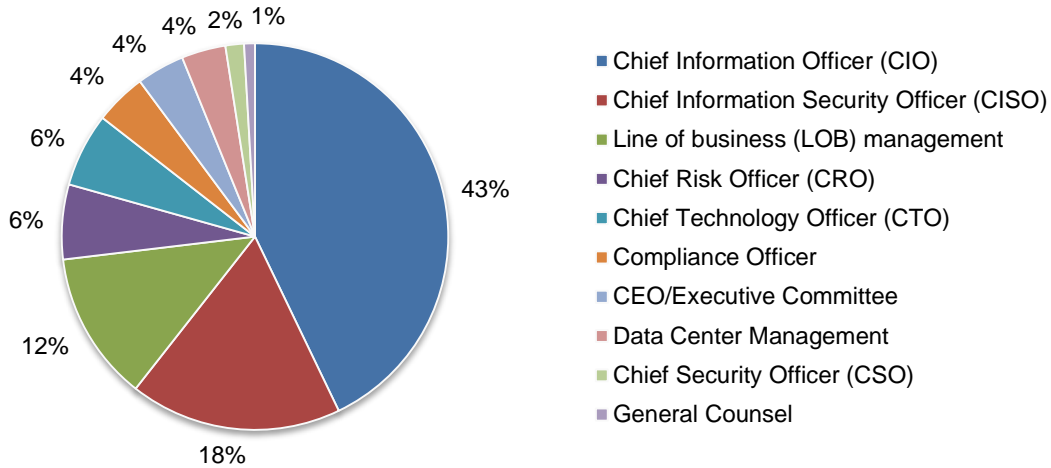
Pie Chart 1 reports the current position or organizational level of the respondents. Fifty-nine percent of respondents reported their current position as supervisory or above.

Pie Chart 1. Distribution of respondents according to position level



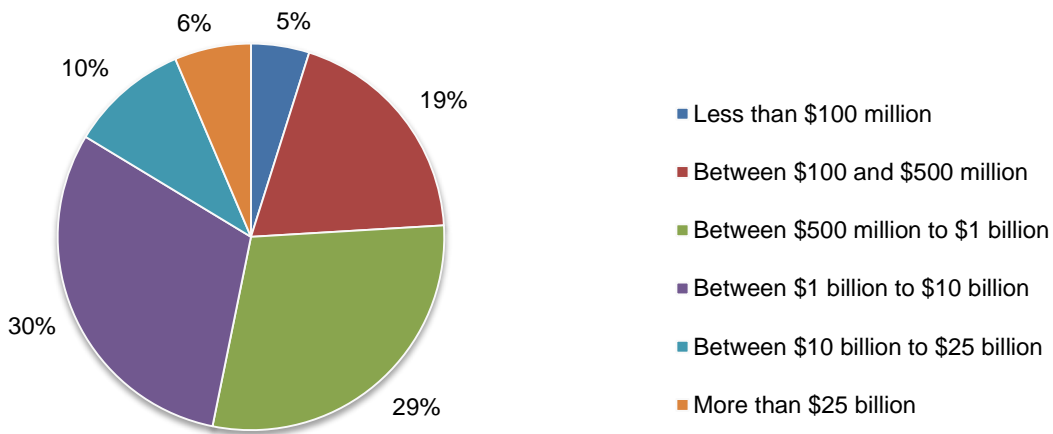
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Forty-three percent of respondents identified the chief information officer as the person to whom they report. Another 18 percent indicated they report directly to the chief information security officer and 12 percent of respondents report to a line of business leader.

