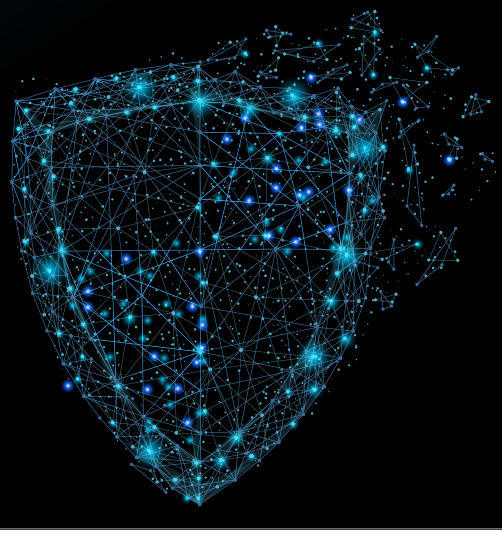
2017 Next-Generation Endpoint Security Vendor Landscape and Five-Year Market Forecast

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report
Written by David Monahan

Q3 2017



Sponsored by:

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

2017 Next-Generation Endpoint Security Vendor Landscape and Five-Year Market Forecast

Table of Contents

Executive Summary

This is the second iteration of this report (the first was distributed in 2015). The vendor-related research focuses on solution providers that are supplying proactive next-generation endpoint security services covering prevention, detection, and response. EMA provided all identified participants the opportunity to participate in a vendor-answered questionnaire and interviews. EMA then combined that information with research efforts external to the providers to create company profiles and assess each vendor on their applicability to the space, as well as their market share by revenue and license volumes. Most of the vendors competing in this space emerged or refocused in the last few years, with only a few having competed in the market for more than five years.

As with any study, this study is only as good as its data inputs. This research identified 42 solution-provider candidates as participants. Of those companies, eleven vendors elected not to respond or share data. Within the remaining 31, some were unable to provide complete data due to company policies limiting some analysis, but efforts were made to fill in as many blanks as possible using publically-available information.

The NGES market is highly competitive. With a 2014/2015 annual growth rate over 100 percent and 2016–2017 shaping up similarly, NGES is pushing a five-year average annual growth rate of over 50 percent.

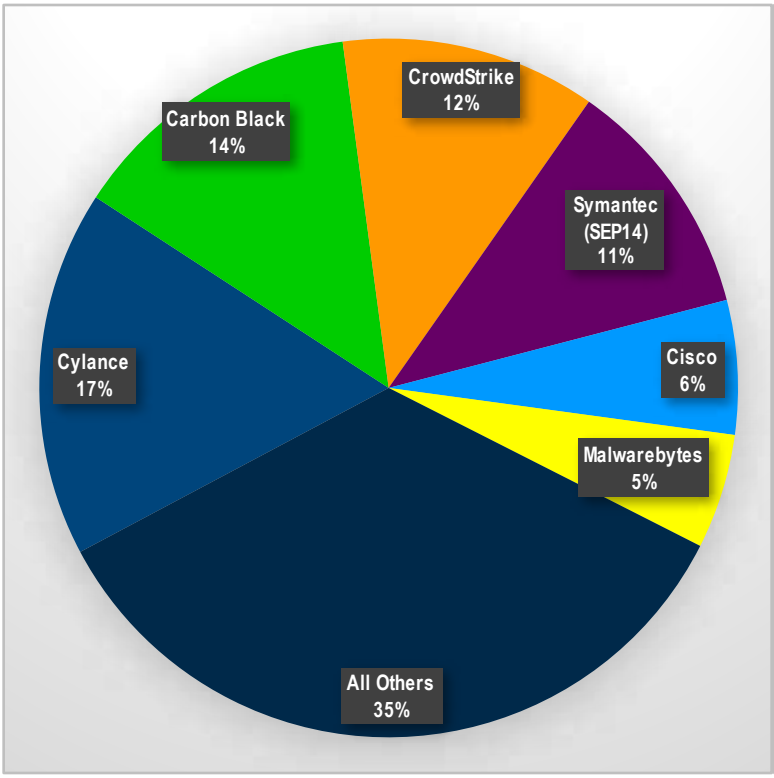


Figure 1: 2016/2017 Top 5 Ranked NGES Vendors by Revenue Market Share

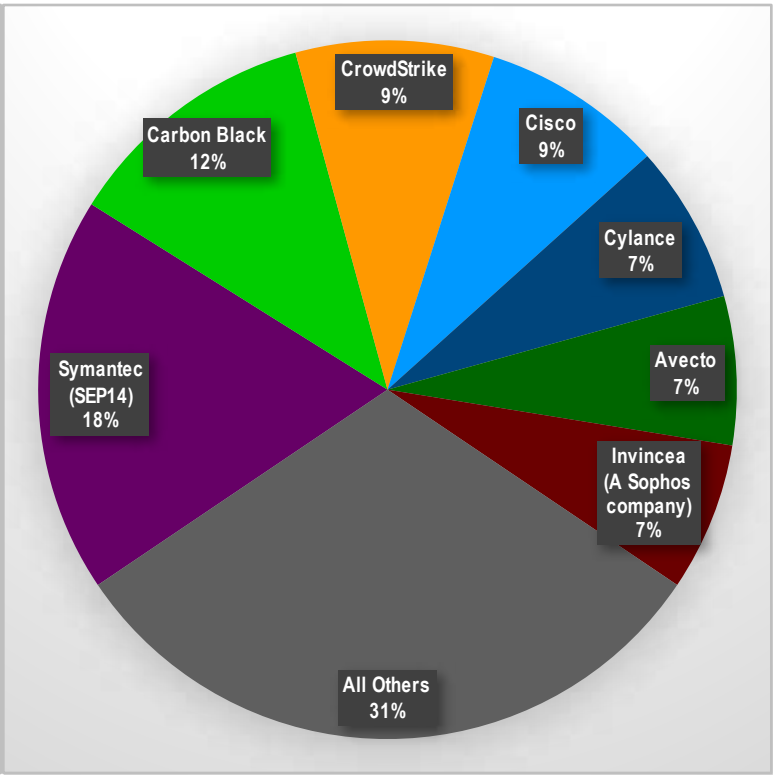


Figure 2: 2016/2017 Top 5 Ranked NGES Vendors Market Share by Licenses Sold

Background and Scope

Vendors providing next-generation endpoint security are focused on endpoint protection via prevention and/or detection and response. However, their approaches vary and each has its own intellectual property around how it provides its protections. Some focus more marketing efforts on their strength in file-less attack defense, while others focus more on file-based attack defense.

Non-signature-based approaches include adaptive and dynamic application control, sandbox containers, virtualization, unsupervised adaptive machine learning, and deep learning for anomaly and behavioral detection, system correlation between endpoint and network for detection, and a few other proprietary methods. It is important to note that while most vendors rely on an endpoint agent, several of them have created a totally agentless solution.

The report focuses on enterprise-capable solution providers. The minimum qualifications for an enterprise-class solution are listed in the "Inclusion Qualifications and Definitions" section. The research was open to all enterprise-focused vendors; none of the invited vendors paid EMA or was paid to participate in the research.

Though significant time was put into selecting vendors, there are probably a few that were not identified. However, EMA believes any remaining vendors are small enough compared tt the overall market that their exclusion does not significantly affected the outcome of the analysis.

