2017 Trends to Watch: Security

2017 is the year next-generation security providers need to step up to the plate
Summary

Catalyst

In 2017 the IT security market will continue to evolve to meet a new and ever-changing range of cybersecurity threats. In this context, IT security will increasingly be referred to generically as cybersecurity. This reflects the fact that more and more business is conducted online, more individuals and companies collaborate over networks, more data is held in the cloud, and more consumers interact almost exclusively with product and service providers on screens rather than face-to-face.

Meanwhile, the market for cybersecurity products is booming, as evidenced by its size in dollars, the amount of VC funding for start-ups, and the success of initial public offerings in this space. The market for security products and services is also changing, however, with increasing amounts of security functionality being delivered as a service from the cloud.

Ovum view

2017 is the year Ovum expects next-generation security providers to step up to the plate. The time is right, and the requirement for better and more inclusive security facilities and services already exists. All that is needed is the ability to deliver.

The security intelligence community, with the vast amount of threat data it has available, claims to be able to identify and deal with cyber threats at the earliest opportunity. User entity behavior analytics (UEBA) and endpoint detection and response (EDR) suppliers make similar claims in their own areas of expertise. Nevertheless, IT decision-makers need to see measurable proof that newer forms of cybersecurity protection are making a real difference. Only then should they think about winding down the use of older, often signature-based, protection tools.

Key messages

- Security intelligence must deliver on its promise to protect critical business systems and infrastructure.
- Next-generation protection systems need to safeguard an organization's reputation and trust.
- Identity underpins all business relationships and the delivery of services on all types of platform.
- Cyber threats must not be allowed to interrupt the adoption of digital services.

Recommendations

Recommendations for enterprises

Hold “next-gen” and “old school” vendors alike to account

If you are operating traditional signatures-based security products in your environment and are noting a decrease in their ability to protect your infrastructure, quiz some of the so-called next-generation security vendors about how they can improve your security posture. Then go back to your supplier of
traditional technology and find out what its plans are to bolster its offering with next-gen capabilities. Depending on the timeframe, it might well be preferable to increment what you have today rather than deploy a separate next-gen silo. And definitely do not rip and replace any signatures-based technology you have.

**If vendors offer threat intelligence, ask them about making it actionable**

Many companies are offering threat intelligence, but before making a decision, ask them how you will be able to use the data provided in your environment. Will it automatically feed into you SIEM? Can your security analysts receive it in a format that will enable them to take immediate action? Will they prioritize the threats they are seeing with specific reference to your infrastructure/vertical market/geography?

**Recommendations for vendors**

**Consider your users when designing security intelligence solutions**

Most security vendors have sources of security and threat data readily available. Passing this data on and turning it into relevant security intelligence that client organizations can immediately access and use still seems to be a stage too far for many. Consider your users and the resources they have available to deal with threat information. Targeted, actionable security intelligence is what they are looking for and is what needs to be delivered.

**Identity management must support the needs of all user groups**

Identity management may have started out as an enterprise tool to manage business to employee (B2E) relationships, but the requirement now extends to controlling business and consumer relationships in all their different forms. Current and future requirements for IoT and identity as a service (IDaaS) are extending the role of identity management further, and vendors need to ensure that their service delivery strategies can meet the needs of all potential clients and user groups.

**Business trends and technology enablers**

**Security needs to operate at the heart of all business systems**

**Monitor the business environment**

Cybersecurity protection systems are needed to allow business systems to operate safely. What CISOs are looking for from their technology providers are facilities that keep users and their devices safe and free from infection, and at the same time, control and facilitate access to new and ever more open business systems. To achieve these objectives, a balanced and inclusive security strategy is needed.

**Create the technology portfolio**

Building a balanced and inclusive security protection portfolio that can keep business systems and users safe is a worthy objective. The fragmented nature of the security market doesn't help. However, leading security vendors are extending their coverage and partnership arrangements, and there are further opportunities to work with managed security service providers (MSSPs). There are greater prospects of working with security providers that have a portfolio of products and services that can fulfill enterprise requirements.
Select solutions and services

The deliverable components of a cybersecurity strategy need to fit business requirements and have the capacity to support existing and future operational strategies. Access to systems and the data they hold is likely to involve a hybrid mix of on-premise and cloud-based systems and services. When selecting a security technology supplier or service provider, organizations must therefore decide on a strategy that meets their risk profile, their regulatory compliance commitments, and their security budget.

Manage deployment outcomes

Once technology partners and appropriate security approaches (direct, managed, outsourced, and so on) have been decided on, delivery of service and levels of protection need to be maintained in order to preserve successful outcomes. Levels of security performance need to be measurable and provable for IT security management, security audit, regulatory compliance, and senior management purposes.