Pie Chart 2. Distribution of respondents according to reporting channel



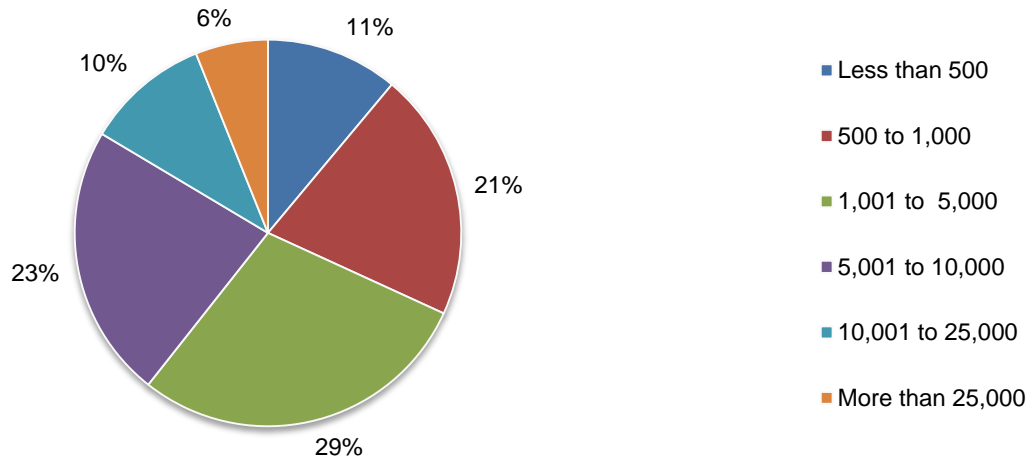
Pie Chart 3 reports the worldwide revenue of the respondents' organizations. Seventy-six percent of respondents reported their organization's annual worldwide revenue to be more than \$500 million.

Pie Chart 3. Distribution of respondents according to worldwide revenue
US dollars



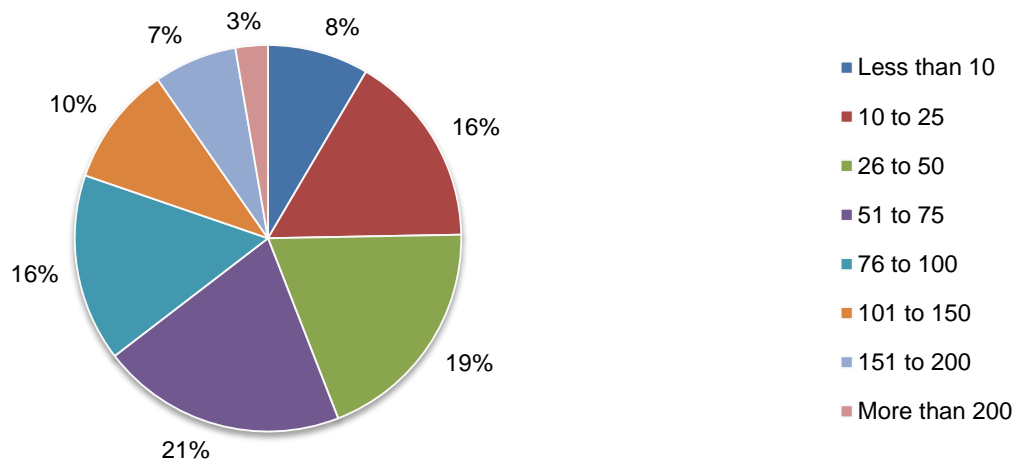
According to Pie Chart 4, 68 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Distribution of respondents according to the number of employees within the organization



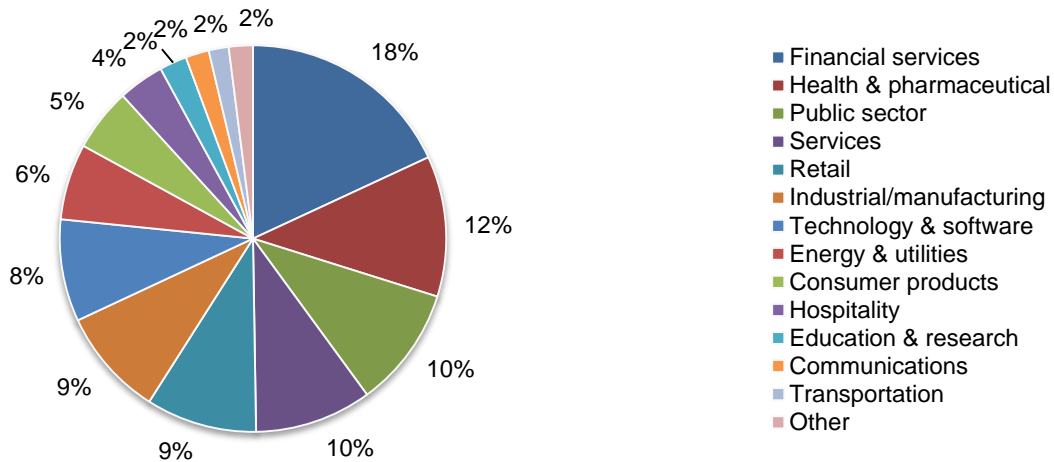
Pie Chart 5 reports the number of security solutions in use within the respondents' organizations. Seventy-six percent of respondents reported that their organizations are currently using more than 25 security solutions.