A significant driver of this report is to provide the buying community information about the vendors in the space and give vendors the opportunity to discuss their next-generation protection capabilities and, especially for the traditional antivirus players, to break out of their perceived molds. With this goal in mind, it was disappointing that some vendors chose to not participate.

Inclusion Qualifications and Definitions

In order to qualify as a next-generation endpoint security player, vendor solutions must meet the following criteria.

Functionality Definitions

1. **Prevention solutions** must stop the execution of malware. Depending on the solution, the means of prevention and the place in the kill-chain at which the prevention activates will vary considerably. Some solutions stop executables from activating, while others use behavioral monitoring of the program during its lifecycle and stop attempts to perform actions that are outside the realm of normal operations. These activities can include writing to system memory space, process injection, opening network connections, and many others.
2. **Detection solutions** do not attempt to stop execution, but rely on their ability to identify activities and changes that the advanced persistent threat (APT) makes to the operating system, configuration and/or data files, processes, memory, etc. Other patterns can include new and unknown files such as data accumulation for exfiltration, and endpoint-initiated communications and connections that can indicate command and control.

Qualifications for Consideration

1. **Non-reliance on signature- and pattern-based enforcement or detection** – This is one of the most significant entrance requirements. It is clear that signature- and pattern-based solutions have passed their peak. First, enterprises are less tolerant of the signature approach because it leaves them vulnerable to early attacks prior to signature creation. For an organization that is one of the early targets, this can easily equate to millions of dollars in losses. Second, with more threat actors creating code and a proliferation of code recombining tools, signature writers can't keep up with the variants and users won't put up with broad signatures that cause excessive false positives.
2. **Proactive detection or prevention** – Users of these solutions depend on the solutions' ability to proactively identify and/or prevent device compromise, and alert and notify administrators of incidents they detect and/or stop. The solutions may not prevent or detect all issues, but when they do, they let someone know.
3. **Centrally manageable and scalable** – To qualify as an enterprise-class system, the solution must have the capacity to be installed across thousands of endpoints and be centrally managed. It should require only a few administrators to install and maintain it. The solution provider preferably creates and supports the central management console, but that is not a hard-and-fast requirement. If the solution cannot be centrally managed, then no business will seriously consider it because they will not be able to meet administration needs in any sizeable environment.
4. **Granular policy-based control** – Regardless of how each of the solutions accomplishes its task, the requirements for operation, enforcement, alerting, and access must be controlled by a policy (or rules) engine. Existence of this engine is important for consideration in any business environment, since companies require consistent policy alignment within the environment and usually have limited personnel resources for management.

More Detailed Requirements List

Next-Generation Endpoint Security Solutions Must Have:

1. Comprehensive protection services in the form of prevention and/or detection services.
2. Hunting or forensic capabilities to identify artifacts as indicators of compromise and identify adversary activities. Hunting relies on real-time data collection and dissemination, while forensics rely on historical artifact collection.
3. The ability to provide the people managing the endpoints with some form of endpoint search and status interrogation.
4. Centralized software distribution for updates or integration with an existing distribution solution.
5. Some form of centralized management console for determining the status of and issues with all managed endpoints.
6. Components for centralized data collection and/or threat analysis.
7. The ability to provide the protection services in real time (as an incident occurs) or near real-time (consistently operate within a few minutes).
8. The ability to identify zero-day or emerging attacks against endpoint vulnerabilities, including custom malware, advanced persistent threats (APTs), and advanced targeted attacks (ATAs).
9. The ability to provide the people managing the endpoints with sufficient visibility and context that will create high confidence of and actionable insights into the endpoint attack or compromise.

10. The ability to provide some form of automated and/or automatic mitigation actions to support incident response.
11. Some form of centralized reporting capabilities for both operations and management-level reporting.

Next-Generation Endpoint Security Solutions May:

1. Provide continuous endpoint monitoring, and posture assessment and status. This would be a specialized function within items 5, 6, and 9 above.
2. Have cloud components for management, data collection, and/or threat analyzation.
3. Have hardware appliances for management, data collection, and/or threat analyzation.

Next-Generation Endpoint Security Solutions Should Not:

1. Rely solely on signature-based prevention or detection methods.
2. Rely on static indicators of compromise (static IOCs are artifacts used in compromise or that are left post-compromise that must be consistent across attacks for the attack to be prevented and/or detected).

All solutions in this space have a response capability. At a bare minimum, response capabilities include common alerting of incidents to a log management, security incident and event management (SIEM), or similar solution. However, more advanced detection solutions provide mitigation and/or remediation capabilities. While many in the market are still building their confidence around these new remediation capabilities and mitigation techniques while continuing to reimage machines, some are taking full advantage of the capabilities to initiate surgical strikes against malware on the infected system, leveraging the automation and accuracy to save significant time and money, both for the IT teams and for the affected individual. On average, the time savings of this technique over rebuilding a system is three hours of IT time per infected system, plus the end-user time to re-customize the desktop, apps, and other system settings, as well as reloading data.

Market Maturity and Evolution

The NGES market sprung out of an inability of traditional antivirus to protect endpoints from the varied threats. The signature-based model that was used for the last 20+ years cannot defend against previously unseen threats, and often has problems with balancing efficacy against attack derivatives. By definition, a signature is pattern-made to match an identified threat, so someone has to be patient zero and suffer the consequences—and the consequences of compromise keep getting more severe. Generally, organizations have become intolerant of that approach. While users should not entirely discount signatures as a means of filtering out the common or nuisance threats, as the more advanced adaptive solutions continue evolving, the need and desire for signature-based defenses continue to decline.

The increasing pressures from advanced malware and ransomware allowed innovative and more agile newcomers to develop and market their varied approaches. A recent Enterprise Management Associates (EMA) study saw as much as a 38 percent adoption rate of NGES solutions used both in parallel with and replacing traditional antivirus (this was a six-point increase from the previous study).[1] The proportional use of NGES in parallel with traditional AV is declining in favor of removing traditional AV. Reasons for this trend are discussed in the following section.

[1] EMA, Data Driven Security Unleashed, 2017

The Big 5 and NGES

"The Big 5" is a term for the largest and most established enterprise antivirus companies that have been attacking the problem of endpoint defense for well over 20 years: Kaspersky, McAfee, Sophos, Symantec, and Trend Micro. They have all been identified as leaders in the traditional antivirus market, and each has yearly revenue rivaling the combined revenue of all of the pure-play NGES vendors combined. However, it was their dedication to the signature-based antivirus approach that brought about the birth or the NGES vendors and the emergence of the NGES space. The arrival of NGES solutions has been credited to the Big 5's lack of innovation or lack of agility to adapt to the changing endpoint threat landscape. While these labels have some merit, they are not entirely fair or true. Each of the Big 5 had and still has a viable business selling signature-based antivirus and while they were late to the non-signature-based defense game, at least some, and maybe all, have been working to enhance their solutions to address current threats.

This year only one of the Big 5, Symantec, substituted information detailing their NGES solution details, the others are represented with public information, where available. The market size calculations do attempt to include estimates for those vendors that discussed next-gen capabilities with EMA. Being the only vendor that sat down with EMA to dig into the numbers for their next-gen solution, SEP14, Symantec put together a compelling story. More information on the details can be found later in the report and applicable profiles.

Acceptance of NGES by Auditors and Regulators Affecting NGES Industry

One of the most significant drivers in the change in approaches from running NGES parallel with traditional AV has been the expansion of understanding about these solutions and how they can operate independently of traditional antivirus. Auditors had time to see the demonstrated efficacy of these solutions against both known and unknown malware, and have begun accepting these solutions as valid replacements even though they do not use the term "antivirus."

There is also a current industry push to apply the common label of next-generation antivirus (NGAV) to these tools to facilitate further acceptance on the part of auditors and regulators.

Market Evolution

In the previous NGES market sizing report, EMA estimated the market to be within the adoption point of the "Market Evolution Curve." Given this report's data, it is obvious that this technology segment has rapidly passed the adoption gap in the emerging market and is on the steep upward curve of the growth market.

This transition from emergence to growth was quite rapid, taking place over the course of about four to five years with significant acceleration in the last two and the full emergence into growth.

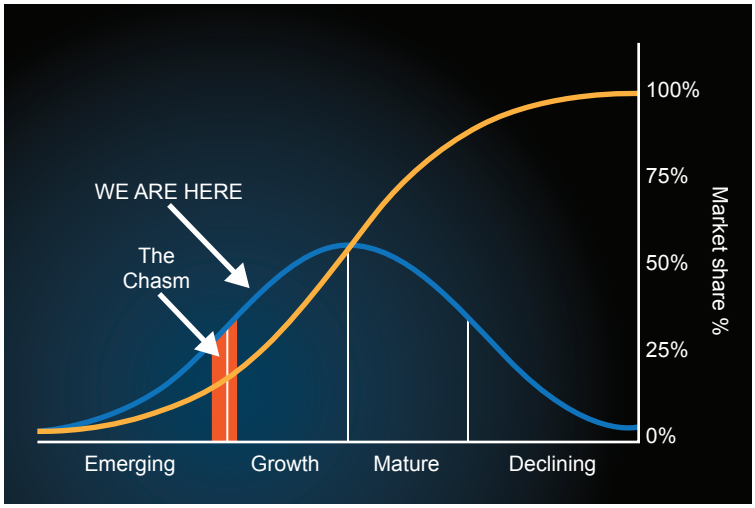


Figure 3: Market Evolution Curve and "The Chasm"

Other facts that support this estimate of the market stage include the following:

1. There is (still) a yearly increase in the number of vendors supplying next-generation endpoint security (over 45 vendors identified for this report).
2. Average vendor growth, though lower than the previous report, is still in the extraordinary range at over 100 percent.
3. Of the identified vendors, more than half have been operating in the enterprise endpoint space for five years or less.

Though the number of new entrants slowed significantly since 2014, it hasn't stopped. The trend can be seen in Figures 4 and 5.

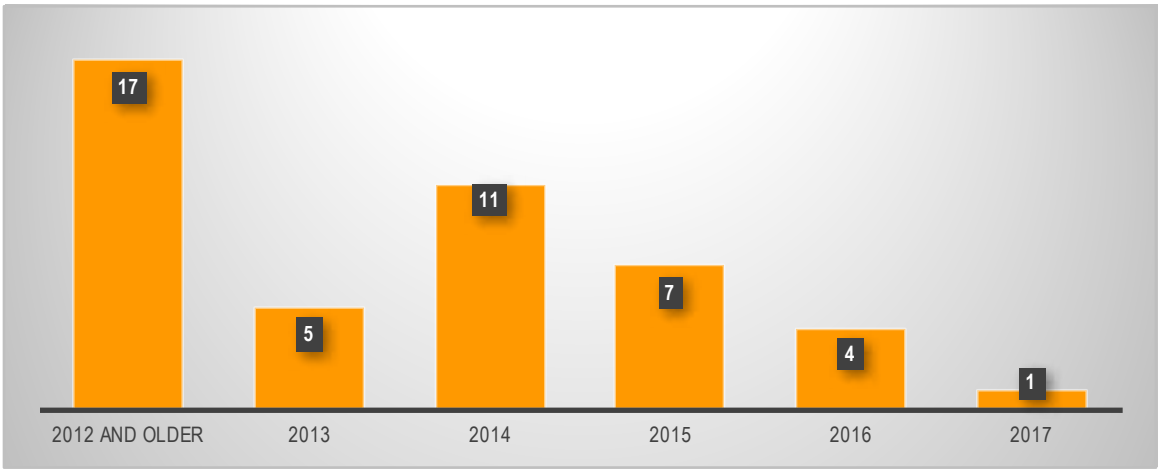


Figure 4: 2016/2017 Vendor Start Years

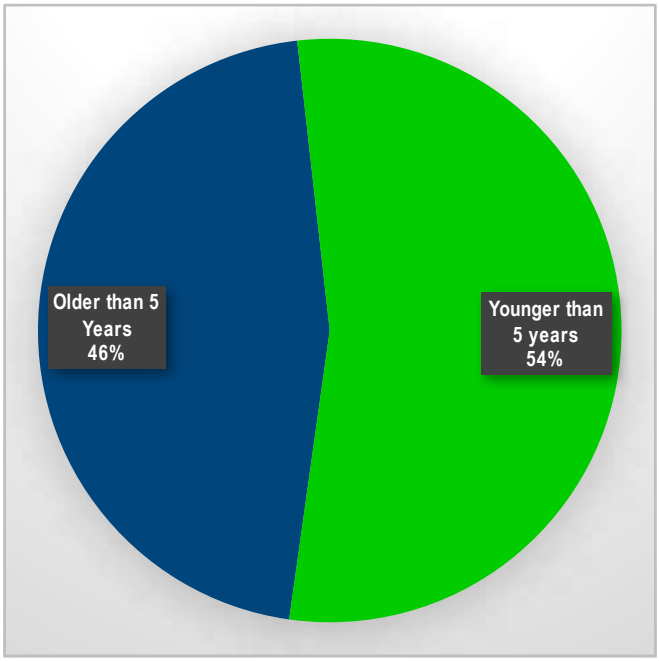


Figure 5: 2016/2017 Vendors Five Years Old & Newer vs. Over Five Years Old

Convergence of Detect and Prevent Into Protect

Historically in the endpoint protection arena, there has been a battle between users and vendors of prevention versus detection. Each has its pros and cons. However, since the last report, a convergence has begun. While there are still pure plays in each camp, some of the vendors began combining the strengths of both approaches. Many organizations like having protections of both a strong detection solution and a similarly strong prevention solution. However, most cannot afford to pay for two vendors to provide these services, so innovative and opportunistic vendors have been branching out to include both capabilities in their solutions.

Researched Vendors

PARTICIPATING VENDORS (NEW PARTICIPANTS MARKED IN BLUE)				
1E	Cyberbit	Fidelis Cybersecurity	Nuix	SentinelOne
Bufferzone	Cybereason	FireEye	Nyotron	Invincea (A Sophos Company)
Carbon Black	Cylance	Fortinet	Palo Alto Networks	Symantec
Cisco	Deep Instinct	IBM	Panda Security	Tanium[A]
Comodo	Digital Immunity	Malwarebytes	Promisec	Ziften
Countertack	Endgame	Minerva Labs	Romad Cyber Systems	
CrowdStrike	EnSilo	Morphisec	RSA	

Table 1: Next-Generation Endpoint Security Providers Participating in Research

[A] See discussion on Tanium in "New Entrants, Acquisition and Market Consolidation" and "Vendor Profiles"

NON-PARTICIPATING VENDORS (PREVIOUS PARTICIPANTS WITHOUT UPDATES ARE MARKED IN RED)		
Avast	Guidance Software	Outlier
Avecto	Intezer	Sophos
BitDefender	Kaspersky	Trend Micro
Bromium	McAfee	Webroot

Table 2: Next-Generation Endpoint Security Providers Declining to Participate in Research

New Entrants, Acquisition, and Market Consolidation

New Entrants

Based out of the UK, **1E** has operated for twenty years primarily focused on software life-cycle automation. However, since its entrance into the North American markets it has expanded into the NGES marketspace with its Tachyon product. Tachyon adoption has soared with 80 percent of its current NGES client base being large US-based organizations. Due to its feature-set, 1E is also a contender in the emerging "Syssecops" area, discussed later in the report, competing with the likes of IBM, Tanium, Ziften and others.

IBM is the most recent entrant into the market (it is really more of a reentry). In the previous report, IBM was supporting the Apex endpoint solution acquired with Trusteer. IBM has placed Apex into end of sale and reentered on a broader scale with a detection solution based on augmenting features of their BigFix endpoint management solution, which it has labeled IBM BigFix Detect.

Nuix was founded 2000 in Australia and made a reputation as one of the most advanced eDiscovery and electronic investigation platforms and endpoint forensics services companies. Using expertise gained there, it created an NGES solution, formed a US headquarters, and entered the North American endpoint protection market.

Minerva Labs is headquartered in Tel Aviv, Israel. Founded in 2014, the first delivery of its endpoint protection solution was in January 2016.

Morphisec is headquartered in Be'er Sheva, HaDarom, Israel. Founded in 2014, the first delivery of its endpoint protection solution was in January 2016.

Acquisitions

Confer was acquired by Carbon Black on July 19, 2016

Invincea was acquired by Sophos on February 8, 2017

Triumfant was acquired by Nehemiah Security in October, 2016

Multiple factors individual to each acquirement drive these acquisitions, but the common factor is in portfolio expansion. Each company contained some technical capability that the acquirer felt it needed to enhance its market attractiveness or viability. While it is outside of the scope of this report to delve into these in detail, one aspect crucial to the current report (based on predictions in the last report) is the Sophos acquisition of Invincea. In the EMA 2015 endpoint buyers' guide report,[2] the author made a prediction that the Big 5 antivirus vendors would most likely have to purchase an existing NGES vendor to gain market credibility for the NGES capability. Sophos already had Intercept X as their NGES entrant, but decided to make the Invincea purchase anyway. While it is a good addition to the portfolio, it also gives Sophos the benefit of more credibility of now having what was already recognized as a solid NGES solution.

Other Vendor Consolidation

Hexis Cyber Solutions' technology portfolio was divested by its parent company, KeyW. The company assets were sold to WatchGuard Technologies on June 7, 2016, and then incorporated into WatchGuard's Network and Endpoint Threat Correlation solution.

Light Cyber had both a network and an endpoint solution that worked together to identify threats. Light Cyber had moved into the category of Advanced Breach Detection, and therefore out of NGES, just prior to Palo Alto Networks' acquisition of them on February 28, 2017.

McAfee had a hard run over the last few years. With any luck, some of those problems are past them. In September of 2016, Intel sold a majority stake to investment firm TPG, who spun it back out into its own company.

The market consolidation will continue. In the emerging and growth market cycles, everything is up for grabs and the laurels may not go to the best technology, but to the best marketers. While EMA does not believe there will be an "overnight" consolidation, with so many vendors identified in this space, the competition for dollars and technical resources is fierce.

Just as Cisco, Palo Alto Networks, FireEye, Carbon Black, Fidelis Cybersecurity, IBM, Sophos, and RSA already leveraged acquisition as a means to enter the market and some companies failed, more will follow one road or the other. Each of the players has significant intellectual property, and as the smaller companies prove themselves, they are ripe for the picking from the other, larger NGES competition for either technical enhancements or customer bases. Four of the Big 5 still have significant reason to make an acquisition in the space.

[2] Next-Generation Security Buyer Perceptions, Priorities, and Issues: A Guide for Endpoint Security Consumers and Vendors

Vendor Market Shares

EMA evaluated market share and market stature using three variables. Each variable speaks to a core aspect of the market and how consumers perceive it.[3]

1. **Largest single deployment –** This variable speaks to scalability of the product from the enterprise perspective. All of the participants had single deployments in the tens of thousands, and many had single deployments in the hundreds of thousands.
2. **Customer licenses –** This variable speaks to the overall penetration of the solution provider in the marketspace.
3. **Revenue –** This variable speaks to the financial viability of the solution provider.

As readers compare the rankings by revenue and licensing, they should note some ranking alignments and some disparities in rankings. These features demonstrate the differences in promotional and "strategic" pricing, as well as early beta customer license incentives, the latter of which is a significant factor with so many of the companies being very young.

Largest Single Deployment

(Within the tied levels, vendors are listed in alphabetical order.)

COMPANY NAME	2016/2017 RANK BY LARGEST DEPLOYMENT
Symantec	1
Avecto	2
FireEye	3
Bromium	4
CrowdStrike	4
Cylance	4
Fidelis Cybersecurity	5
Invincea (A Sophos company)	5
Bufferzone	6
Carbon Black	6
Cisco	7
Cybereason	7
RSA	7
Cyberbit	8
Malwarebytes	8
Ziften	8
1E	9

COMPANY NAME	2016/2017 RANK BY LARGEST DEPLOYMENT
Countertack	9
Endgame	9
Fortinet	9
Panda Security	9
Promisec	9
Palo Alto Networks	10
SentinelOne	11
Comodo	12
Deep Instinct	12
EnSilo	12
Morphisec	12
Minerva	13
Nyotron	13
Digital Immunity	*Insufficient Data*
IBM BigFix Detect	*Insufficient Data*
Nuix	*Insufficient Data*
Romad Cyber Systems	*Insufficient Data*

Table 3: Next-Generation Endpoint Security Providers Ranked by Largest Single Deployment

[B] Sophos did not disclose its largest Intercept X deployment

[3] Not all vendors who participated in the research were able to disclose all aspects of the requested information due to various business constraints. In those cases and where other information was available, estimates were generated and used in calculations.

All vendors ranked through number nine have at least 100,000 endpoints deployed and managed by a single customer, demonstrating significant ability to scale. Even the vendors ranked from nine to the end of the list have reported single deployments in the tens of thousands, indicating that scale may only be an issue for the largest of perspective buyers.

In each of the vendor profiles, the management console is identified as on-premises or cloud. The management console architecture is a consideration in-scale as on-premises consoles will cost more to create and maintain than an included cloud console.

Vendors that use agentless endpoint protection are identified in their profiles. With an agentless installation, they have the advantage of being operational in far less time (hours to a couple of days, depending on number of endpoints). They have no need to make changes on the endpoints themselves and use correspondingly less maintenance time because there are no agents to maintain. The trade-off is that prevention is not possible. These solutions allow only detection and response. Also, the technology implementation and the interval between polling cycles may affect attack detection time.

Market Share by Licenses Sold

Special Notes:[4]

IBM BigFix Detect is a new licensed capability only unveiled in 2017, so though BigFix has a very large customer base, the current adoption rate is only a small percentage of the base and was undisclosed.

Sophos did not share numbers around their Intercept X solution, which was their contender in the NGES market space prior to the Invincea acquisition. Given the information it has previously shared, it should be noted that Sophos did have Intercept X customers so the combination of both solutions under Sophos would be greater than represented in the Invincea line item.

