IDC Analyze the Future

IDC FutureScape

IDC FutureScape: Worldwide IT Security Products and Services 2016 Predictions

— APEJ Implications

Simon Piff

spiff@idc.com; AVP, Asia/Pacific Enterprise Infrastructure

November 2015

In This Study

IDC FutureScape

IT security is fast becoming a matter of national defense across the APEJ region. Governments are rapidly acknowledging that this is now a matter of national security and are rushing to set up cybercrime and cyber-defense centers with the associated levels of infrastructure and investment.
And yet business organizations are still struggling to balance the IT security cost with the impact it can potentially have on their business, and business owners are challenged by the issues of the elusive return on investment from IT security as compared to other types of IT investment.

This document offers IDC analysts' collective understanding of major industry transitions and advice to IT buyers to consider in their strategic planning in relation to IT security and services investment and operations.

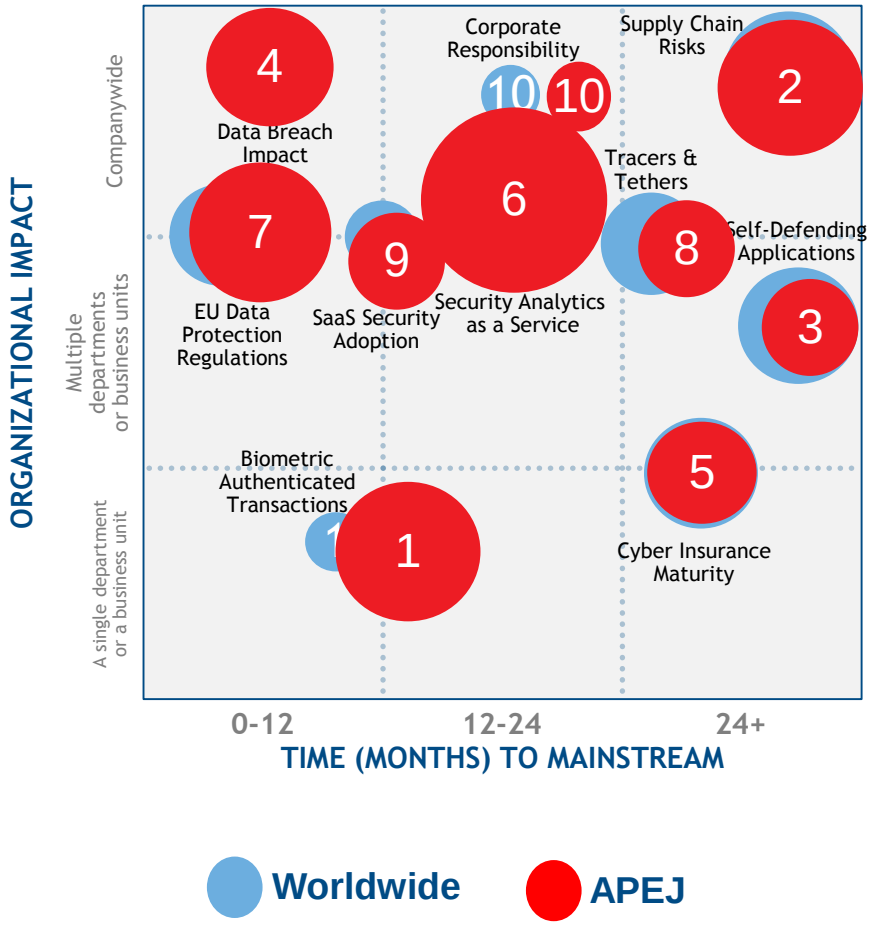
We advise decision makers to approach each prediction in three steps:

- **Assess its relevance:** Should I pay heed to this prediction? Does this prediction apply to me? Can I reasonably enough ignore it? What do I risk if I ignore it? Strategy is, after all, as much about what you decide to do as what you decide not to do.
- **Assess its urgency:** Does it apply to me now or in the future? If it applies in the future, when do I have to get started to deliver enabling capabilities as needed?
- **Assess its resource requirements:** What resources do I need and at what costs? What would I have to forego or postpone to achieve the capability? What do I have to speed up to achieve it? What priority does this prediction have relative to other projects consuming resources?

In the following slide, Figure 1 presents IDC's IT security top 10 predictions in terms of their likely impact across the enterprise and the time it will take for the predictions to reach mainstream. By mainstream, IDC means the broad middle of the bell curve of adoption (i.e., the 40–60% of enterprises that are neither the first movers and early adopters nor the last to act). Each bubble's size provides a rough indicator of the complexity and/or cost an enterprise will incur in acting on the prediction.