Security intelligence must deliver on its promise to protect critical business systems and infrastructure

Threat intel should deliver relevance as well as information

The efficacy of signature-based approaches such as anti-virus (AV) software and intrusion detection and prevention systems (IDS/IPS) is waning, so to remain safe, companies are increasingly feeling the need to have as much information as possible about all the threats currently active around the Internet, in order to craft appropriate responses.

Threat feeds, as this information is known, have been around for a number of years, but the cybersecurity industry has recently begun to talk about the need to offer more in the form of threat intelligence. With threat feeds covering every type of new vulnerability and every exploit happening anywhere in the world, there is just too much information in them to be of any real use to customers. Instead, the argument goes, a threat intelligence service should sift out the "noise", enabling the customer to focus on identifying the most pressing concerns and immediate threats faced in their vertical market and geography, bearing in mind the specific systems used within their infrastructure.

Targeted and prioritized information is needed

Security intelligence-gathering tools and the threat feeds that source their information resources are already collecting and collating billions of pieces of threat data. This approach is necessary to ensure nothing is missed, but at the same time, the information presented to security analysts needs to have a better and more targeted focus.

Security management resources are finite. Valuable analyst time cannot be wasted chasing down false-positive threat reports and items that may be of interest but not of sufficient relevance to warrant detailed investigation. Threat Information needs to be prioritized so that security experts are working with the threats that put the organization at the greatest risk. This needs to be supported by levels of granular threat content that target the right actions and remediation responses.
In the year ahead, client and vendor security discussions should focus on the prioritization of threat protection that is relevant to the business, its operations, and its assets.

**Next-generation protection systems need to safeguard an organization’s reputation and trust**

**The threat landscape is changing**

The threat landscape is constantly evolving, requiring new and different responses from the defenders within enterprises. The efficacy of signature-based approaches, such as anti-virus (AV) software and intrusion detection and prevention systems (IDS/IPS), continues to wane, with the result that security professionals must now look for the “unknown unknowns”, detecting threats for which there is no signature, purely on the basis of their behavior.

Network-based sandboxing, which provides a safe environment in which to “detonate” suspect code to see how it acts, enjoyed considerable popularity earlier this decade. However, in the last couple of years, malware writers have developed methods for their code to discover that it is in a sandbox and therefore evade detection.

An approach that is now taking off is user and entity behavioral analytics (UEBA), which uses machine learning to determine what constitutes normal behavior for employees and their work devices, as well as other corporate assets such as servers, then compares current activity with this norm to detect and flag anomalies. Many would argue that in this area of data protection, data loss prevention (DLP) technology has an important role to play. DLP may not as yet have fulfilled its potential, but used in monitoring and protection mode, as required here, it provides a good approach for helping organizations stay in control. When used alongside a well-thought-out UEBA and data encryption strategy, DLP has the potential to keep business operations safe.

The longest-standing perimeter defense for enterprise networks, the firewall, is also now required to address new, application-layer (Layer 7) threats, instead of focusing exclusively on the data, network, and transport layers (Layer 2-4). The stateful firewalls of yesteryear are therefore being replaced with so-called next-generation firewalls (NGFW) with application awareness, while corporate applications that reside entirely on the company’s website are protected by a dedicated web application firewall (WAF).

Another tech development requiring a response from the security sector is the evolution of application programming interfaces (APIs), which are increasingly used in websites to enable one application to interact directly with another, such as, for instance, to enable a payment card to be used on an e-tailer’s site, or to provide geographical information to someone looking for a store or restaurant.

With hackers harnessing bot technology to mount attacks on websites, the API is clearly an appealing vector. Hackers can pose as a legitimate price-comparison bot harvesting price information, when in fact they are planting a Trojan for subsequent use in attacking the site’s owner, for instance.

These developments require an API security layer in front of the website to identify what is trying to interact with its APIs and determine whether to allow it. This technology can even decide whether to slow down a bot, in the case where it is a “grey” (as opposed to a “black”) bot, which should not be allowed to worsen legitimate customers’ user experience, even though it is not malicious. These
capabilities are now starting to be provided by API management platform vendors such as Apigee and Mulesoft, as well as other types of company such as Distil and Akamai.

The corporate workplace is now anywhere on any device

At the same time, the corporate workplace is undergoing significant change, with more and more employees working remotely, often accessing applications that reside in public, private, and hybrid cloud environments. All of this represents new challenges for IT security. Corporate endpoints spend more time off the company network, and have been joined by bring-your-own-device (BYOD) smartphones and laptops as a target for cyberattacks.

This has led to the emergence of a new class of security product called endpoint detection and response (EDR). EDR places agents on endpoints to analyze all the applications on them, sending information to a back-end server in the cloud where their behavior is categorized, enabling the system to detect and flag anomalous activity.