Symantec is competing in the NGES market using an update to its flagship SEP product, it is important to note that Figure 6 below includes Symantec as it relates only to its SEP14 release which is it first product release that is primarily dependent on non-signature-based detection and prevention. This includes only customers that have installed or upgraded to SEP14 as of data gathering for the report. Other Symantec customers running previous versions are not included to maintain an apples-to-apples caparison.

Tanium is not included in this ranking due to factors discussed later in the report. If only half of Tanium's clients are using the solution for security use cases, Tanium would have been ranked in the top five.

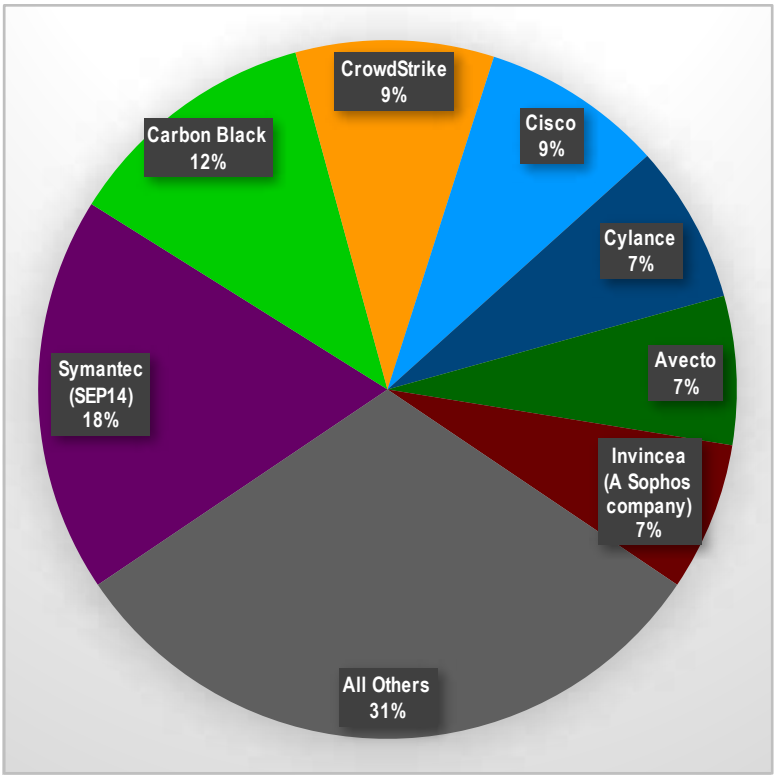


Figure 6: 2016/2017 Top 5 Ranked NGES Vendors' Market Share by Licenses Sold

[4] Values for vendors that provided information for the previous year's reports, but not this year's report, were estimated.

Market share by licenses is significant because, aside from there only being so many seats to fill, it demonstrates overall penetration of the vendor in the marketplace. The volume of licenses may be a more accurate indication of the overall size of the company than revenue due to the fact that you can't give away a poor product at any scale, especially in a commercial environment where people's reputations and livelihoods are at stake.

(Within the tied levels, vendors are listed in alphabetical order.)

COMPANY	2016/2017 RANK BY LICENSES SOLD
Symantec (SEP14)	1
Carbon Black	2
CrowdStrike	3
Cisco	4
Avecto	5
Cylance	5
Invincea (A Sophos company)	5
Cybereason	6
Fidelis Cybersecurity	7
Malwarebytes	8
FireEye	9
SentinelOne	9
Bromium	10
1E	11
Bufferzone	11
Comodo	11
Countertack	11

COMPANY	2016/2017 RANK BY LICENSES SOLD
Cyberbit	11
Endgame	11
Panda Security	11
Ziften	11
Deep Instinct	12
Digital Immunity	12
EnSilo	12
Fortinet	12
Minerva Labs	12
Morphisec	12
Nyotron	12
Promisec	12
Romad	12
RSA	12
IBM BigFix Detect	*Insufficient Data*
Nuix	*Insufficient Data*
Palo Alto Networks	*Insufficient Data*

Table 4: Next-Generation Endpoint Security Providers Ranked by Licenses Sold

Significant Licensing Ranking Changes

- **CrowdStrike** had the most significant ranking change, moving from eighth place in the 2014/2015 report to third in 2016/2017.
- **Fidelis Cybersecurity** dropped from second place in 2014/2015 to seventh place in 2016/2017.

Market Share by Revenue

Market share by revenue is a relevant measure. The issue with revenue is that, despite the list price, there is no common value. As larger companies, prospects considered "strategic," and tougher and timelier negotiators may get better pricing, revenue is all over the place. The percentage of support cost for perpetual licensing also varies because of the same factors. However, revenue shows how viable and solvent a company is and thus how likely it is to weather economic downturns and other financial crises.

Special Notes:

Symantec is competing in the NGES market using its SEP14 product. SEP14 is an entire overhaul of the product which relies more upon machine learning and other newer protection techniques rather than signature. It is for this reason that Symantec is included in Figure 7 below. As Symantec's customers convert to SEP14 Symantec can turn up the marketing engine to discuss the benefits of SEP14 and how it competes with the other NGES solutions. As Symantec applies its marketing might, and very large revenue stream, to promoting the benefits of SEP14 as an NGES solution, it may be able to slow the growth of others in the market. This will remain to be seen but will be captured in the next iteration of this report.

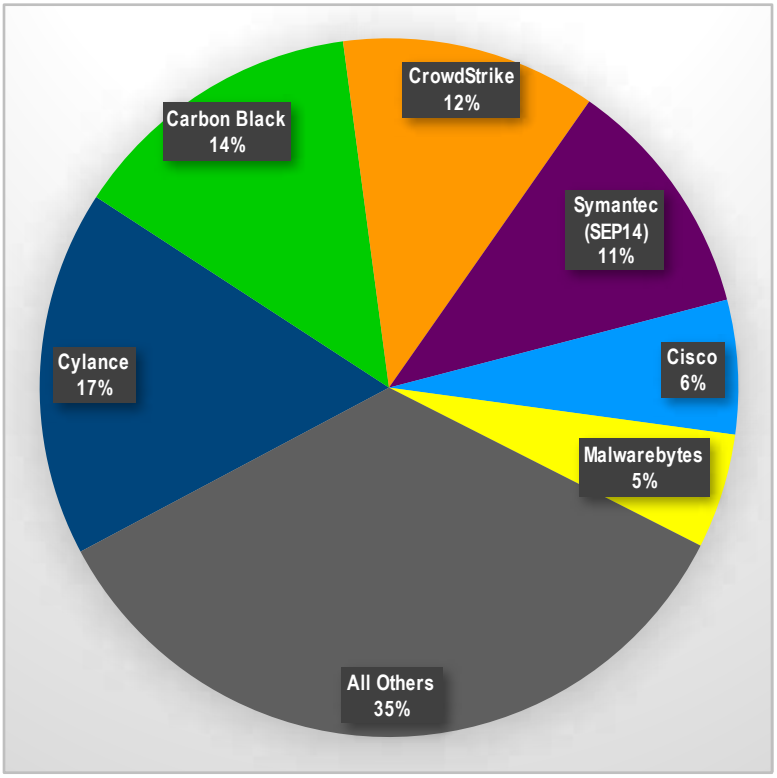


Figure 7: 2016/2017 Top 5 Ranked NGES Vendors by Revenue Market Share

(Within the tied levels, vendors are listed in alphabetical order.)

COMPANY	2016/2017 RANK BY MARKET SHARE
Cylance	1
Carbon Black	2
CrowdStrike	3
Symantec (SEP14)	4
Cisco	5
Bromium	6
Malwarebytes	6
FireEye	7
Cybereason	8
Invincea (A Sophos company)	8
Avecto	9
Cyberbit	9
Endgame	9
Panda Security	9
SentinelOne	9
1E	10
Comodo	10

COMPANY	2016/2017 RANK BY MARKET SHARE
Countertack	10
EnSilo	10
Fidelis Cybersecurity	10
Nuix	10
Palo Alto Networks	10
Ziften	10
Bufferzone	11
Deep Instinct	11
Fortinet	11
Minerva Labs	11
Morphisec	11
Nyotron	11
Promisec	11
Digital Immunity	*No Data*
IBM BigFix Detect	*No Data*
Romad	*No Data*
RSA	*No Data*

Table 5: Next-Generation Endpoint Security Providers Ranked by Revenue

Composite Ranking[5]

The aggregate rank number may tell the best story, since it takes into account both licenses and revenue. If a vendor keeps a relatively level pricing structure, then their rankings by revenue and by licenses should be consistent. On the other hand, the organizations giving away or "strategically discounting" large numbers of licenses, though they are gaining market saturation by licensing, will have a significantly lower ranking by revenue.

(Within the tied levels, vendors are listed in alphabetical order.)

COMPANY	2016/2017 COMPOSITE RANK
Carbon Black	2
Symantec (SEP14)	2.5
CrowdStrike	3
Cylance	3
Cisco	4.5
Invincea (A Sophos company)	6.5
Avecto	7
Cybereason	7
Malwarebytes	7
Bromium	8
FireEye	8
Fidelis Cybersecurity	8.5
SentinelOne	9
Cyberbit	10
Endgame	10
Panda Security	10
1E	10.5

COMPANY	2016/2017 COMPOSITE RANK
Comodo	10.5
Countertack	10.5
Ziften	10.5
Bufferzone	11
EnSilo	11
Deep Instinct	11.5
Fortinet	11.5
Minerva Labs	11.5
Morphisec	11.5
Nyotron	11.5
Promisec	11.5
Digital Immunity	*Insufficient Data*
IBM BigFix Detect	*Insufficient Data*
Nuix	*Insufficient Data*
Palo Alto Networks	*Insufficient Data*
Romad	*Insufficient Data*
RSA	*Insufficient Data*

Table 6: Next-Generation Endpoint Security Providers Ranked by Composite of Licenses and Revenue

Market Size and Forecasts

The next-generation endpoint security market is part of both the larger Endpoint Software Security Market, which includes traditional antivirus as the majority of its revenue, and the even more expansive Endpoint Security Market, which includes all of the previous plus antispyware and antimalware, firewall, endpoint device control, intrusion prevention, and endpoint application control. Both of those markets include commercial and consumer purchases. It most closely aligns with the Specialized Threat Analysis and Protection (STAP) market defined by IDC, though that definition included perimeter protection solutions while NGES does not.

[5] Vendors who did not supply enough information to make both license and revenue calculations are not included in this table

Total Revenue and Growth Rate

Participating vendors were asked to provide data from their most recent closed fiscal year. Total market revenue, including allowances for yet unidentified smaller vendors, is listed in Table 7.

	Est. NGES Market Value	Market Value Growth Rate	Average Company Growth Rate
2014/2015	$426,462,500	109%	105%
2016/2017	$847,080,000		

Table 7: Next-Generation Endpoint Security Market Revenue 2014 to 2016

Though most of the vendors are on a calendar year for financial reporting, not all are. The vendors that were able to provide revenue information reported similar growth rates between 2015 and 2016 as they reported in 2013 to 2014.

Due to the relatively small size of many of the vendors in the space, the average vendor growth rate was 105 percent. Many of even the largest vendors are seeing over 100 percent year-over-year growth, with smaller vendors seeing well over a 250 percent annual growth rate and extremes seeing 1000 percent. Though this level of growth is unsustainable for any long period of time, there is a huge amount of potential revenue to claim if the Big 5 and other large antivirus competitors cannot convince the market that they have competing solutions.

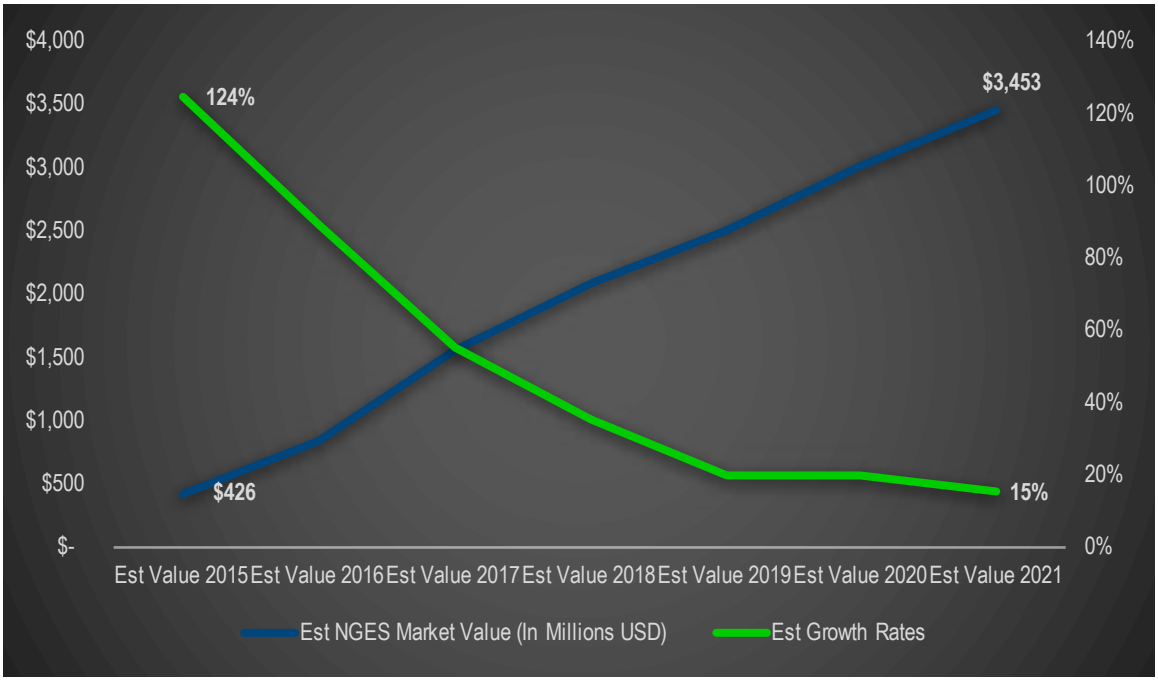


Figure 8: Estimated NGES Growth Curves 2015-2022

The current projected average growth rate for the NGES market across the next five years is between 45 percent and 55 percent.

The NGES market has grown faster than the anticipated growth rate. The previous midrange estimate for the closing 2016/2017 year was $724,986,250 with the calculated value being $847,080,000.

EMA Perspective

Though the endpoint security market slowed dramatically since 2014, it is still seeing new entrants. It is also seeing phenomenal growth rates in excess of 100 percent for nearly every vendor. The legacy antivirus vendors are pushing forward with updated technology and messaging to reflect the change in defensive needs. Their issue is market perception. Each of the Big 5 has revenue that rivals the entire NGES market, so from their perspectives, none of the vendors individually is a threat and the entire market is only a nominal threat. However, each year the NGES vendors are nibbling away at their foundation.