Pie Chart 5. Distribution of respondents according to the number security solutions



Pie Chart 6 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by health and pharmaceuticals (12 percent of respondents), the public sector (10 percent of respondents) and the services sector (10 percent of respondents).

Pie chart 6. Distribution of respondents according to primary industry classification



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in various organizations in Asia-Pacific, EMEA, North America, Australia, Brazil, Germany, India, Japan, Mexico, Singapore and the United Kingdom. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured March 6 to March 20, 2018.

| Survey response | Global |
|------------------|---------|
| Sampling frame | 115,471 |
| Total returns | 4,385 |
| Rejected surveys | 519 |
| Final sample | 3,866 |
| Response rate | 3.3% |
| Same weights | 1.00 |

Part 1. Screening

| S1. What best describes your involvement in IT security investments within your organization? | Global |
|---|--------|
| None (stop) | 0% |
| Responsible for overall solution/purchase | 50% |
| Responsible for administration/management | 58% |
| Involved in evaluating solutions | 68% |
| Total | 176% |

| S2. What best describes your role within your organization's IT or IT security department? | Global |
|--|--------|
| Security leadership (CSO/CISO) | 38% |
| IT management | 43% |
| IT operations | 50% |
| Security management | 53% |
| Security monitoring and response | 65% |
| Data administration | 29% |
| Compliance administration | 16% |
| Applications development | 25% |
| Data protection office | 2% |
| I'm not involved in my organization's IT or IT security function (stop) | 0% |
| Total | 321% |

| S3. How knowledgeable are you about your organization's IT security strategy and tactics? | Global |
|---|--------|
| Very knowledgeable | 36% |
| Knowledgeable | 48% |
| Somewhat knowledgeable | 16% |
| Slightly knowledgeable (stop) | 0% |
| No knowledge (stop) | 0% |
| Total | 100% |

Part 2: Attributions

| | |
|--|--------|
| Q1. Please rate each one of the following statements using the agreement scale provided below each item. | |
| Q1a. Security teams lack visibility and control into all the activity of every user and device (i.e., mobile, BYOD, IoT) connected to their IT infrastructure. | Global |
| Strongly agree | 32% |
| Agree | 35% |
| Unsure | 14% |
| Disagree | 11% |
| Strongly disagree | 8% |
| Total | 100% |

| | |
|--|--------|
| Q1b. New technologies such as machine learning are needed to discover and understand threats that are active in the IT infrastructure. | |
| | Global |
| Strongly agree | 29% |
| Agree | 35% |
| Unsure | 16% |
| Disagree | 13% |
| Strongly disagree | 7% |
| Total | 100% |

| | |
|--|--------|
| Q1c. In my experience, the IT security infrastructure has gaps that allow attackers to penetrate its defenses. | |
| | Global |
| Strongly agree | 29% |
| Agree | 33% |
| Unsure | 20% |
| Disagree | 11% |
| Strongly disagree | 8% |
| Total | 100% |

| | |
|---|--------|
| Q1d. My organization is getting the full value from our current security investments. | |
| | Global |
| Strongly agree | 20% |
| Agree | 25% |
| Unsure | 27% |
| Disagree | 18% |
| Strongly disagree | 10% |
| Total | 100% |

| Q2. What are the primary gaps in your organization's IT security infrastructure? Please select your top four choices. | Global |
|---|--------|
| Security staff and skills shortages | 49% |
| Too many alerts to address | 36% |
| Too many false positives | 45% |
| Security solutions can't keep up with exponentially increasing amounts of data | 41% |
| Hard to protect expanding and blurring IT perimeter with IoT, BYOD, mobile and cloud | 55% |
| Siloed security solutions | 38% |
| Inability of traditional perimeter-based security solutions to detect and stop advanced targeted attacks | 41% |
| Lack of visibility into every user and device connected to the IT infrastructure | 45% |
| Lack of visibility into what every user and device is doing while connected to the IT infrastructure | 49% |
| Other (please specify) | 1% |
| Total | 400% |

| Q3. Despite all the cybersecurity investments made by companies, why are breaches still happening? Please select your top three choices. | Global |
|--|--------|
| It is difficult to protect complex and dynamically changing attack surfaces (mobile, BYOD, cloud, IoT, etc.) | 49% |
| There is a lack of adequate security staff with the necessary skills | 48% |
| Attackers are persistent, sophisticated, well trained and well financed | 46% |
| Complexity and the inability to integrate security solutions | 42% |
| Lack of visibility into the network | 36% |
| Threats that have evaded traditional security defenses and are now inside the IT ecosystem | 35% |
| Human error | 43% |
| Other (please specify) | 1% |
| Total | 300% |

Part 3. Attacks on the inside

| Q4. Please rate each one of the following statements using the agreement scale provided below each item. | |
|--|--------|
| Q4a. Attacks that have reached inside the network have the potential to do the greatest damage. | Global |
| Strongly agree | 26% |
| Agree | 25% |
| Unsure | 21% |
| Disagree | 17% |
| Strongly disagree | 11% |
| Total | 100% |

| Q4b. We are confident that attacks inside the IT infrastructure can be detected before they cause a cybersecurity breach that results in data being stolen, modified or viewed by unauthorized entities. | Global |
|--|--------|
| Strongly agree | 18% |
| Agree | 20% |
| Unsure | 20% |
| Disagree | 26% |
| Strongly disagree | 16% |
| Total | 100% |

| Q5. Which of the following do you believe pose the greatest inside threat to your IT infrastructure? Please rank each threat from 1 = highest threat to 5 = lowest threat. | Global |
|--|--------|
| Compromised legitimate users | 1.67 |
| Malicious insiders | 4.18 |
| Negligent users | 2.75 |
| Compromised IoT devices | 3.14 |
| Advanced targeted attacks that have bypassed traditional perimeter defenses | 3.37 |
| Average | 3.06 |

| Q6. What steps should be taken to minimize stealthy, hidden threats within the IT infrastructure? Please check all that apply. | Global |
|--|--------|
| UEBA | 40% |
| SIEM | 47% |
| NTA (Network Traffic Analysis) | 34% |
| Monitoring privileged users | 53% |
| None of the above | 31% |
| Other (please specify) | 1% |
| Total | 206% |

| Q7. Using the following 5-point scale, please rate the importance of the following types of visibility in terms of detecting attacks on the inside from 1 = not important to 5 = very high importance. | |
|--|--------|
| Q7a. Network traffic visibility | Global |
| 1 = not important | 6% |
| 2 = low importance | 11% |
| 3 = moderate importance | 20% |
| 4 = high importance | 37% |
| 5 = very high importance | 26% |
| Total | 100% |
| Extrapolated value | 3.65 |

| Q7b. Server visibility | |
|--------------------------|--------|
| | Global |
| 1 = not important | 9% |
| 2 = low importance | 11% |
| 3 = moderate importance | 18% |
| 4 = high importance | 31% |
| 5 = very high importance | 30% |
| Total | 100% |
| Extrapolated value | 3.62 |

| Q7c. Application visibility | |
|-----------------------------|--------|
| | Global |
| 1 = not important | 1% |
| 2 = low importance | 5% |
| 3 = moderate importance | 22% |
| 4 = high importance | 31% |
| 5 = very high importance | 40% |
| Total | 100% |
| Extrapolated value | 4.03 |

| Q7d. Data visibility | Global |
|--------------------------|--------|
| 1 = not important | 7% |
| 2 = low importance | 11% |
| 3 = moderate importance | 22% |
| 4 = high importance | 29% |
| 5 = very high importance | 32% |
| Total | 100% |
| Extrapolated value | 3.69 |

| Q7e. Cloud visibility | Global |
|--------------------------|--------|
| 1 = not important | 7% |
| 2 = low importance | 13% |
| 3 = moderate importance | 15% |
| 4 = high importance | 35% |
| 5 = very high importance | 29% |
| Total | 100% |
| Extrapolated value | 3.65 |

| Q7f. IoT visibility | Global |
|--------------------------|--------|
| 1 = not important | 9% |
| 2 = low importance | 15% |
| 3 = moderate importance | 24% |
| 4 = high importance | 26% |
| 5 = very high importance | 25% |
| Total | 100% |
| Extrapolated value | 3.43 |

| Q7g. Endpoint visibility | Global |
|--------------------------|--------|
| 1 = not important | 1% |
| 2 = low importance | 10% |
| 3 = moderate importance | 20% |
| 4 = high importance | 35% |
| 5 = very high importance | 34% |
| Total | 100% |
| Extrapolated value | 3.91 |

Part 4. AI-based Machine Learning – Hype or Reality?

| Q8. AI technologies (machine learning, behavioral analytics) are essential to detecting attacks on the inside before they do damage. | Global |
|--|--------|
| Strongly agree | 22% |
| Agree | 29% |
| Unsure | 25% |
| Disagree | 17% |
| Strongly disagree | 6% |
| Total | 100% |

| Q9. What are the top three key security benefits of using ML and advanced analytics? Please select your top three choices. | Global |
|---|--------|
| Automate routine tasks | 32% |
| Find stealthy threats that have evaded the standard security defenses | 56% |
| Increase effectiveness of security teams | 63% |
| Better integration with threat intelligence sources | 44% |
| More efficient investigations | 60% |
| Reduction in white noise/false positives | 28% |
| Supplement to SIEM systems | 18% |
| Total | 300% |

| Q10a. What one statement best describes the use of ML for security purposes within your organization? | Global |
|---|--------|
| ML is implemented extensively throughout the IT infrastructure | 12% |
| ML is implemented partially throughout the IT infrastructure | 17% |
| We are planning to use ML in the next 12 months (please skip to Q12) | 26% |
| We are planning to use ML in more than a year (please skip to Q12) | 20% |
| No, we are not planning to use ML (please skip to Q12) | 24% |
| Total | 100% |

| Q10b. What one statement best describes how ML is deployed for attack detection? | Global |
|--|--------|
| We built our own ML capabilities | 20% |
| We started with basic ML software and adapt it for our purposes | 24% |
| We engaged a managed service provider to provide ML capability | 26% |
| We acquired a turn-key ML product | 30% |
| Total | 100% |

| Q11. What best describes how the market considers ML-based attack detection solutions? | Global |
|--|--------|
| It is important to be a standalone function as the last line of defense | 21% |
| It is considered an important supplement to SIEM | 15% |
| It will be a feature in other security products | 29% |
| Too early to tell | 35% |
| Total | 100% |

Part 5. Automation

| Q12. Using the following 5-point scale, please rate the importance of the following benefits of automation to achieving a more efficient and effective security posture from 1 = not important to 5 = very high importance. | |
|---|--------|
| Q12a. Reduce the number of false positives that analysts must investigate | Global |
| 1 = not important | 3% |
| 2 = low importance | 7% |
| 3 = moderate importance | 21% |
| 4 = high importance | 38% |
| 5 = very high importance | 30% |
| Total | 100% |
| Extrapolated value | 3.84 |