Worldwide 2016 IT Security Predictions

APEJ Implications



- Source: IDC, 2015

1. By 2020, half of all AP electronic transactions will be authenticated biometrically, driven by the widespread adoption and use of biometric-enabled mobile devices.
2. By 2019, geopolitical divisions and global economic instability will result in cyberattacks targeting suppliers, forcing businesses in AP to increase spending by 35% or more to mitigate supply chain risks.
3. By 2019, the adoption of application containerization for 3rd Platform applications in private, public, and hybrid cloud scenarios will rise more than 30%, creating an era of self-defending applications.
4. By 2020, more than 1.5 billion people will be affected by data breaches, increasing calls for regulation and alternative authentication measures.
5. By 2019, the insurance industry will gain the ability to influence security spending in three quarters of all IT security buying decisions in regulated industry verticals due to their maturing cyber insurance models.
6. By 2017, the security services market will increase by at least 30% due to the scarcity and high price of available data scientists, leading sub Fortune 100 companies to seek alternatives.
7. By 2019, 20% of security spending will be driven by EU data protection regulation and privacy concerns. Jurisdiction issues among trading regions will not be resolved, leading to a patchwork of compliance regimes.
8. By 2018, 2nd Platform perimeter defenses will be surpassed by 3rd Platform-architected, meshed security systems based on a tracers and tethers architecture, creating symbiotic security defenses.
9. By 2020, more than half of Web security market revenue will come from cloud-based offerings over traditional on-premises gateways.
10. By 2017, one-third of corporate boards will fill a seat with a risk mitigation expert who can provide guidance on data privacy and security initiatives.

APEJ in a Glance

IDC FutureScape

IT security is fast becoming a matter of national defense across the APEJ region. Governments are rapidly acknowledging that this is now a matter of national security and are rushing to set up cybercrime and cyber-defense centers with the associated levels of infrastructure and investment. And yet business organizations are still struggling to balance the IT security cost with the impact it can potentially have on their business, and business owners are challenged by the issues of the elusive return on investment from IT security as compared to other types of IT investment.

Australia — long seen as the most developed market in the APEJ region.

- Australia spends more on IT security than any other market — including China, for software products — although Beijing did surpass Canberra for security services spending in 2014.
- Australia invests heavily in the security software space as a percentage of overall software investment, second only to South Korea.
- The country suffered multiple high-profile computer attacks in 2015, including leading retailers David Jones and Patagonia.
- Ransomware also hit the Australia market particularly hard in 2015, creating a lot more awareness of the risk of global cybercrime in the public at large.
- The changing political and economic landscape makes Australia a target-rich market for highly focused hackers, be it commercial- or consumer-based.

Source: IDC Asia/Pacific Team, 2015

APEJ in a Glance (cont.)

IDC FutureScape

South Korea invest the most in security software as a percentage of overall software investments. The country has long been a market highly focused on IT security due to its ongoing disputes with North Korea.

- Ironically, South Korea has been identified as one of the three leading countries where botnet activity for launching distributed denial-of-service (DDoS) attack is highest (behind the U.S. and China).

India is third from the bottom of the list of countries investing in security software as a percentage of overall software investment (ahead only of the Philippines and Indonesia) in spite of major government scares over recent years.

- Security services, however, are strong in the India market.
- Hacking reports are mostly about government and military establishments being breached by supposed nation-state.
- While cybercrime is on the rise, most thefts appear to arise from more traditional scams brought about by social media.

ASEAN as a group does not heavily invest in IT security software and is below the APEJ average, in large part pulled down by Indonesia and the Philippines.

- Vietnam currently has the largest investments in IT security software and is the only ASEAN country that invests above the APEJ average but marginal in the services markets.

Source: IDC Asia/Pacific Team, 2015

APEJ in a Glance (cont.)

IDC FutureScape

China is something of a conundrum with regard to IT security.

- Many organizations believe they are protected by the Great Firewall of China against external attacks.
- Software investments in this market are marred by the omnipresence of piracy.
- China is frequently cited as a source of many cyberattacks.
- The Internet economy of China, as evidenced by Alibaba's US$14.3-billion gross merchandise value in one day, is fast becoming a significant contributor to the country's overall GDP, and therefore, an industry that will require more protection.

The potential for China to become a major opportunity for IT security markets is marred by the ongoing trade disputes with the U.S. that is pushing U.S. technology out of China government operations. Nowhere will this be more significant than in the sensitive area of security.

Overall, the APEJ region has a mix of developed and developing markets when it comes to IT security. Some markets offer robust legal frameworks that do drive aspect of the IT security markets, but there is a growing awareness that compliance does not equate to security.

Future threats will continue to rise, and it is only a matter of time before news reports of major breaches of Asian companies appear, at which time IDC expects the markets to respond in a more positive manner than what it is currently doing.

Source: IDC Asia/Pacific Team, 2015

Prediction #1: Biometric Authenticated Transactions

IDC FutureScape

By 2020, half of all AP electronic transactions will be authenticated biometrically, driven by the widespread adoption and use of biometric-enabled mobile devices.