Informed by the approaches of UEBA on the network and EDR on endpoints, a further group of products known as next-generation endpoint protection (NGEP) has recently emerged. These products are in some senses a superset of EDR and traditional AV in that they still rely on signatures for the 30% to 35% of threats that can be blocked using them, then bring to bear the anomaly detection and machine learning aspects of EDR to look at everything that has made it through the AV.

Cloud usage now requires policing

The availability of cloud-based applications, such as in the area of collaboration and data storage, has created a further challenge for corporate IT departments, in that employees can simply decide to use services such as Dropbox or Evernote without notifying anyone else in their company.

The potential for intellectual property or other sensitive data to find its way outside the company via these software-as-a-service (SaaS) applications is huge. Therefore, alongside the network and endpoint security systems, a new class of product is now emerging to enable corporate IT departments to regain visibility over what SaaS applications are in use.

A number of these products, known as cloud access security brokers (CASBs), also enable companies to enforce policy for these apps. For instance, certain types of document should not be exported to the cloud at all, while others require some form of obfuscation such as encryption or tokenization, and still others may be read-only, so that anyone else looking at them cannot copy them or print them off. Beyond providing visibility into the “shadow” IT created by users doing their own thing without the IT department’s knowledge, these CASBs can therefore also enable control over “sanctioned” IT, the SaaS applications that the IT department approves of but still needs to control interactions with.

Some CASBs are even more ambitious, offering the potential to track employees’ use not only of SaaS apps, but also of infrastructure- and platform-as-service (IaaS and PaaS). The recent acquisition by Oracle of one such vendor, Palerra, to complement its newly launched identity-as-a-service (IDaaS) offering called Identity Cloud Service, raises the question of whether CASB can sustain itself as a standalone market.

It is Ovum’s view that more CASB functionality will ultimately be bundled into other platforms/services, and the M&A activity that has already taken place in this market (Cisco, Microsoft, Imperva, Blue Coat, Digital Guardian, and now Oracle have all bought CASB developers) appears to vindicate this
belief. IBM did not buy a CASB, but instead developed its own CASB functionality and bundled it with its IAM technology in an appliance. As we move into 2017 and beyond, identity management platforms look like a natural home for CASB functionality.

### Figure 1: CASB acquisitions in the last two years

<table>
<thead>
<tr>
<th>CASB vendor</th>
<th>Bought by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skyfence</td>
<td>Imperva</td>
<td>February 2014</td>
</tr>
<tr>
<td>Armor5</td>
<td>Digital Guardian</td>
<td>October 2014</td>
</tr>
<tr>
<td>Perspecsys</td>
<td>Blue Coat</td>
<td>July 2015</td>
</tr>
<tr>
<td>Adallom</td>
<td>Microsoft</td>
<td>September 2015</td>
</tr>
<tr>
<td>Elastica</td>
<td>Blue Coat</td>
<td>November 2015</td>
</tr>
<tr>
<td>CloudLock</td>
<td>Cisco</td>
<td>June 2016</td>
</tr>
<tr>
<td>Palerra</td>
<td>Oracle</td>
<td>September 2016</td>
</tr>
</tbody>
</table>

Source: Ovum

Identity underpins all business relationships and the delivery of services on all types of platform

**B2E, B2B, and B2C are all requirements**

Identity and access management (IAM) platforms started out enabling mainly large enterprises to grant their many employees access to the various systems in their IT infrastructure that they needed to do their jobs. Different staff groups required access to different systems, and IAM controlled who could access what, provisioning credentials for new joiners and changing access rights for people as their roles within the organization changed, then decommissioning their access when they left the company.
That business-to-employee (B2E) role underpinned the entire first wave of IAM growth, but then as companies moved to outsource certain business functions to third parties or took on contractors to perform specific tasks for limited periods of time, the need to include this emerging business-to-business (B2B) use case placed new pressures on IAM systems. Not all identities to be used in the system resided in the corporate directory, leading to initiatives in the area of federation to enable companies to use partners’ directories as and when the need arose.

Now the requirements have moved on again. Driven by the explosion of e-commerce, companies now need to use IAM to manage and control their online interactions with customers. This represents a challenge, not only in terms of the sources of identity, because the corporate directory won’t be the right place for it to reside, but also in terms of scalability, where the largest B2E implementations might run into the hundreds of thousands. For the business-to-consumer (B2C) environment, however, many e-tailers and other companies selling primarily online can expect to interact with many millions of customers.

The cloud is the future of IAM

Not surprisingly, the cloud is emerging as the locus for identity services, particularly as customer IAM (CIAM) markets start to take off. Cloud offers the scalability required to handle millions of identities, as well as the flexibility that the globalized, outsourced, work-from-anywhere economy now requires.