Market Evolution

Sophos was the first to dive in and make a major acquisition of an NGES vendor. Whether or not the remaining four will seize need or opportunity in the near future is a question only each of them can answer definitively, but as the new companies get larger, the threat of lost revenue will increase. CrowdStrike and Cylance all made significant growth over the last year. Two or three more years of equal growth may make them too large for a comfortable acquisition, leaving them on the market for the long haul not as major contenders, but major market share and revenue threats.

The good news for the remaining four is that there is still time to decide if an acquisition will be worth it. There are a variety of approaches and intellectual properties in the space, so an acquisition does not have to be for namesake only. Careful planning will show which of the NGES vendors could be a good match. The other option is to continue to tough it out, but that will require not only significant messaging pushes, but also some trusted (and unbiased) third-party testing to show how their next-generation approaches match up.

IBM chose to follow a slightly different path. Having acquired Trusteer Apex and learned some lessons, IBM decided to redirect efforts on making a single solution for both endpoint management and detection with BigFix Detect. Using the already-strong endpoint management brand, IBM is augmenting its capabilities to include detection. This is a great move. It already has a leading endpoint management solution with a large embedded install base, so adding the detect functionality and offering to those clients is virtually a no-brainer. Those who adopt get to remove an agent and a vendor, or not add one for detection, reducing cost and lowering complexity and the chance of agent conflicts.

Decouple Signature and Signature-Less

The Big 5 are not the only vendors to use a signature approach for defense. A few of the other NGES vendors augment their solutions with signatures. The approach is to catch the nuisance threats using signatures leaving the advanced processing engines to deal only with the more advanced threat detection and prevention.

For the Big 5 who have yet to make a decisive product move or split between signature-based defense and signature-less defense, it will be imperative to decouple the use of their AV engines with their next-generation capabilities. They should at least make identifying and configuring that part of the engine less complex and easier to distinguish so their engineers and marketers can easily identify those competitive features in sales meetings, shows, and general marketing.

Enter "SysSecOps"

SysSecOps, (systems, security, operations) is a new term floating around, used to discuss the integration of endpoint management and security functions to provide a more holistic view of the endpoint situation and risk associated with that posture. A number of vendors adopted their broader approach, including 1E, IBM, Ivanti (formerly Heat Software), Micro Focus, Nehemiah, Tanium, and Ziften.

While included in this report based upon their various endpoint protection capabilities, some of these vendors have additional endpoint management capabilities, which both enhance and expand on what are considered traditional endpoint security features. This looks to have all of the traits of a new market segment evolution, so EMA will continue to monitor this potentially emerging segment.

Convergence of "EPP" and "EDR" in Endpoint Protection

In the beginning, vendors for endpoint security were classified together and then the markets were redefined as those providing detection versus those providing prevention. In the last 18 to 24 months, a trend has begun. Some vendors began to merge their approaches into providing both detection and prevention (the vendors that combined protection are identified in their profiles). This trend is good for technology consumers and likely to continue for two main reasons. The first is that though security teams will load additional agents on their systems, they only do it begrudgingly and/or as a last resort. Having fewer agents on systems is highly preferred, so combining these defenses becomes a selling point for NGES vendors. Secondly, it will also be a means for the smaller, more agile vendors to attempt to get a leg up on the larger NGES vendors. If they can adapt their software faster, they have a claim to superiority, or at least preferential differentiation.

Endpoint Security Moving to the Cloud

Despite the vendors using the "lightweight agents," with everything happening on the endpoints, vendors are still a little leery of overtaxing resources, which was a major point of contention with antivirus and other endpoint tools when they kicked into action. One of the things the vendors are doing is pushing parts of management and/or analytics to the cloud.

By pushing management into the cloud, vendors can be more agile in the development of their management console and customers do not have the same installation and change control impacts. Customers also save money on the infrastructure costs because the NGES vendors are footing the bill for the console as part of the service price. The only downsides to cloud-based management consoles are external connectivity interruptions and having some level of data out in the cloud. Prospects should ask about what types of data are being pushed and stored in the cloud to ensure the vendor architecture does not violate corporate policy or governmental regulation for data sovereignty.

Vendors are also pushing some of the heavier threat analytics to the cloud. In general, this is also good for customers. It is less impactful on their endpoints and therefore less impactful on the users. The analysis and visualizations provided can be more extensive and the historical data can be maintained longer in aggregate than on an individual endpoint, without risk of loss from a malware incident or hardware failure. The caveat to analytics in the cloud is to ensure protection does not stop or is significantly weakened if the endpoint has lost its Internet connection logically or physically. If prevention or detection relies on the cloud, and connection is lost, that leaves the endpoint vulnerable during that window, which is not acceptable (an example is opening email attachments that are already downloaded into the client while Internet is down, and therefore the endpoint is unprotected because analytics can't take place).

Vendors able to leverage cloud for analytics also gain the advantage of being able to nearly instantly share gained intelligence to all cloud connected customers, thus protecting each more proactively.

Both the management and analytics functions should maintain persistent data when an Internet connection is lost, upholding that information on the endpoint until the connection is restored without loss of fidelity.

Vendors using and offering cloud analytics and cloud management consoles are identified in their profiles.

Educating Auditors and Regulators

In the previous report, EMA identified auditor and regulator or regulation body acceptance of NGES as an antivirus replacement as a crucial factor in market growth. This appears to be taking place with many groups accepting that NGES solutions perform at least as well as traditional antivirus. This is a good omen for continued market expansion.

Differentiation

In a market with more than 40 participants, creating and maintaining product differentiation is difficult—maybe even impossible. As soon as a thought-leading marketer is able to create a new concept and differentiate the company or product to gain attention, other less-imaginative marketers or those seeking to tagalong on the success latch onto the concept and create their own campaigns based on the original.

Imitation is frustrating not only for the company, but also for the consumers. Every year EMA sees similar messaging coming from security vendors across multiple technology markets, which confuse the customers and prospects alike. It is up to the marketers to keep their messages simple and focus on the components that are most unique to their solutions. Some of these differentiating features are captured in the vendor profiles this year.

Those interested in purchasing an NGES solution must devise and prioritize a list of requirements and use cases that best fit their businesses, and use those criteria to differentiate among the available solutions.

Comments on Current Market Leaders and Contenders

Bromium has previously been a strong contender in Intel processor-based endpoint protection. However, it appears it has lost momentum over the last two years. It is not nearly as vocal at events and though it had a $40M USD series D-funding round in 2016, its price per share was simultaneously cut from $2.95 USD to $1.22, indicating lower than expected/projected growth. It did not participate in this report, so EMA was not able to get all of the information necessary to fully determine their state.

Key Market Vendors

Carbon Black was the market leader in the 2014/2015 report for both licenses and revenue. It was able to maintain position in licenses, but slipped in revenue. It experienced a significant metamorphosis over the last few years by combining technologies from Bit9, Carbon Black, and Confer. It will continue to push the market and its competitors to maintain pressure. The combination of technologies and push into the cloud expanded it far beyond what it once was and provided a layered defense model.

Cisco had a healthy market share in both reports. Its integrated strategy to leverage its network prowess and market penetration to combine system and network telemetry is very compelling to those that have a Cisco infrastructure. Its approach is evolving to resemble more of an advanced breach detection provider than an endpoint security provider. EMA will continue to track this evolution.

CrowdStrike has really put the pressure on to gain market share. Its growth curve significantly outpaced the incumbent leader to take over the top spot for market share based on revenue. The marketing and vocal partnerships CrowdStrike has created have really paid off.