Biometrically driven authentication methods are available to validate the authenticity of an individual for a variety of personal transactions and services. The most visible form of the biometric authentication method is associated with fingerprint readers on mobile devices, which may be used to get access to the device or specific applications or to validate a purchase. IDC forecasts proximity payments to increase significantly, with the five-year compound annual growth rate for proximity mobile payments expected to reach 85.9% by 2020.

This percentage is higher than the WW rate due to the prolific use of smartphones in the region — notably in China, India, and South Korea, where smartphone technologies and mobile payments are already emerging as accepted components of the infrastructure. Combine this reality with the fact that the scale of providing other multifactor authentication hardware to Asian population would be fiscally prohibitive, and we begin to see why mobile-based biometrics is more economically viable.

Prediction #1: Biometric Authenticated Transactions

IDC FutureScape

By 2020, half of all AP electronic transactions will be authenticated biometrically, driven by the widespread adoption and use of biometric-enabled mobile devices.

IT impact

- Using fingerprint readers as a secondary authentication method results in risk reduction.
- Security use cases for biometrics are expanding with a number of biometric methods. Call centers can use voice recognition to detect fraudulent callers, and facial recognition has been used to document participants at large gatherings.
- Competitive markets require IT leadership to support emerging authentication or potentially get blamed for causing customer churn.

BU impact

- Potential improvements in consumer experience can become a competitive differentiator for early adopters while being fully cognizant of the associated risks.
- Banks, billers, payment providers, and merchants must factor in support for mobile payments as part of strategic planning due to the rising customer demand. A thorough analysis of customer buying trends may help avoid alienating customers while integrating biometrics support for customers using a digital wallet and mobile applications.

Prediction #1: Biometric Authenticated Transactions

IDC FutureScape

By 2020, half of all AP electronic transactions will be authenticated biometrically, driven by the widespread adoption and use of biometric-enabled mobile devices.

Essential guidance for tech buyers	• CIOs should be aware of the intrinsic value mobile-based biometrics can offer to deliver a range of new services for both end customers as well as internal customers, and accordingly advise business units on the opportunities and challenges. • It is important to be aware of the technology and its limitations early enough to advise the business units that are probably already looking into this solution.
Essential guidance for IT suppliers	• Robust technologies will be required to support the level of risk implied by the use of such technologies for financial transactions. • Scale will be critical for the APEJ markets, where customers in key markets can easily number in millions. • The pricing of such technology may also be a challenge for traditional enterprise-based security offerings since the technology is enterprise-owned but consumer-facing. • Existing competition is in hardware-based 2FA, which is not frequently widely adopted due to its financial impact.

Prediction #2: Supply Chain Risks

IDC FutureScape

By 2019, geopolitical divisions and global economic instability will result in cyberattacks targeting suppliers, forcing businesses in AP to increase spending by 35% or more to mitigate supply chain risks.

Increasing uncertainty over economies globally could increase physical risk to supply chains, but for the first time, the cost and expertise needed to support a cyberattack is low enough for dangerous attacks that disrupt or bring down support systems. These attacks could be nation-state driven, targeted at the economy of a foe or hacktivist in nature, and aimed at damaging the reputation of a major corporation. Attacks of this nature would likely be high profile and would prompt organizations to assess their supply chain support systems and invest in additional security measures where risks are considered the highest.

In AP, the rise in number of component manufacturers, driven by initiatives such as the TPP, makes many markets in the region "target-rich environments." Combined with the low levels of IT security investment, the connectivity between IT and OT in the manufacturing space, the potential for this to be significantly more of a challenge in AP is substantially high.

Prediction #2: Supply Chain Risks

IDC FutureScape

By 2019, geopolitical divisions and global economic instability will result in cyberattacks targeting suppliers, forcing businesses in AP to increase spending by 35% or more to mitigate supply chain risks.

IT impact

- Taking no preventative action could result in a disruption of business operations.
- Supply chain management platform makers can expand functionalities to add security risk.
- Understanding the risk posed by business partners will require business, legal, and IT security leadership.
- The highly vulnerable will be those that have not secured the IT/OT connectivity sufficiently.

BU impact

- Organizations that rely on overseas manufacturers and suppliers will need to consider the security posture of their business partners.
- IT security assurance may emerge as a competitive differentiator for AP-based manufacturers when bidding for new international contracts.
- Increases in IT security budgets may need to be considered and that, in turn, can impact the cost of finished goods. But if well-managed in terms of the overall quality offering, the increases in IT security budgets may not necessarily impact profitability.

Prediction #2: Supply Chain Risks

IDC FutureScape

By 2019, geopolitical divisions and global economic instability will result in cyberattacks targeting suppliers, forcing businesses in AP to increase spending by 35% or more to mitigate supply chain risks.

Essential guidance for tech buyers	• Recent malware has been focused on the manufacturing sector in AP, which has given rise to an increased awareness in IT security. However, this new threat is more about service disruption — something that needs an ongoing review process to be instigated. • Clear views into the IT/OT connections and ensuring the establishment of a risk-based process for connectivity will emerge as an important part of this process. • Business Continuity and Disaster Response planning will be critical to ensuring zero disruption.
Essential guidance for IT suppliers	• IT providers should partner with OT providers to create an IT/OT security ecosystem that provides BCDR capabilities in the event of a disruptive attack. • OT providers need to consider this new disruptive security threat and start to reconsider how open connectivity and security co-exist. • Opportunities will arise in the supply chain of key customers; partner more deeply to reap recommendation rewards.

IDC Analyze the Future

Prediction #3: Self-Defending Applications

By 2019, the adoption of application containerization for 3rd Platform applications in private, public, and hybrid cloud scenarios will rise more than 30%, creating an era of self-defending applications.

It is still an early innovation but application container technology is quickly gaining adoption for its ability to reduce the compute necessary to run applications and its flexibility to run in cloud environments. While these microservice architectures support rapid delivery and some security benefits, future innovation could enable organizations to encapsulate and inject features and policies to enable applications to respond to threats.

In AP, the adoption rate for containers is somewhat slower than the global average, but the rate of adoption will increase at a higher velocity as non-AP businesses start to reap the rewards and share the benefits publicly. However, with the overall IT security readiness at relatively low levels, the embedded security approach will likely only materialize after a number of attacks reveal issues in the architecture locally.

Prediction #3: Self-Defending Applications

IDC FutureScape

By 2019, the adoption of application containerization for 3rd Platform applications in private, public, and hybrid cloud scenarios will rise more than 30%, creating an era of self-defending applications.

IT impact

- Microservice architectures change the security model from the development of modern applications to their deployment and maintenance.
- Application container technology is gaining adoption for its ability to reduce the compute necessary to run applications and its flexibility to run in cloud environments. These microservice architectures support rapid delivery, and some security benefits are immediately recognized by this approach.
- Future innovation could enable organizations to encapsulate and inject features and policies to enable applications to respond to threats.

BU impact

- In the rush to containerize, security may be left out of the business conversation.
- Being able to create secure apps that could be easily moved across cloud environments is a compelling business due to the potential to constantly manage operational expenses.
- The danger is that multiple apps can create management confusion, and so a DevOps approach from IT should help keep the business on track with their business needs versus technical proliferation.

Prediction #3: Self-Defending Applications

IDC FutureScape

By 2019, the adoption of application containerization for 3rd Platform applications in private, public, and hybrid cloud scenarios will rise more than 30%, creating an era of self-defending applications.

Essential guidance for tech buyers	• Begin laying the groundwork to evaluate the technology in nonproduction environments. • Identify the impact of the technology on application development processes when creating modern applications associated with container technology. • Assess the use and management of virtualization in the environment and consider the business and security benefits of microservice architectures.
Essential guidance for IT suppliers	• Both skills and knowledge in the containerization technology area will be scarce for a significant period of time. The opportunity is there for a vendor to grab the mindshare, but skills will be critical to capturing revenues in this market. • For many organizations in APEJ, there are multiple hurdles to overcome to move into this arena: the move to DevOps, the acceptance of cloud, and the ability to work in a containerized environment. The challenge is not insignificant, but early adopters will emerge to drive this market.

Prediction #4: Data Breach Impact

IDC FutureScape

By 2020, more than 1.5 billion people will be affected by data breaches, increasing calls for regulation and alternative authentication measures

Despite increased spending associated with security program initiatives, the sustained line of data breaches continues, impacting a greater number of people. By calculating the number of lost records and other factors, IDC has projected the impact to reach 1.5 billion people. This number takes into account the significant increase in sensitive data about individuals from blogs, forums, and other publicly available sources that help criminals craft convincing social engineering campaigns. Data breach investigations also shed light on the continued failure of organizations to maintain adequate security controls and the ability of attackers to bypass some of the most effective security products available in the market. Emerging solutions show progress in detecting custom malware and other modern threats, but it will take considerable amount of time before novel technologies with the most efficacy are uncovered. Until then, data breaches will continue to grab headlines.

This equates to one in four people, and APEJ is not immune. As millennials realize the impact of personal data theft, the outcry from them will grow, forcing governments and businesses to respond more proactively than what they are currently doing.

Prediction #4: Data Breach Impact

IDC FutureScape

By 2020, more than 1.5 billion people will be affected by data breaches, increasing calls for regulation and alternative authentication measures.

IT impact

- Inactivity to consumer demands for tighter data protection (DP) and privacy controls could result in escalating customer churn, legal costs, and the introduction and enforcement of more regulatory fines in local markets.
- IT organizations risk failing to adapt their security programs to the new paradigm brought on by the 3rd Platform of IT corporate innovation.
- An increasing number of threats is designed to evade signature-based detection, giving attackers an easy way to gain initial access to the corporate network.

BU impact

- Public data losses have the potential to not only impact organizations but individuals' careers too. In AP, where many organizations are also family-owned, there are other "reputational" issues at stake.
- Businesses that do not take steps to secure personal customer data may well be shunned by customers and experience higher churn and lower customer acquisitions as a result.
- The costs of data loss fines are currently not high, but this is likely to change as the number and scale grow across the region.

Prediction #4: Data Breach Impact

IDC FutureScape

By 2020, more than 1.5 billion people will be affected by data breaches, increasing calls for regulation and alternative authentication measures.

Essential guidance for tech buyers

- Conduct a thorough assessment of the security program and include a careful examination of all deployed security infrastructure.
- Identify the location and classify sensitive corporate assets.
- Specifically identify customer data that has personal identifiable information and ensure it is suitable protected and monitored.
- Evaluate specialized threat analysis and protection products and determine their ability to integrate with existing security investments.

Essential guidance for IT suppliers

- Increasing headlines will continue to spur the C-Suite to want to invest into IT security products, but frustration around defining the ROI for some scenarios will continue.
- Work closely with the IT security lead in the customer to help them clearly articulate the value and consequences of a poorly executed IT security strategy.
- Discussion around "risk-based decision-making" is only useful if the IT security lead is sufficiently educated on this process internally.

Prediction #5: Cyber Insurance Maturity

IDC FutureScape

By 2019, maturing cyber insurance models will enable insurers to influence security spending in three quarters of industry-regulated buying decisions.

Cyber insurance, which has existed in various forms since the 1990s, has been stymied by inadequate data to feed risk models. A lack of data about the nature and cause of data breaches and an inadequate account of security protections and procedures in place at the time of a successful attack have made data collection even more challenging. But the knowledge base about attacker tools and tactics, software vulnerabilities and configuration weaknesses, and adequate ways to reduce an organization's attack surface has raised insurers' ability to accept more risk and increase their underwriting of insurance premiums. This in turn should yield a great deal of additional metrics to feed risk models and ultimately increase insurer influence over buying decisions in some markets.

This global model will be challenging for many AP organizations that are neither compelled to disclose any such attacks legally nor will want to for fear of bad publicity. The resulting effect is that cyber insurance will likely be more expensive for AP organizations — if, indeed, they adopt this tool — unless a more open relationship with the insurance company is maintained.

Prediction #5: Cyber Insurance Maturity

IDC FutureScape

By 2019, maturing cyber insurance models will enable insurers to influence security spending in three quarters of industry-regulated buying decisions.

IT impact

- Insurer influence on buying decisions could drive businesses to adopt a compliance-driven security spending strategy, which ensures minimal safeguards but could potentially fail to incentivize organizations to deploy security controls that are not prescribed.
- Insurer influence on buying decisions outside of retail, healthcare, and other regulated industry verticals could result in significant security improvements at some organizations.
- Insurer influence may have a negative impact on security technology innovation by prompting security vendors to build technology that meets insurer requirements.

BU impact

- For many enterprises, cyber insurance will not make it on the radar until after a costly attack occurs, and in non-regulated industries and geographies, even then there will be resistance from business owners.
- There will however be many locally sourced products in the markets as local insurers see an opportunity, and in markets such as China and South Korea, where there is a wealth of local IT security vendors, many relationships may mirror what happens on a global basis.

Prediction #5: Cyber Insurance Maturity

IDC FutureScape

By 2019, maturing cyber insurance models will enable insurers to influence security spending in three quarters of industry-regulated buying decisions.

Essential guidance for tech buyers

- Adopt a risk-based decision-making methodology rather than a compliance-driven one.
- Divert resources to projects designed to increase situational awareness about the organization's security posture.
- Develop ways to measure the effectiveness of existing security investments rather than relying on a snapshot-in-time compliance audit.

Essential guidance for IT suppliers

- In spite of the challenges, IT vendors do need to reach out to insurance companies and explore these relationships in local markets.
- Due to the varying nature of cyber laws and data regulation across the region, this will be a very challenging process for highly centralized vendors looking to create a homogenous strategy for APEJ.
- The most nimble and creative IT security vendors are likely to be better able to partner with locally managed insurance companies.

Prediction #6: Data Security Analytics Windfall

By 2017, the security services market will increase by at least 30% due to the scarcity and high price of available data scientists, leading sub Fortune 100 companies to seek alternatives

Big Data projects, which serve business intelligence benefits, are set to support initiatives to gather contextual threat intelligence by incorporating security analytics engines. The approach will bring organizations a step closer to being able to predict high-risk individuals or complex business systems that could be the most likely chosen pathway of an attack. It may extend the viability of existing legacy security information event management platforms and give incident responders the ability to rapidly respond to potential threats, implement automated response measures, or address high-risk weaknesses before an attacker attempts to exploit them.

The AP challenge is that such skills will be scarce for many years to come, and data science is more likely to be applied to income-based projects rather than security analytics, as such it is more likely to spawn an industry of security-analytics-as-a-service.

Data nationalism, regulations, and the nature of the industry will further make this an in-country-only proposition as legislation and security fears bar the data from going beyond national boundaries.

Prediction #6: Data Security Analytics Windfall

IDC FutureScape

By 2017, the security services market will increase by at least 30% due to the scarcity and high price of available data scientists, leading sub Fortune 100 companies to seek alternatives.

IT impact

- Security analytics deployments could suffer serious setbacks without trained data analysts maintaining them.
- Reliance on outside expertise to manage visibility into business activities and other collected data could result in an increased risk of data exposure.
- Internal data scientists with knowledge about business operations and industry vertical trends and security issues are in better position to direct analysis engines to find the needle in the haystack.

BU impact

- Business will be challenged to find data scientists in the AP markets for a number of years, and when they do find, they will not necessarily want to apply them to security.
- The lack of insight available will be countered by a growing executive demand for deeper insight.
- At the heart of the matter will be a need to focus on internal IT only on technology that delivers competitive differentiation, resulting in the outsourcing or cloudifying of a range of services including security data analytics.

IDC Analyze the Future

Prediction #6: Data Security Analytics Windfall

IDC FutureScape

By 2017, the security services market will increase by at least 30% due to the scarcity and high price of available data scientists, leading sub Fortune 100 companies to seek alternatives

Essential guidance for tech buyers	• Establish a recruitment and retention program for data analysts in order to inculcate a data-first business mentality. • Consider data security analytics offerings that can be adopted through a SaaS subscription model. • Choose security analytics platforms that contain business analysis and visualization tools so business analysts can grow into the data scientists of tomorrow.
Essential guidance for IT suppliers	• ISV's need to ensure that there is an opportunity for channel partners to deliver their offerings as-a-service and create business models that support this. • The channel partner ecosystem needs to be educated to the opportunity, especially where in-country SI's with both the relationships and the potential capability are best placed to deliver this offering. • A realization that analytics, in general, is not widely adopted by local customers, and maturity levels are very low in the analytical market.

IDC Analyze the Future

Prediction #7: EU Data Protection Regulations

IDC FutureScape

By 2019, 20% of security spending will be driven by EU data protection regulation and privacy concerns. Jurisdiction issues among trading regions will not be resolved, leading to a patchwork of compliance regimes.

Jurisdictional data protection rules have long been a challenge for organizations, and the ongoing conflict of jurisdiction between the EU and the United States only serves to highlight how uncertain any restrictions are over processing data in the virtual world. The new EU DP law — the General Data Protection Regulation (GDPR), which is currently in discussion — contains an extraterritoriality clause that extends its reach to any firm processing EU citizen data, irrespective of physical presence.

Few AP organizations are ready for the potential impact of this legislation due to lack of awareness of denial. For enterprises not operating any part of their organizations in the EU, the impact is minimal, but those that do will need both their EU branch and other arms to comply, since fines can be a percentage of global revenue, potentially erasing the value of a small EU branch operation if the head office is found to be non-compliant.

Some may opt to not service EU citizens,but this would be a shortsighted approach.

Prediction #7: EU Data Protection Regulations

IDC FutureScape

By 2019, 20% of security spending will be driven by EU data protection regulation and privacy concerns. Jurisdiction issues among trading regions will not be resolved, leading to a patchwork of compliance regimes

IT impact

- Organizations lacking regional data protection strategies could lose their business or face fines.
- Costs associated with responding to new jurisdictional data protection rules could increase over time.
- Organizations that fail to address jurisdictional issues may be forced to separate the business to a third-party business partner, resulting in lower margins.

BU impact

- A lack of knowledge is never a good defense. Understanding what is needed and making a conscious decision about how to address this legislation is going to be critical.
- The potential for Asian governments to adopt similar legislation is probable, so an eye on what is happening in the local jurisdiction will be even more important.
- Organizations deeming themselves exempt to this, due to locale of current business operations, may be denying themselves future access to the EU markets should they publicly fall out of compliance.

Prediction #7: EU Data Protection Regulations

IDC FutureScape

By 2019, 20% of security spending will be driven by EU data protection regulation and privacy concerns. Jurisdiction issues among trading regions will not be resolved, leading to a patchwork of compliance regimes

Essential guidance for tech buyers	• Take a systematic approach to assessing the impact of newly proposed data protection rules to avoid making knee-jerk reactions to them. • Conduct a business analysis to identify potential low-cost solutions that meet the spirit of regional data protection regulations. • Assess the feasibility of separating or extending existing security solutions to meet locally established data sovereignty rules. • Be aware that an attempt to protect the data can limit or avoid any punitive action by the EU legislators.
Essential guidance for IT suppliers	• Data governance has been higher in some markets than others for years now, driven in large part by local legislation and enforcement. Be prepared for governments to take strong stands either in favor of or against this legislation and do not assume it will be broadly accepted. • Be clear that this is a data governance and management issue as much as it is a security issue, and that some technologies (encryption as an example) will be sufficient to satisfy the EU regulators. • This law is not yet finalized, so the first few months of 2016 will decide its fate. If accepted, there is a two-year period to achieve compliance — many businesses will be waiting until the last minute before committing to this.

Prediction #8: Tracers and Tethers

IDC FutureScape

By 2018, 2nd Platform perimeter defenses will be surpassed by 3rd Platform-architected, meshed security systems based on a tracers and tethers architecture, creating symbiotic security defenses.

IDC has identified an evolving security model that eschews defense in depth, layers, and perimeter security in favor of a 3rd Platform-architected, distributed model based on a hub-and-spokes architecture we call "tracers and tethers" (TnT). A TnT architecture consists of a strong centralized command and control environment connected to decentralized sensors and policy enforcement points (PEPs).

The APEJ markets will see some of the more advanced organizations and governments move to this architecture while the vast majority will still be slowly advancing on a defense-in-depth strategy — and entire revolution behind the current trend.

Prediction #8: Tracers and Tethers

IDC FutureScape

By 2018, 2nd Platform perimeter defenses will be surpassed by 3rd Platform-architected, meshed security systems based on a tracers and tethers architecture, creating symbiotic security defenses.

IT impact

- Adopting a hub-and-spokes architecture creates symbiotic security defenses that are capable of sharing threat indicators and updating policy based on risk determination.
- Organizations that are successful in building out a TnT architecture will have the opportunity to automate policy enforcement at the application level.
- Failing to adopt this strategy will result in the reliance on outdated perimeter defenses that fail to meet the security requirements driven by modern network architecture trends.

BU impact

- The failure to adopt this security strategy will limit the ability of business to safely deliver on 3rd Platform products and services, hampering future growth and competitive objectives.
- The potential to become a less challenging target for the hacking community will increase the likelihood of a fiscally punitive attack taking place.

Prediction #8: Tracers and Tethers

IDC FutureScape

By 2018, 2nd Platform perimeter defenses will be surpassed by 3rd Platform-architected, meshed security systems based on a tracers and tethers architecture, creating symbiotic security defenses.

Essential guidance for tech buyers

- Lay the foundation for a cohesive security architecture by identifying solutions that bridge siloed security systems.
- Evaluate modern security products that integrate with existing security investments.
- Analyze the technology partner ecosystem of potential technologies under consideration to determine established integration points.

Essential guidance for IT suppliers

- Integration with a broad range of complimentary and competing security products will be the key to future existence.
- Isolationist and protectionist product strategies and execution will limit access to the future markets.
- Start by identifying the ecosystem of collaborative partnerships that can fill out the broader IT security offerings, and bring the corresponding channel players together where and when they meet the customer.

Prediction #9: SaaS Security Adoption

IDC FutureScape

By 2020, more than half of Web security market revenue will come from cloud-based offerings over traditional on-premises gateways.

Security vendors continue to invest heavily in SaaS-enabling on-premises software and appliances. This activity is visible in the endpoint, messaging, and Web security markets and, at least, partially driven by customers that require security protection to extend to remote offices, mobile users, and some cloud-based resources. Adoption of SaaS-based Web security platforms is rising significantly. Platforms in this market are evolving from traditional, on-premises Web Security Gateways to hybrid and full SaaS-based offerings that typically require the installation of an agent or sensor on endpoint devices and a proxy to send network traffic into cloud-based inspection systems. Driving this adoption is rising demand from end users, requiring always-on access to corporate resources and an increase in smartphone and tablet use.

Prediction #9: SaaS Security Adoption

IDC FutureScape

By 2020, more than half of Web security market revenue will come from cloud-based offerings over traditional on-premises gateways.

IT impact

- Once all Web security vendors bring their SaaS-based offerings into parity with their on-premises gateways, the decision to migrate to a SaaS model may be driven by economics.
- The current hybrid approaches being adopted to address remote and mobile employees may be subsumed by a fully SaaS model connected to client software.
- Organizations rejecting SaaS Web security offerings for on-premise gateways could miss out on the vendor's ability to rapidly deploy protection and add new features and capabilities.

BU impact

- The ability to offload the work for this type of security offering should allow businesses to make better use of their internal IT staff, allowing the SaaS offering to automatically run necessary updates without internal resource intervention.
- Increased standardization and clear processes will need to be defined across mobile applications to ensure ongoing compatibility.

Prediction #9: SaaS Security Adoption

IDC FutureScape

By 2020, more than half of Web security market revenue will come from cloud-based offerings over traditional on-premises gateways.

Essential guidance for tech buyers	• Assess the value of modernizing the Web security gateway to take advantage of integration with modern threat detection offerings. • Assist all stakeholders in validating the effectiveness of the SaaS-based Web security platforms to gain a comfort level with the functionality and management capabilities. • Create a set of requirements and incorporate standard best practices for evaluating vendor SaaS security approaches.
Essential guidance for IT suppliers	• A SaaS first sales approach may not necessarily resonate with all customers in all markets in the APEJ region, but not having a SaaS offering will deny access and create a potentially negative impression. • Ensuring the channel is fully educated and suitably compensated in the SaaS model will be critical for APEJ success. • Transforming this channel from transactional to relational will be critical to the future success of the channel in the cloud/SaaS world.

Prediction #10: Corporate Responsibility

IDC FutureScape

By 2017, one-third of corporate boards will fill a seat with a risk mitigation expert who can provide guidance on data privacy and security initiatives.

The increasing complexity of national and international data governance legislation — complemented by announcements of new, high-profile attacks that cause personal, financial, or material damage to large organizations — will drive the need for corporate boards to be far better informed about the impact and consequences of potential data breaches.

While clearly visible within the multinational enterprise community, this will slowly emerge in the pan-Asian organizations and any enterprise that do significant business with either the U.S. or the E.U. out of necessity.

Prediction #10: Corporate Responsibility

IDC FutureScape

By 2017, one-third of corporate boards will fill a seat with a risk mitigation expert who can provide guidance on data privacy and security initiatives.

IT impact

- An individual with knowledge about cybersecurity issues could provide the champion needed to bolster the risk mitigation initiatives by the chief information security officer (CISO).
- The establishment of a board seat would mean that senior business executives will be held accountable for security incidents under their watch.
- A corporate board seat could foster a positive perception of the company, differentiating it from competitors.

BU impact

- Publicizing such a board role could offer valuable positive PR, assuming a significant data breach does not take place.
- The adoption of such a role will ensure that responsible data management becomes a design feature of new projects, and not a bolt-on-after-the-fact tactical issue.

Prediction #10: Corporate Responsibility

IDC FutureScape

By 2017, one-third of corporate boards will fill a seat with a risk mitigation expert who can provide guidance on data privacy and security initiatives.

Essential guidance for tech buyers

- Organizations should first name a CISO of the IT security organization.
- Evaluate a mixture of candidates who understand the business and have experience addressing data protection, privacy, and regulatory compliance issues.
- The CISO may need to directly report to the CEO as a direct line to understanding the security risks associated with business decisions.

Essential guidance for IT suppliers

- Organizations with such a role will have a far more structured approach to IT security and procurement — becoming a trusted adviser to such an individual could pay dividends or deny access to the customer if managed badly.
- Such a role is currently being defined, becoming a part of the process of role definition will result in significant advantages for the future.

Predictions at a Glance: APEJ Implications

IDC FutureScape

1. **Biometric Authenticated Transactions.** By 2020, half of all AP electronic transactions will be authenticated biometrically, driven by the widespread adoption and use of biometric-enabled mobile devices.
2. **Supply Chain Risks**. By 2019, geopolitical divisions and global economic instability will result in cyberattacks targeting suppliers, forcing businesses in AP to increase spending by 35% or more to mitigate supply chain risks.
3. **Self-Defending Applications.** By 2019, adoption of application containerization for 3rd Platform applications in private, public, and hybrid cloud scenarios will rise more than 30%, creating an era of self-defending applications.
4. **Data Breach Impact.** By 2020, more than 1.5 billion people will be affected by data breaches, increasing calls for regulation and alternative authentication measures.
5. **Cyber Insurance Maturity.** By 2019, maturing cyber insurance models will enable insurers to influence security spending in three quarters of industry-regulated buying decisions.
6. **Data Security Analytics Windfall.** By 2017, the security services market will increase by at least 30% due to the scarcity and high price of available data scientists, leading sub Fortune 100 companies to seek alternatives.
7. **EU Data Protections Regulations.** By 2019, 20% of security spending will be driven by EU data protection regulation and privacy concerns. Jurisdiction issues among trading regions will not be resolved, leading to a patchwork of compliance regimes.
8. **Tracers and Tethers.** By 2018, 2nd Platform perimeter defenses will be surpassed by 3rd Platform-architected, meshed security systems based on a tracers and tethers architecture, creating symbiotic security defenses.
9. **SaaS Security Adoption.** By 2020, more than half of Web security market revenue will come from cloud-based offerings over traditional on-premises gateways.
10. **Corporate Responsibility.** By 2017, one-third of corporate boards will fill a seat with a risk mitigation expert who can provide guidance on data privacy and security initiatives.

About IDC

IDC FutureScape

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Asia/Pacific Headquarters (Singapore)

80 Anson Road, #38-00
Singapore 079907
65.6226.0330
Twitter: @IDC
idc-insights-community.com
www.idc.com