| Q12b. Reduce the amount of time and effort required to investigate an alert | Global |
|---|--------|
| 1 = not important | 1% |
| 2 = low importance | 5% |
| 3 = moderate importance | 23% |
| 4 = high importance | 41% |
| 5 = very high importance | 30% |
| Total | 100% |
| Extrapolated value | 3.95 |

| Q12c. Find attacks before they do damage | Global |
|--|--------|
| 1 = not important | 4% |
| 2 = low importance | 10% |
| 3 = moderate importance | 26% |
| 4 = high importance | 36% |
| 5 = very high importance | 24% |
| Total | 100% |
| Extrapolated value | 3.67 |

| Q12d. Improve the coordination between the networking, operations and security teams | Global |
|--|--------|
| 1 = not important | 6% |
| 2 = low importance | 10% |
| 3 = moderate importance | 26% |
| 4 = high importance | 30% |
| 5 = very high importance | 28% |
| Total | 100% |
| Extrapolated value | 3.63 |

| Q12e. Automate key tasks in the investigation, decision making and remediation process | Global |
|--|--------|
| 1 = not important | 5% |
| 2 = low importance | 12% |
| 3 = moderate importance | 24% |
| 4 = high importance | 29% |
| 5 = very high importance | 30% |
| Total | 100% |
| Extrapolated value | 3.65 |

| Q13. Which of the following processes will most likely be automated by your organization? Please rank each process from 1 = most likely to 5 = least likely. | Global |
|--|--------|
| Risk scoring and alert prioritization | 4.01 |
| Forensic data aggregation | 4.58 |
| Alert investigation | 2.99 |
| Attack containment (e.g. quarantining) | 1.57 |
| Attack remediation (blocking, system wiping, etc.) | 2.02 |
| Average | 3.03 |

Part 6. Network Access Control (NAC)

| | |
|---|--------|
| Q14. What is your level of confidence that you know ALL the users and devices connected to your network ALL the time? | Global |
| Very confident | 5% |
| Confident | 13% |
| Somewhat confident | 16% |
| Not confident | 32% |
| No confidence | 34% |
| Total | 100% |

| | |
|--|--------|
| Q15. What statements best describe your opinion about NAC products deployed by your organization? Please check all that apply. | Global |
| Are not important to our security strategy | 21% |
| Provide visibility into what is on the network | 53% |
| Are difficult to set up and administer | 51% |
| Are a key component of our overall security strategy | 52% |
| Can be used for both network access and attack response | 47% |
| Not familiar with NAC products | 24% |
| Essential tool for proof of compliance | 38% |
| Total | 286% |

| | |
|--|--------|
| Q16. For what purposes are NAC systems deployed within your organization? Please check all that apply. | Global |
| Wired networks | 60% |
| Wireless networks | 51% |
| Guest access | 45% |
| BYOD | 34% |
| IoT | 11% |
| Cloud | 45% |
| Policy-based access and control | 40% |
| NAC is not used | 27% |
| Total | 313% |

Part 7. Internet of things (IoT)

| | |
|--|--------|
| Q17. Using the following 5-point scale, please rate your organization's ability to secure IoT devices and apps from 1 = no ability to 5 = very high ability. | Global |
| 1 = no ability | 28% |
| 2 = low ability | 38% |
| 3 = moderate ability | 18% |
| 4 = high ability | 10% |
| 5 = very high ability | 5% |
| Total | 100% |
| Extrapolated value | 2.27 |

| Q18. What is required to achieve a strong level of IoT security within your organization? Please check all that apply. | Global |
|---|--------|
| NAC | 41% |
| Continuous monitoring of network traffic for each IoT device to spot anomalies | 52% |
| Peer group IoT device comparisons to spot anomalies | 37% |
| Real time solutions to stop IoT activity that is identified as compromised or malicious | 37% |
| Tools to prove compliance requirements have been met | 35% |
| No additional security beyond what is provided by the manufacturer | 25% |
| Other (please specify) | 0% |
| None of the above | 31% |
| Total | 258% |

| Q19. Please rate each one of the following statements using the agreement scale provided below each item. | Global |
|---|--------|
| Q19a. IoT devices are appropriately secured with a proper security strategy in place. | Global |
| Strongly agree | 11% |
| Agree | 13% |
| Unsure | 14% |
| Disagree | 33% |
| Strongly disagree | 29% |
| Total | 100% |

| Q19b. Legacy IoT technologies are difficult to secure. | Global |
|--|--------|
| Strongly agree | 33% |
| Agree | 38% |
| Unsure | 18% |
| Disagree | 9% |
| Strongly disagree | 2% |
| Total | 100% |

| Q19c. IoT devices that simply monitor or perform minor tasks pose little threat to our organization's overall security. | Global |
|---|--------|
| Strongly agree | 11% |
| Agree | 12% |
| Unsure | 17% |
| Disagree | 29% |
| Strongly disagree | 31% |
| Total | 100% |

| Q20. Who within your organization is most responsible for ensuring the security of IoT devices and apps? | Global |
|--|--------|
| Chief information officer (CIO) | 34% |
| Chief technology officer (CTO) | 5% |
| Chief information security officer (CISO) | 18% |
| Chief security officer (CSO) | 3% |
| Line of business leadership | 11% |
| End-users of IoT devices | 13% |
| Data Protection Officer (DPO) | 0% |
| No one function has overall responsibility | 15% |
| Other (please specify) | 1% |
| Total | 100% |

Part 8. Your role and organization

| D1. What organizational level best describes your current position? | Global |
|---|--------|
| Senior Executive/VP | 5% |
| Director | 17% |
| Manager | 23% |
| Supervisor | 14% |
| Technician/Staff | 35% |
| Consultant/Contractor | 4% |
| Other | 1% |
| Total | 100% |

| D2. Check the Primary Person you or your leader reports to within the organization. | Global |
|---|--------|
| CEO/Executive Committee | 4% |
| General Counsel | 1% |
| Chief Information Officer (CIO) | 43% |
| Chief Technology Officer (CTO) | 6% |
| Chief Information Security Officer (CISO) | 18% |
| Compliance Officer | 4% |
| Line of business (LOB) management | 12% |
| Chief Security Officer (CSO) | 2% |
| Data Center Management | 4% |
| Chief Risk Officer (CRO) | 6% |
| Other | 0% |
| Total | 100% |

| D3. What range best defines the worldwide revenue of your organization? (US dollars) | Global |
|--|--------|
| Less than \$100 million | 5% |
| Between \$100 and \$500 million | 19% |
| Between \$500 million to \$1 billion | 29% |
| Between \$1 billion to \$10 billion | 30% |
| Between \$10 billion to \$25 billion | 10% |
| More than \$25 billion | 6% |
| Total | 100% |

| D4. How many employees are in your organization? | Global |
|--|--------|
| Less than 500 | 11% |
| 500 to 1,000 | 21% |
| 1,001 to 5,000 | 29% |
| 5,001 to 10,000 | 23% |
| 10,001 to 25,000 | 10% |
| More than 25,000 | 6% |
| Total | 100% |

| D5. How many security solutions does your organization use? | Global |
|---|--------|
| Less than 10 | 8% |
| 10 to 25 | 16% |
| 26 to 50 | 19% |
| 51 to 75 | 21% |
| 76 to 100 | 16% |
| 101 to 150 | 10% |
| 151 to 200 | 7% |
| More than 200 | 3% |
| Total | 100% |
| Extrapolated value | 68 |

| D6. What best describes your organization's primary industry classification? | Global |
|--|--------|
| Agriculture & food services | 1% |
| Communications | 2% |
| Consumer products | 5% |
| Defense & aerospace | 0% |
| Education & research | 2% |
| Energy & utilities | 6% |
| Entertainment & media | 1% |
| Financial services | 18% |
| Health & pharmaceutical | 12% |
| Hospitality | 4% |
| Industrial/manufacturing | 9% |
| Public sector | 10% |
| Retail | 9% |
| Services | 10% |
| Technology & software | 8% |
| Transportation | 2% |
| Total | 100% |

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.