Cylance has also been hitting the market hard to gain market share. Its growth curve significantly outpaced the incumbent leader bringing it within striking distance for both licenses and revenue. It has valuable technologies for defending against both file-based and file-less (memory-based) attacks and is leveraging those capabilities with key endpoint hardware vendors such as Dell. Given its market pressure and partnership it is a strong contender for first place in the next report.

Malwarebytes grew significantly in the last two years, emerging as a well-known but relatively small player. It was well-known in IT and security circles due to its freemium model, which gave it significant momentum on entering the commercial and enterprise markets. Since its entrance, it has been steadily evolving its protection portfolio and management capabilities, giving it an almost meteoric rise.

Symantec is committed to staying a viable option in the endpoint protection game and in taking a stand in the NGES market. As of SEP version 14, it has pushed forward by adding advanced prevention features found in the NGES market and elimination the need for signatures in its solution. Though it still provides signature-based defense for nuisance threats, it relies on cutting edge techniques using machine-learning and other approaches to identify system-focused attacks as early in the attack chain as possible.

Because of its already massive market footprint its growth for new customers is only in the single digits. However, the adoption of SEP14 within its client base has been significant. As of the close of data collection, it had the fastest adoption rate of a new version of SEP in the companies history. Symantec should not be discounted in its efforts to stay in the endpoint protection game and become the name in NGES protection as it has in antivirus. SEP14 has also addressed a number of previous customer complaints including agent configuration complexity and EMA is told more are coming.

Tanium is still a bit of an anomaly. It made a name for itself in the operations area, providing great insights on endpoints, and has definite security use cases. It is based on a polling architecture to gather information parallel from those endpoints, so it lacks the true proactive and defensive nature of an NGES solution. It has become a measuring stick for performance and delivery of endpoint operational intelligence and for other tools attempting to perform similar functions. As it stands today, within the currently forming Syssecops category, Tanium is the gold standard that others judge solutions by.

Vendors to Watch

Comodo has been in the consumer endpoint protection business for over 10 years but only entered the enterprise NGES space in 2014. Due to its size and market exposure from its consumer endpoint and certificate authority business lines, it has an excellent transition opportunity from both brand recognition and funding perspectives. They promote default deny security posture with default allow usability and currently have more than 87 million endpoints with no endpoint infections or security breaches reported thus far.

Digital Immunity, coming out of nowhere, is set to impress. Though only emerging in 2016, solution development started in 2007. Its approach is different than any of the major competitors in the space and as such should be able to compete with the largest of them given a little time to get itself off the ground. (see the Digital Immunity vendor profile for more details on the solution.

Minerva Labs also has a very unique approach to endpoint defense. Instead of attempting to directly block access to suspicious files or terminate processes, it intercepts OS calls that malware might use to evade existing security tools. Minerva returns a fictitious responses that results in the malware electing to terminate itself or to stop working because it believes it is in an inhospitable environment. (For example, Minerva can simulate the presence of forensics tools, insufficient resources for malware to operate, or even that there is a duplicate copy of the malware already on the endpoint.)

Nyotron is a very new entrant into the NGES foray. Its approach is very different than others in the market. It states that the way to get into a system are infinite but the interfaces to compromise and cause damage are finite so it monitors those interfaces for activity. This combined with behavioral analytics makes for a formidable defense. (See the Nyotron profile page for more details.)

Analyst Notes

1. Some organizations chose not to fully respond to the questionnaire based on company policies or other situations. A few chose not to participate, and several vendors failed to respond at all to numerous requests. Non-responsive vendors do not have a profile included. If information was not provided to EMA, then certain aspects of the profile will be marked as "No Data Provided" or "Information Unavailable," identified in their profile.
2. An attempt was made to include all relevant vendors. However, EMA recognizes that some smaller vendors may have been missed in the research process and not included in the report. EMA believes that those missed vendors, should they exist, would not make a significant impact on the estimates. The forecasts made attempt to accommodate for this situation.
3. An invitation to participate in the research project included the major antivirus companies serving the commercial markets that also claim some form of next-generation endpoint security to try to understand how their solutions qualify for the report. These vendors include (in alphabetical order): Avast, Comodo, Kaspersky, McAfee, Sophos, Symantec, and Trend Micro. This year's report included more information from Symantec and Sophos, while the others still refrained from participation. Because of the lack of response, EMA was unable to render a full decision on these vendors' ability to deliver next-generation endpoint protection, so the companies were excluded. EMA hopes more of these vendors will participate in future iterations of this report.

Vendor Profile Next Page

2017 Next-Generation Endpoint Security Vendor Landscape and Five-Year Market Forecast - SYMANTEC

Symantec

Symantec has really responded to its customers and the marketspace for next-generation endpoint protection. Over the course of the last few years, Symantec Endpoint Protection (SEP) pushed changes in the product. They moved from signature-based to a signature-based hybrid, which was signature defense with some advanced techniques to an advanced protection hybrid.

Without a doubt, Symantec has invested heavily in a multifaceted, hybrid approach. They poured significant resources into SEP14. SEP14 is their first release, relying on advanced techniques for the bulk of detection and prevention with signatures taking a backseat and being used for the quick-hit nuisance threats. The hybrid approach works well because evaluating incoming threats against known signatures is a relatively low resource task, while using more advanced methods has higher system resource utilization.

Its in-house integrations with Bluecoat WSG and acquisitions like Fireglass create additional layers of protection before malware even makes it to the endpoint, complementing the strength of SEP14 and creating a broader protection portfolio. SEP14 provides a complete next-generation endpoint security platform to prevent advanced targeted attacks across traditional endpoints, mobile devices, embedded devices, servers, and cloud workloads. APIs are provided to integrate with other security infrastructure such as Proxies, IT ticketing systems, and SIEMs to strengthen an organization's overall security posture. Symantec ATP (Advanced Threat Protection) is its endpoint detection and response (EDR) solution, which leverages the same endpoint client as SEP14 to solve for endpoint-based incident investigation and response.

SEP14 includes a comprehensive set of technologies against every phase of the attack chain, from incursion through infestation and exfiltration. Protection includes (but is not limited to) memory exploit mitigation, browser protection (via host IPS), application and device control (whitelisting, blacklisting, and isolation), reputation analysis (using artificial intelligence techniques in the cloud), advanced machine learning (to detect and prevent malware variants in the pre-execution stage), device control, and virtual sandbox emulation (to detect polymorphic and custom-packed malware).

Category: Prevention, Detection, and Response for Windows (NT-10), Mac OS, Red Hat Linux, CentOS, Oracle Linux, SUSE Linux, Amazon Linux, Ubuntu, VMWare ESX, Solaris, AIX, and HP-UX. SEP Cloud also supports iOS and Android.

Entered Enterprise Market: 2008/ 2016 for SEP14

2016/2017 Company growth: 2% overall (SEP14 adoption 9% of customer base in two months)

2016/2017 Rank by largest single deployment: #1

2016/2017 Market share by licenses sold: 18%

2016/2017 Rank by licenses sold: #1

2016/2017 Market share by revenue: 11% (SEP14 only)

2016/2017 Rank by market share: 4 (SEP14 only)

Analyst Notes:

SEP14 supports the broadest range of operating systems and platforms of any vendor in the report. Customer adoption of SEP14 is the most rapid of any version release in Symantec history and is receiving excellent feedback from administrators and users alike, making it not only a viable competitor, but a market leader in the NGES space.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3708.092117