The impact this has had on the IAM market is predictable, insofar as most traditional IAM platform providers see the cloud as a new opportunity and a natural extension of their overall IAM coverage.
However, identity-as-a-service (IDaaS) specialists, such as Centrify, Okta, OneLogin, and Ping, which came into existence to create a cloud-based identity management platform for delivery as a service, see IDaaS as a separate market that they own.

To date a steadily growing number of organizations are taking up the IDaaS challenge. Most are taking the hybrid route that requires support for a mixed range of on-premise and in-the-cloud IAM services, which in the short to medium term is a fair representation of identity management requirements within the enterprise.

Beyond customers are things

While B2C can be considered the next frontier for identity management technologies, the frontier after that is already visible in the shape of the Internet of Things (IoT). If managing the identities of millions of online customers is a challenge for traditional IAM platforms, the problem is only compounded with the advent of IoT, where there are estimates that as many as 20 billion unmanned devices will be Internet-connected by 2020. We have already seen this year how IoT devices can be harnessed for cybersecurity exploits such as DDoS attacks. Connected car infrastructure has also been hijacked by security researchers to demonstrate the potential dangers in automotive IoT.
Figure 3: All these things will need identity to be secure

Source: Ovum

Figure 3 illustrates some of the security issues on the horizon, and even though a lot of the devices are low-power, and have only limited compute capabilities, their threat potential should not be ignored. Indeed, we are only now starting to perceive the potential security issues around having vast numbers of devices on the Internet, communicating autonomously without human interaction.

In 2017 and for the foreseeable future, identity management will continue to have a vital role to play. IoT will extend this role further, also making it responsible for policing the world of unmanned devices. It will be used to assure that a device is what it claims to be, and that its integrity has not been compromised since its last communication.
Cyber threats must not be allowed to interrupt the adoption of digital services

Cybersecurity protection must be in place to deal with the latest threats

Technology provides businesses with ever-widening opportunities to communicate with all types of user, but at the same time it increases the risk from cyber threats. The use of cloud-based services and the opening up of mobile communication channels supports open access to business systems and globalization opportunities, including mergers and acquisitions to help grow the business, the extension of third-party networks and relationships to add operability and improve efficiency, and the outsourcing and adoption of managed services to deliver potential cost savings. Nevertheless, and despite the long list of business benefits, what all these forward-looking approaches have in common is their inherent capacity to increase business risk.

To keep business operations safe while also maintaining performance levels and the ability to execute new business strategies, cybersecurity protection services need to be at the heart of all operational initiatives. They need to be a fundamental, base-line consideration each time changes and new strategies are discussed.

Change and the use of new technology has to be supported

As business systems move forward, nothing is going to stop the demand for more change and greater operational efficiencies. Business decision-makers will accept some of the operational risks their actions cause, but at the same time will reasonably expect their security providers to keep pace and deliver on the promise of better, intelligence-led security services that are fit for purpose.

The components of automated security analytics, artificial intelligence, and machine learning, along with a host of EUBA and EDR-based analysis, protection, and remediation services are readily available. We recognize that the trend toward their use is growing, and 2017 has to be the year they start to have a real impact.

Failure to deal with all forms of cyber attack brings significant business risk, and because of the many high-profile cyber breaches already reported, cyber attack and security breach responses are now quite rightly board-level issues. The fallout goes beyond IT infrastructure damage. It can include multiple millions in breach and remediation costs and significant trade and revenue losses, along with brand and reputation damage. This is why change the use of new technology has to be supported by business-focused cybersecurity systems that are fit for purpose.

Appendix

Further reading


*Service Provider Strategies in Managed Security Services, IT0019-003571 (September 2016)*
Identity and Access Management: Providing Safe and Simple Access for All, IT0022-000658 (April 2016)

"Symantec acquires Blue Coat and Greg Clark becomes CEO", IT0022-000710 (June 2016)

"Akamai buys Soha for secure remote access over the public Internet", IT0022-000795 (October 2016)

Author

Andrew Kellett, Principal Analyst, Infrastructure Solutions
andrew.kellett@ovum.com

Rik Turner, Senior Analyst, Infrastructure Solutions
rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum’s consulting team may be able to help you. For more information about Ovum’s consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

The contents of this product are protected by international copyright laws, database rights and other intellectual property rights. The owner of these rights is Informa Telecoms and Media Limited, our affiliates or other third party licensors. All product and company names and logos contained within or appearing on this product are the trademarks, service marks or trading names of their respective owners, including Informa Telecoms and Media Limited. This product may not be copied, reproduced, distributed or transmitted in any form or by any means without the prior permission of Informa Telecoms and Media Limited.

Whilst reasonable efforts have been made to ensure that the information and content of this product was correct as at the date of first publication, neither Informa Telecoms and Media Limited nor any person engaged or employed by Informa Telecoms and Media Limited accepts any liability for any errors, omissions or other inaccuracies. Readers should independently verify any facts and figures as no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.
CONTACT US
www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES
Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo