Cognizant

2019 Security Trends Report

The Security Challenge: What's next?

While regulatory actions and the move to SaaS has added complexity to keeping enterprise IT secure, new technologies such as AI and DevSecOps offer new forms of relief.

July 2019

Executive Summary

In a recent survey we asked security managers and architects across multiple industry verticals to rank the top trends they believed would be impactful in 2019 (see Methodology, page 15).

Four major trends emerged, ranked as follows:

1. **Artificial intelligence (AI) and machine learning promise to speed the analysis of reams of network and security data**, easing the jobs of analysts who today must juggle as many as 100 tools to decipher up to 10,000 alerts per day. Judging the AI claims of security vendors is tricky. AI itself requires new, hard to find skills, to implement properly and can itself be compromised with disastrous results when used incorrectly.

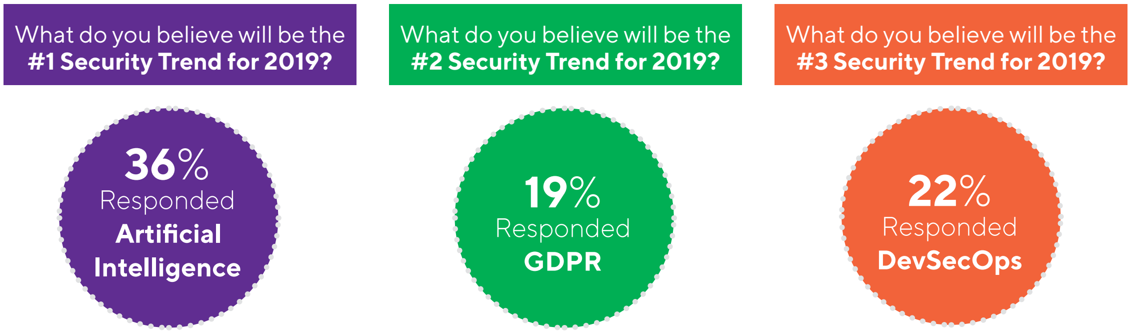
2. **The European Union's General Data Protection Regulation (GDPR)** is still causing major compliance headaches, especially in coping with data subject access or deletion requests, and reviewing and enforcing privacy requirements in third party contracts.

3. **More organizations are using DevSecOps** – the process of integrating security within the software development lifecycle long before an app reaches the traditional testing stage to speed deployment of new application releases to market. But it requires major changes to processes and culture, such as more open communication between security and development teams and empowering developers to take responsibility for testing their own code.

4. **More organizations are turning to software as a service (SaaS)** offerings to meet growing security needs. The lower up-front costs and subscription based service fee, quick turnaround on setup, ease of upgrades, accessibility, and scalability are highly attractive to any consumers of IT Services, but some respondents worry about its dependability, understanding they will lose a level of control over some elements like connectivity, or access to the environment, which is particularly concerning due to the sensitive nature of data stored in security systems. While we only asked respondents for the top three trends, SaaS in our opinion would be the fourth.

In this research summary we examine the respondents' plans in each of these four areas and, combining our research with that of other industry leaders, provide recommendations for action moving forward. We also examine other less often cited, but still important issues such as securing data from the Internet of Things (IoT), and security orchestration, automation and response (SOAR).

Scoring Security Threats



What do you believe will be the **#1 Security Trend for 2019?**

36% Responded **Artificial Intelligence**

What do you believe will be the **#2 Security Trend for 2019?**

19% Responded **GDPR**

What do you believe will be the **#3 Security Trend for 2019?**

22% Responded **DevSecOps**

- Artificial intelligence / Machine learning
- DevSecOps
- GDPR
- Integrated risk management
- IoT
- SaaS (software as a service)
- SOAR (security orchestration & automation response)

Source: Cognizant Response base: 71
Figure 1

TREND 1

Artificial Intelligence

Six out of ten respondents called AI a top trend in 2019, with their plans focusing about equally on security analytics, security incident and event management, and endpoint protection.

Over 50% of those citing AI as a top trend planned to purchase more of this technology in 2019, with implementation equally split between the development of internal tools and buying from a vendor.

There were a wide variety of use cases and vendors mentioned by respondents, which range from:

- Identity and access management solutions such as Sailpoint or Silverfort. This includes AI in its adaptive authentication.
- Security analytics tools such as Elastic/Elk stack
- SIEM (security information and event management) solutions such as Splunk AIops, or the Logrhythm AI engine. which contain AIdriven anomaly detection
- Endpoint protection applications, such as Darktrace Enterprise Immune System

We didn’t consider physical security applications such as robotic process automation and intelligent CCTV, which were also mentioned by respondents to the survey.

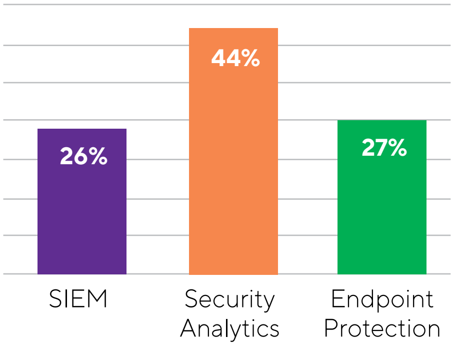
Machine learning is a branch of artificial intelligence which uses algorithms that can learn from example data sets, and experience. This can help identify anomalies such as suspicious network traffic patterns and log-in attempts more quickly in order to prevent security breaches.

AI can be used to mimic human behavior and to some degree simulate cognitive reasoning by training on data sets using deep learning techniques. Public cloud providers such as Amazon Web Services sell pre-trained AI services, allowing organizations to quickly deploy intelligent applications and data science software at scale, using a pay-as-you-go model. This gives them the flexibility to procure additional algorithms for highly diverse purposes, and immediately start using themin what could be called ‘intelligence-as-a-service.”

AI is emerging as a useful tool as networks have become increasingly complex, as have new threats such as self-propagating fileless polymorphic shellcode that can leverage encryption to avoid detection by more traditional means. Endpoint security is also becoming a greater challenge due to the proliferation of personal devices, which hackers target with phishing scams, as well as the growth of IoT. Increasingly sophisticated attackers can now find, and exploit, new vulnerabilities in a matter of minutes.

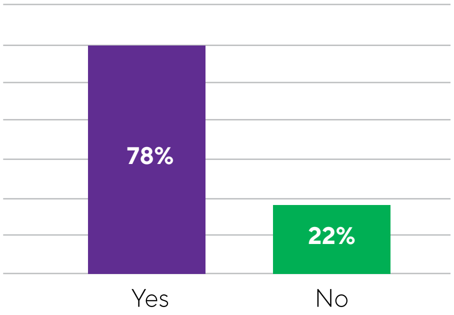
Amid these threats, enterprises report a chronic shortage of staff skilled in the 25, 50 or even 100 security tools the average organization uses, to respond to up to 10,000 alerts a day. With recent surveys indicating analysts can only investigate five to ten issues per day, it is of critical importance to apply AI to reduce the time required to look for outliers, connect widely diverse data points, and develop a threat profile.

What products would be best suited for your environment that incorporate artificial intelligence/machine learning?



Source: Cognizant Response base: 43
Figure 2

Will the product(s) greatly improve your security posture?



Source: Cognizant Response base: 43
Figure 3

All this has resulted in a tendency to see AI as the magic bullet to get ahead in the arms race. While pragmatic AI applications such as anomalous user behavior monitoring and detecting spam and phishing emails are likely to become commonplace, nearly every vendor is trying to integrate this technology buzzword into their software whether it has any tangible benefit or not.

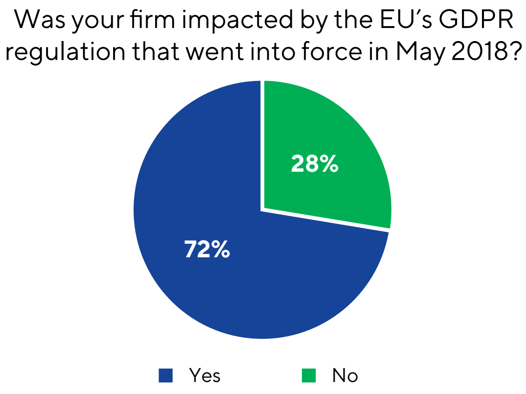
As we know from experience, the bad guys will simply adapt their approach as well, using AI to fool and circumvent these defenses like they have others. One example is using AI to retrain malware on-the-fly to adapt and respond to external circumstances, making it far less easy to detect using popular sandbox technologies. There is also the risk hackers will infect an AI system with bias so it fails to correctly identify attacks. All this means that, despite the real promise of AI, it will ultimately also result in more complex and highly targeted attacks.

It is worthwhile to use AI to crunch through the large data sets generated, and reduce the amount of false positives in a modern SIEM environment. But simply investing in this new technology is not likely to be enough in the long run, and only exacerbates the skills shortage issue as security analysts need to be trained in AI. To get the most from AI, security staff must:

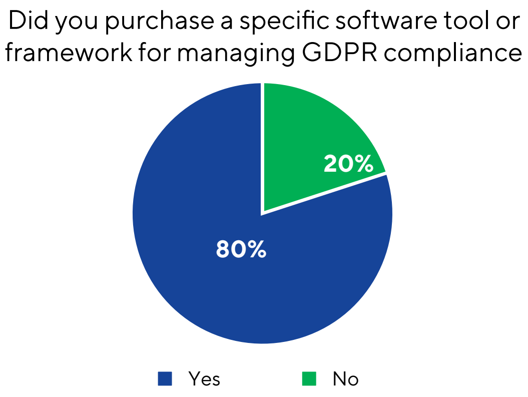
- Learn to navigate vendor claims about whether and how AI really improves their security.
- Properly integrate newer AI tools with existing security databases and analytic platforms.
- Give their security staffs the proper skills to use AI (or partner with other firms that have such skills,) and
- Recognize and minimize the threat that hackers will use AI to strengthen their attacks or to subvert AI security systems o they cannot detect actual attacks.

TREND 2

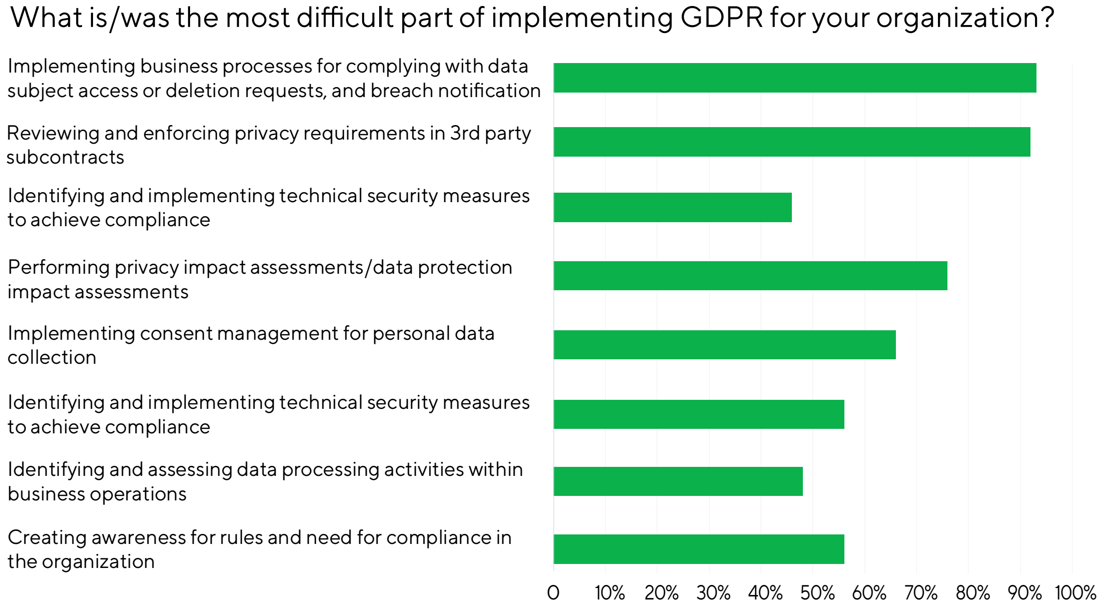
GDPR Compliance



Source: Cognizant Response base: 29
Figure 4



Source: Cognizant Response base: 21
Figure 5



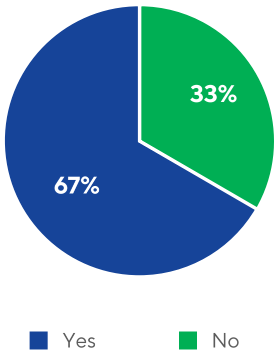
Source: Cognizant Response base: 21 Note: Multiple responses permitted
Figure 6

The European Union 's GDPR covers more than 500 million citizens in 28 countries. Devising and executing a compliance plan is a significant challenge, as shown by the fact that 72% of respondents' organizations are affected by GDPR, and 40% of our respondents listed it as a top trend for 2019. It is also not for the faint-hearted, and there are no quick fixes, as shown by the fact our respondents reported an average 10-month preparation time before the legislation went into effect on May 25, 2018.

Identifying the personal data of EU citizens that organizations process and store has proven complex, with one challenge ensuring that board members and senior executives understand the risks to their business models.

Implementing business processes for complying with subject access or deletion requests, as well as reviewing and enforcing privacy requirements in third-party contracts, were considered the most difficult parts of GDPR implementation. Surprisingly, identifying and implementing technical measures to achieve compliance was seen as the most straightforward. Only 6% of those surveyed indicated they had acquired a specific software tool for managing GDPR compliance, an interesting fact considering the number of tools available on the market, that claim to be able to deliver GDPR compliance.

Was your organization finished with preparations for BAU by May 25, 2018 ?



Source: Cognizant Response base: 21
Figure 6

Many companies have adapted a wait-and-see model, hoping to benefit from the experience of others and assuming it will take time before EU regulators begin fining laggards. This stems from lack of executive buy-in, as well as the natural tendency of humans to procrastinate and lay responsibility for non-compliance at the doorstep of others. As many EU citizens saw when the regulation came into effect, this even resulted in large numbers of (primarily U.S.-based) companies with international visibility completely blocking access to their sites rather than spending the time required to assess and manage their data to assure compliance.

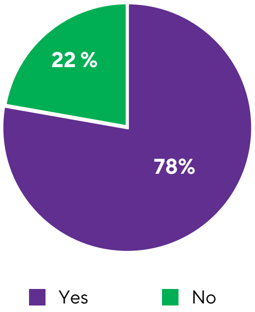
Managing changes to third-party contracts, such as adapting standard terms or corporate rules to include transfer of personal data to processors, can be cumbersome to implement for complex personal data. While those in the financial services and healthcare industries are more conversant with managing regulatory compliance, those in other industries have struggled extensively to meet the compliance goals and have relied on the thriving consultancy business which has sprung up around the regulation. While software vendors are eager to claim their GDPR compliance solution is best, this often reflects changes to their marketing messaging only.

To achieve the most efficient and complete GDPR compliance, organizations doing business with EU citizens should:

- Ensure they have a full understanding of why their businesses collect personal data on EU citizens, ensure these are obtaining opt-in permission for collecting and using this data, and explain clearly what purposes it is used for.
- Ensure they have undertaken data protectionimpact assessments on any high risk data collected, and report any breaches to the relevant data protection authorities within 72 hours.
- Embed full lifecycle security by design, to safeguard the private data of EU Citizens if it is collected.

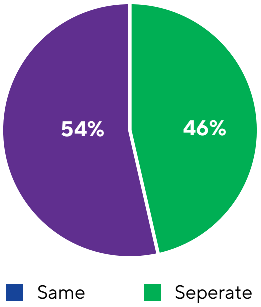
DevSecOps

Is your company using Agile/DevOps or CI/CD methodologies to accelerate software development?



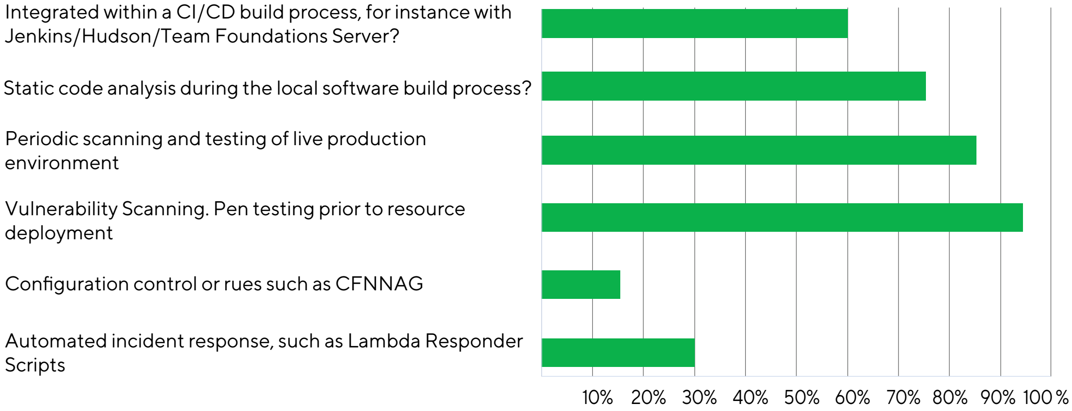
Source: Cognizant Response base: 36
Figure 7

Is the DevOps practice also responsible for ensuring security is built in to the applications or does this fall to a separate team?



Source: Cognizant Response base: 28
Figure 8

Are you using any of the following tools to improve security in your software delivery pipeline?



Source: Cognizant Response base: 28
Figure 9

Security professionals have traditionally believed developers don’t care about security. They do, but are under too much pressure to speed new software to market to collaborate with their counterparts in security. Today, DevOps and continuous integration/continuous delivery models can require code releases multiple times a week or even per day. Even when developers attempt to work with security professionals, they don´t speak the same language. Security has focused on the more traditional, collaborative approach of managing code through audit and review, whereas the DevOps paradigm includes the management of infrastructure as code, using templates and continuous deployment models.

These are the problems DevSecOps – embedding security throughout the software development, deployment, and operations process – seeks to solve. It is no surprise that 49% of the respondents listed DevSecOps as one of their top three trends in 2019.

Our respondents reported mixed success. On the plus side, they reported performing DevSecOps practices such as vulnerability scanning and penetration testing before deployment, as well as periodic infrastructure scans and static code analysis, in around 50% of their use cases.

However, the use of configuration or control rules to restrict capabilities were not commonplace. Roughly half the respondents make the DevOps team also responsible for security, a key enabler of DevSecOps. Such relatively low adoption levels for DevSecOps practices shows that while organizations are trying to embed security in the development process, the security function is still not trusted enough to get out of the way of the business fast enough in a pinch.

Adopting DevSecOps requires changes in both testing methodologies and culture. On the testing side, best practices no longer call for testing every portion of an application as untrusted, and thus requiring the entire application to be scanned, tested, and fully reviewed before deployment. Building security into a nimble DevSecOps practice instead calls for locking down specific areas which, if not changed, can be presumed to be secure.This concept of immutability eliminates configuration drift and reduces changes to the attack surface, maintaining consistency and accelerating the deployment of point releases. It also facilitates deployment rollbacks, should vulnerabilities be found in areas which have been changed to support new features.

A software supply chain which builds infrastructure on the fly using code, must operate at high speed and not pass defects downstream. Compliance and security reviews cannot be permitted to slow down the process, and are frequently overlooked.

Preventive measures must be applied during build and deployment phases, taking advantage of automation, and providing the right set of tools for each area. It is also essential to maintain good communication among the development and security teams, standardize on processes and adopt security policies and common tools, that ensure changes can be enforced at scale, especially in larger environments.

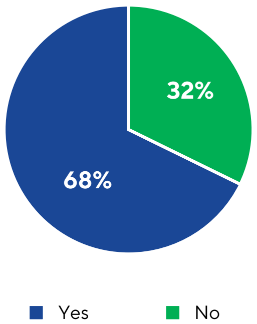
Getting the maximum agility and security benefits of DevSecOps thus requires:

- **Changes to testing processes**, to reflect trends such as the increased immutability of software subcomponents.
- **Changes to culture**, such as more open communication between security and development teams, a joint focus on the twin goals of speed and security and empowering developers to take responsibility for testing their own code, and
- **The appropriate use of automation** to speed processes, especially as they scale.

TREND 4

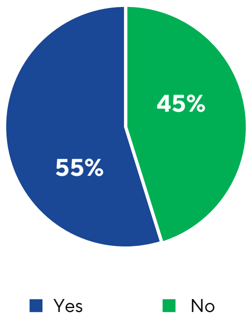
Software as a Service

Are you already using a SaaS platform for some aspect of Security?



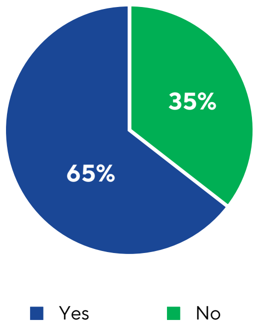
Source: Cognizant Response base: 31
Figure 10

Are you concerned about the dependability of SaaS platforms?



Source: Cognizant Response base: 21
Figure 11

Do you have plans to move any more pieces of your security deployment to a SaaS in 2019?



Source: Cognizant Response base: 21
Figure 12

Cloud-based infrastructure and services often allows organizations to adopt, deploy and scale new capabilities more quickly, cost-effectively, and flexibly than in-house deployments. It’s therefore perhaps no surprise that 43% listed software as a service as one of the top 2019 trends. Two-thirds of our respondents are using cloud applications to provide some aspect of their security, with almost as many (64%) planning to expand such use in 2019.

What is more surprising, and troubling, is that 54% of our respondents are concerned about the dependability of SaaS platforms. Such concerns are warranted because the data collected by security applications is often among the most sensitive in the organization. A compromised SaaS could even be used to distribute malware to some of the most sensitive users, the security department itself. With more and more bad guys taking the time to profile and infiltrate organizations by masquerading as privileged users, the leakage of credentials belonging to the security team members for instance, could result in a difficult and expensive clean-up, as well as allowing attackers to get further access into the organization’s highly sensitive, privileged information that security teams and tools are privy to.

Some essential precautions:

- Storing encryption keys for data in the cloud separately from the data they protect, so the keys are not under the control of the SaaS provider.
- Because many SaaS platforms do not rigorously support user identity management, consider implementing cloud-based identity and access management.
- Consider implementing a high-fidelity cloud access security broker with data loss protection functionality, which integrates with cloud applications to prevent data leakage and keep applications free of malware.

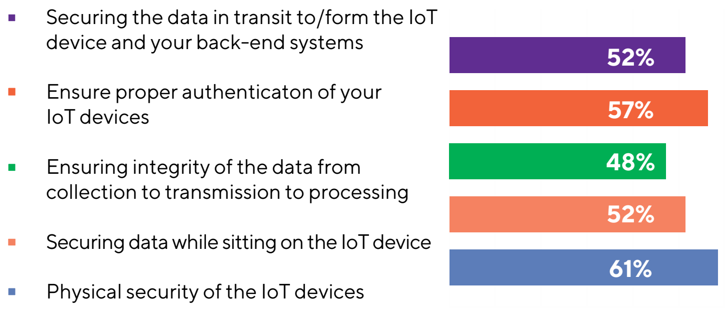
Overlooked Technologies

The security technologies and trends our respondents rated poorly are also important, as they show where the industry marketing hype is outrunning reality, or implementation challenges are holding back customer adoption. This can be due to economic realities, as companies don’t necessarily need to be on the bleeding edge of technology, or complexity of implementing them in a way that generates value to the organization quickly.

While a relatively high 43% of respondents chose IoT as a top trend, only 13% of them are planning an IoT purchase this year. We see an increasing sense that the impact of IoT data collection has been over-emphasized, with many implementers still discovering what data is needed for analysis, and not yet tapping it for insights.

Early adopters have found using IoT data for predictive and preventative maintenance can be a key driver in improving profits. However, the lack of robust security is a big concern in preventing the adoption of IoT devices, as incidents can be extremely costly to an organization. When it comes to IoT data security, our respondents gave equal weight to physical security, securing data on the device, maintaining integrity in transmission, authentication and to back-end systems.

What aspect of securing IoT concerns you the most?



Source: Cognizant Response base: 71

Figure 13

Security orchestration, automation and response (SOAR) – a relatively new term describing the convergence of orchestration, automation, incident response and threat intelligence — generated the least enthusiasm with only 7% considering it a significant trend in 2019. SOAR use cases include enriching alerts with data that helps first responders speed alert triage and investigation, automatic quarantining of machines to prevent lateral movement of malware, responding to phishing attacks and automating retrieval of forensic data and blacklisting IP addresses on perimeter firewalls.

SOAR adoption is likely being held back by the anticipated effort of integrating and implementing a self-remediating solution and developing dependable automation playbooks for security response. These let human analysts focus on designing proper controls, policies and tuning them to handle exceptions, reducing the impact of the security skills gap. However, designing such playbooks requires experienced architects with an in-depth understanding of building and maintaining organizational security policies, as well as relevant automation use cases, skills which are not yet common across the industry.

Final Thoughts

It may sound cynical but adding security as an afterthought to new technology will probably continue as long as it is a profitable business model. However, hardware and software vendors will likely be increasingly challenged by the world at large to build security in from the start, rather than bolting it on afterwards and creating unnecessary complexity and additional vulnerabilities.

Organizations must begin by applying the basic principles of least privilege, compartmentalization and business resilience to their user identities, data, end points and applications. Attempts to legislate security have resulted in a compliance culture, with a reliance on audits proving compliance with weak and outdated regulations, often reviewed by a deliberately overburdened auditor under time pressure to identify areas of non-compliance, wasting valuable time and effort in what is little more than a vanity project for senior security and risk managers.

Companies would be well served to remember that regulations are only implemented when industry fails to do the right thing by itself, and that proactive solutions when conceived, applied and managed properly to ensure the organizations users, data, endpoints and applications are secure, are preferable to after the fact compliance.

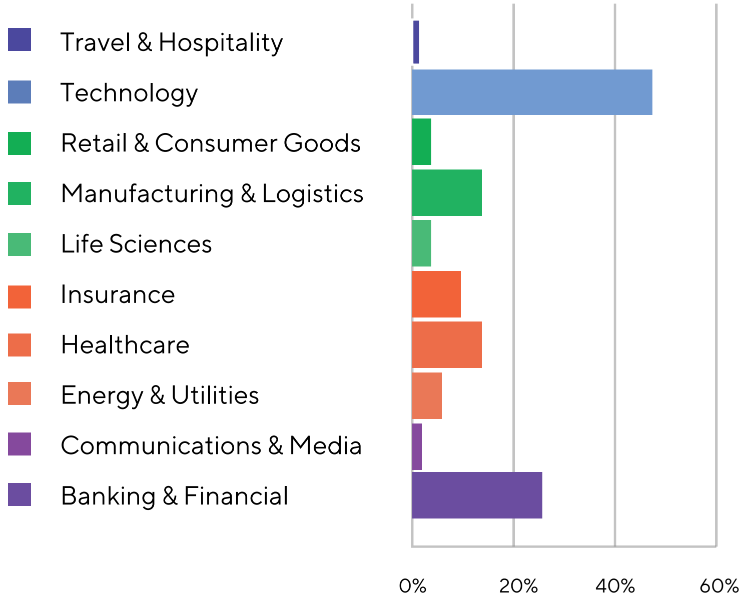
The good news is that the security industry is slowly maturing, with vendors more willing and able to provide real value to back up their marketing. Security budgets are increasingly moving beyond mere compliance to prevention. This will help customers reap the rewards of new development techniques such as DevOps, and meet new challenges such as complying with GDPR.

Security managers across all industries must still continuously expend significant effort to keep up to date on the latest technology trends and vendors, and ensure they share their insights with their peers. With cyberattacks increasing in number and severity, the very real danger of them incurring direct financial loss, as well as the effects publicly disclosed breaches can have on shareholder confidence, has put security firmly on the radar for boards of directors.

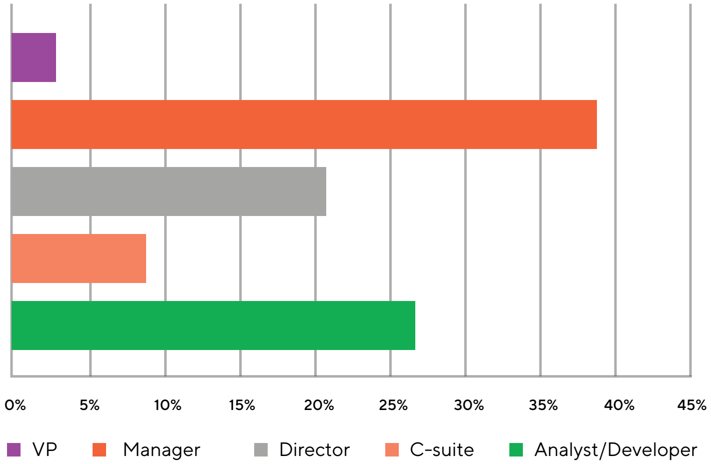
Appendix: Methodology

This survey was an online survey (we provided the survey at a few sponsored events in late 2018). The survey was provided in the U.S. Total number of respondents was 71.

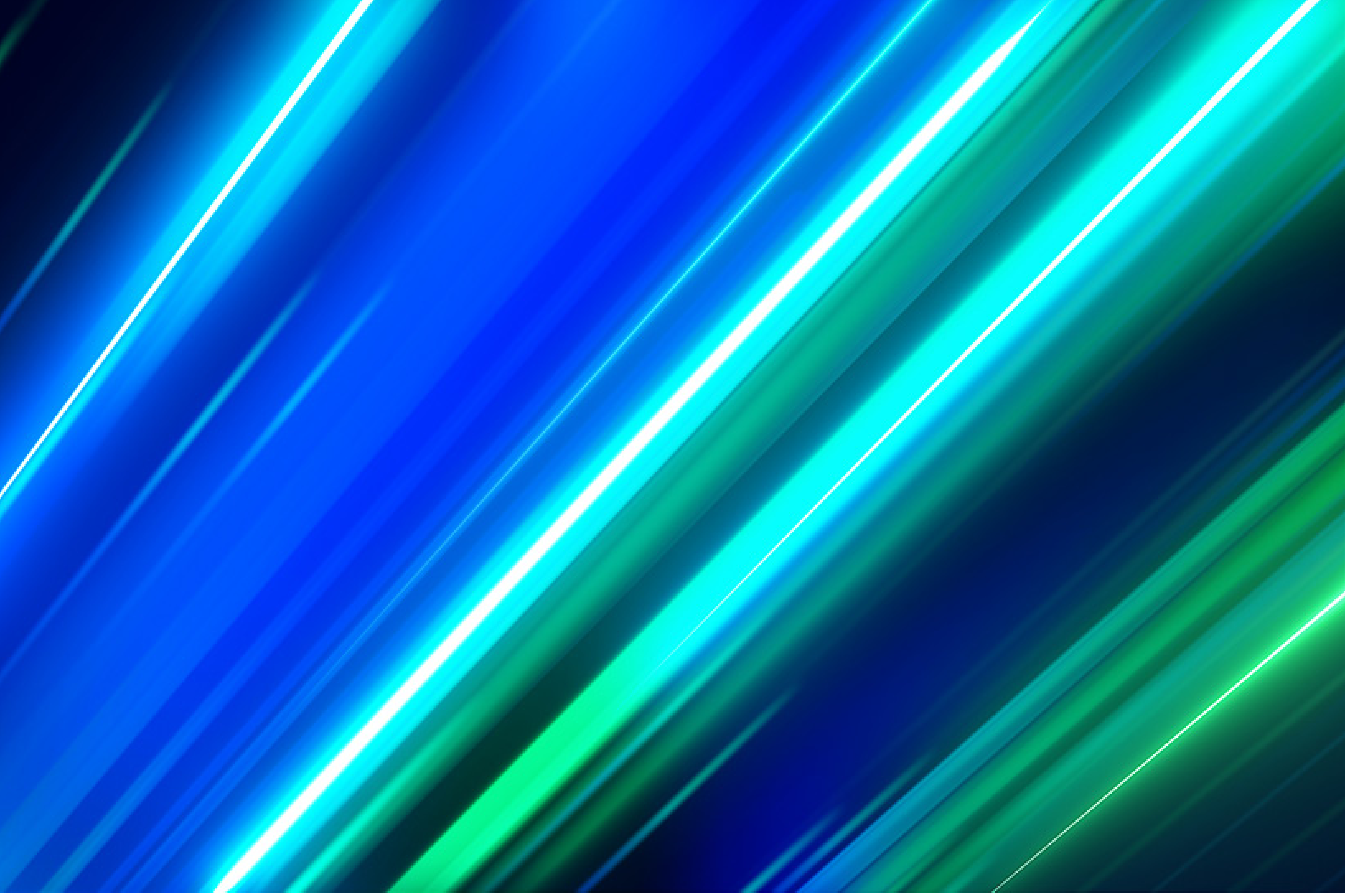
What level is your professional title?



What level is your professional title?



Source: Cognizant Response base: 71
Figure 14



Cognizant Security Practice

Cognizant Security helps you achieve better business outcomes by securing your digital transformation. We provide the security capabilities you need to address ever-changing threats, maintain compliance and reduce the unsustainable burden of managing security infrastructure.
To learn more visit our website, www.cognizant.com/security or feel free to contact us directly at cognizantsecurity@cognizant.com

About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient business-es. Headquartered in the U.S., Cognizant is ranked 193 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

Cognizant

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

Codex 4830.02