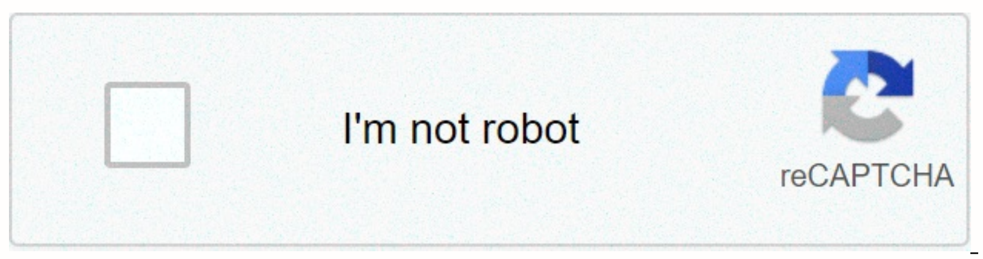
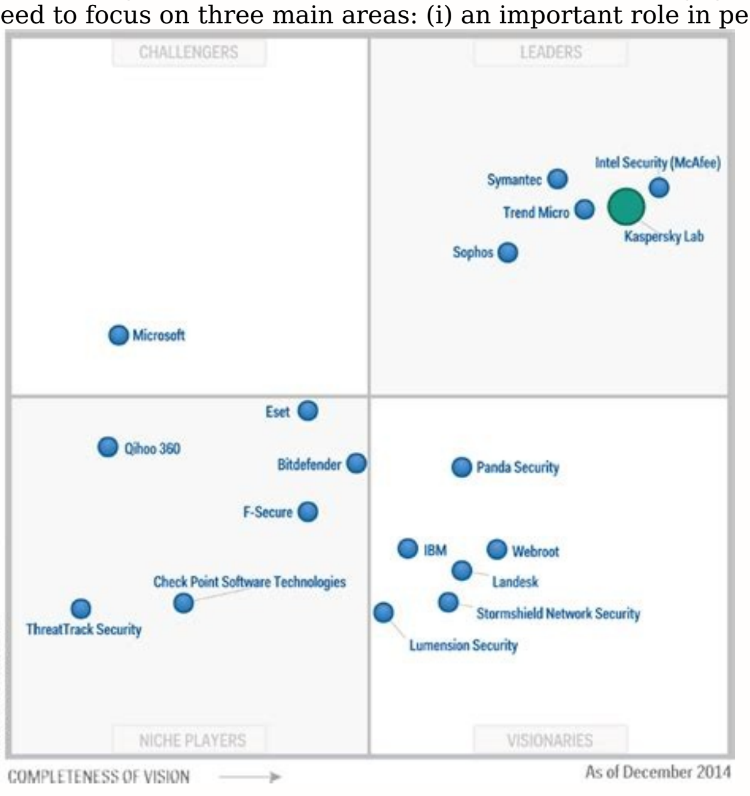

□
I'm not robot
reCAPTCHA

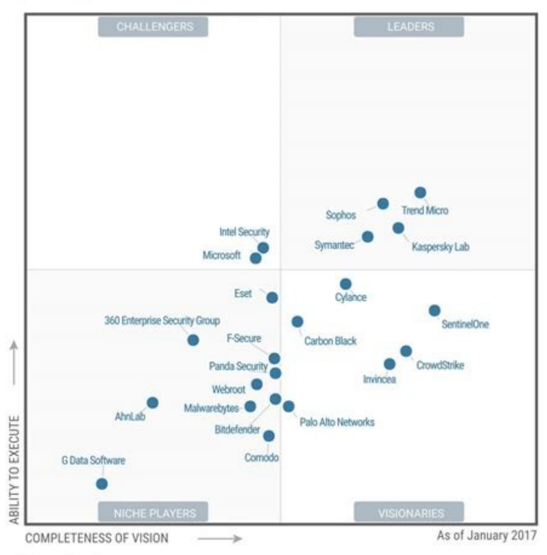
Gartner magic quadrant 2022 endpoint protection

1-20 products were released: 2021. May 5 Summary in this magical quadrant has evaluated innovations that allow companies to protect the company's final points from attacks and violations. Technology and practice in this area are formed in two trends: continuous growth and hiding attacks to final points and sudden increases in the number of work removed. The reviews presented throughout the summary study of what he likes and what he does not like must rethink the security manager (SRM) how to compensate for investment in technology and elements that focus on people cybersecurity is essential to limit security gaps, "he said Richard Addiscott, Senior Director of Gartner. "If you focus on the design and implementation of people who are engaged in control mechanisms, as well as business communication and cybersecurity talent management will help to improve business risk solutions and deal with staff working with cyber security. "To face threats to cyber security and maintain an effective cybersecurity program, SMM leaders need to focus on three main areas: (i) an important role in people successfully and durability security programs; ii) technical security capabilities that provide greater visibility and flexibility throughout the organization Digital ecosystem; and (III) security functions to ensure flexibility without safety.



These nine trends will have a major impact on SMM leaders in these three areas: 1 Trend: Security Design focuses on people. When designing safety projects that focus on people throughout the control management cycle. By 2027, 50% of the cysses in large companies will accept security design practices that focus on people to reduce rubbing through cybersecurity and maximize the implementation of control mechanisms.B'produkai 1-20 Published: 2021. May 5 In this Magic Quadrant evaluate innovations that enable companies to protect their business ends from attacks and security breaches. The technology and practices in this area are shaped by two trends: the continued increase in backpoint attacks and stealth attacks and the sudden increase in remote work. According to Gartner, Inc., security and risk management (SRM) must rethink its investment balance between technology and human-centered elements in accordance with nine-large industry trends. "The reduction of security failures requires a human -centered approach to cyber security," said Richard Addiscott, managing director at Gartner.

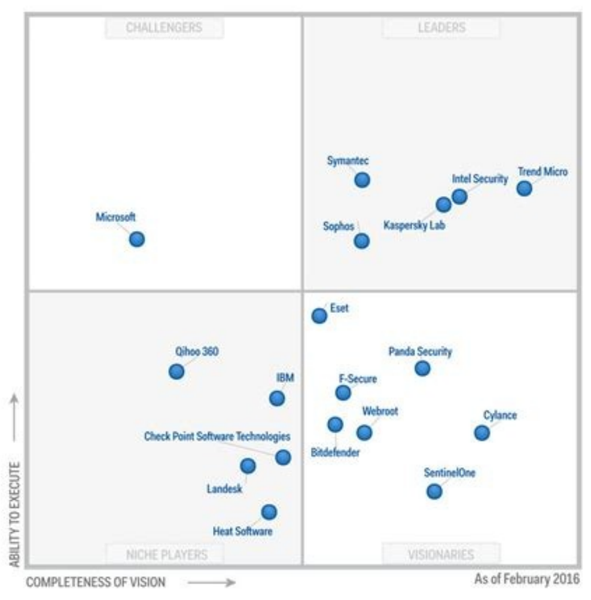
Figure 1. Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (January 2017)

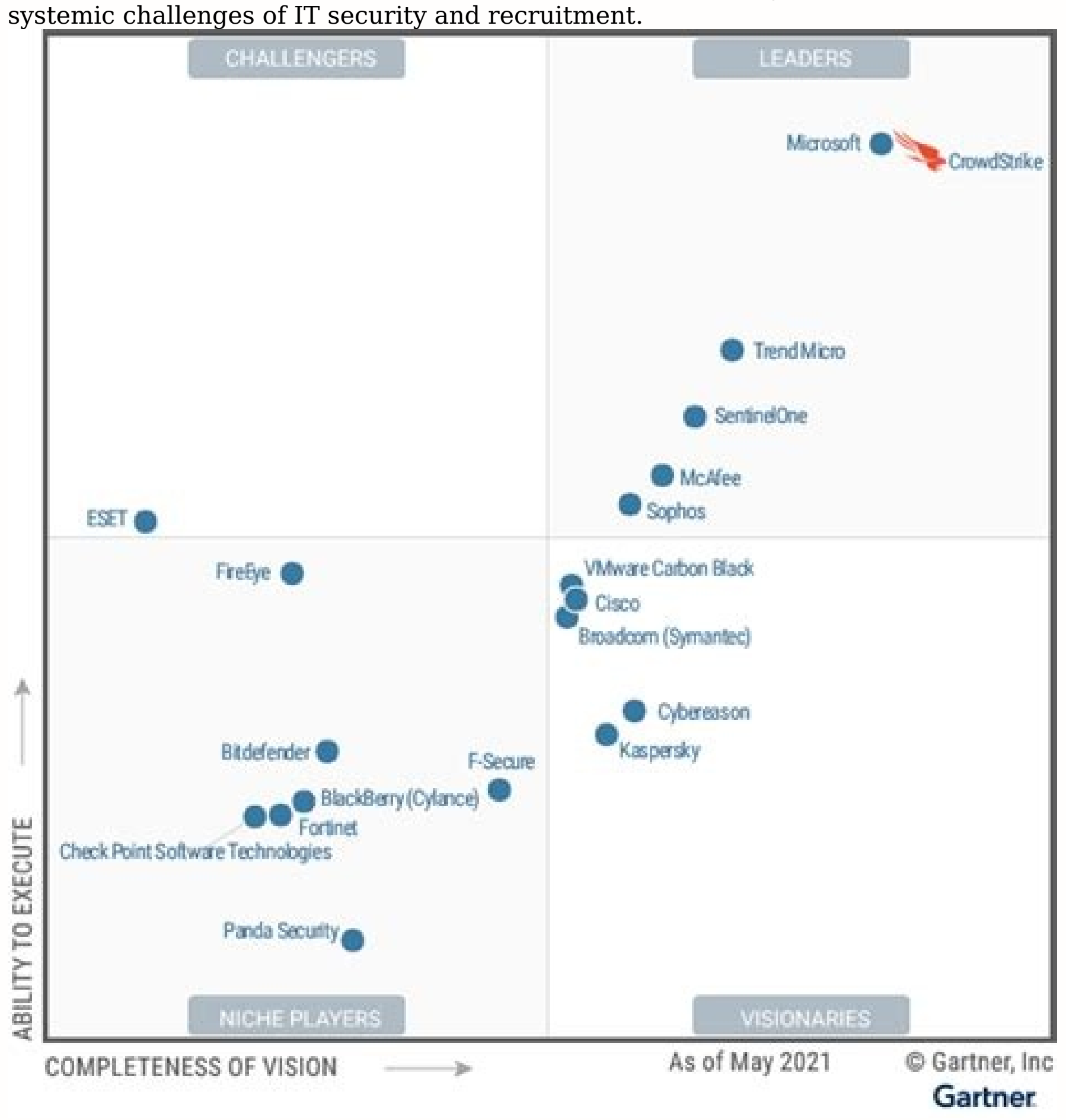
\ XE2 \ X80 \ X9CTime A focus on the development and implementation of controls as well as the use of corporate communication and cyber security talent management will help you to understand the crucial role that people play for the success and sustainability of security programs; (ii) Technical security functions that ensure greater visibility and faster reaction in the entire digital ecosystem of an organization; and III) Reorganization of the functioning of the security function to ensure mobility without impairing security. These nine trends will have a major impact on SMM executives in these three areas: Trend 1: A security design geared towards humans prefers the role of employee experience in the entire life cycle of management measures. By 2027, 50 % of the information security officers of large companies (CYSS) will be geared towards human -centered security design practices in order to reduce friction losses in cyber security and maximize control. \ XE2 \ X80Little attention is paid to people who create these changes.

Figure 1. Magic Quadrant for Endpoint Protection Platforms



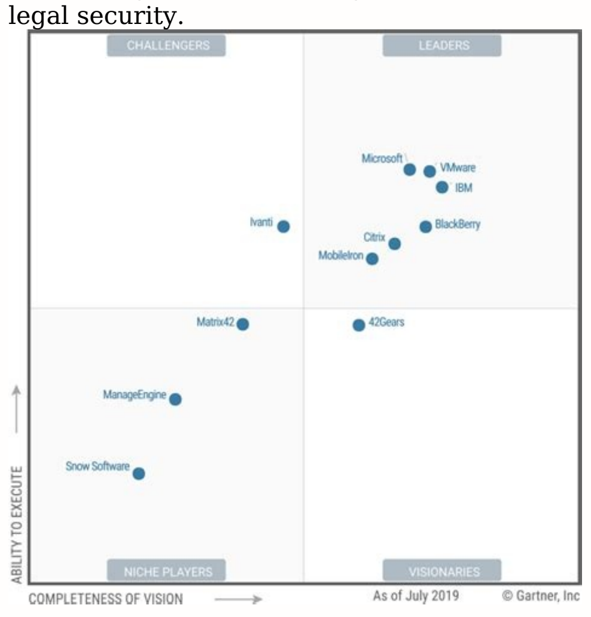
Source: Gartner (February 2016)

The ciso that use an approach focused on people to the management of talents to attract and retain talents have found improvements in their functional and technical maturity. Gartner provides for it by 2026 60% of the organizations will go from the external recruitment to the silent recruitment in the internal markets of talents to deal with the systemic challenges of IT security and recruitment.



Trend 3: Change the operating model of IT security to support the migration of technologies that create value from the main IT functions to business areas, company functions, teams and individual employees. An investigation by Gartner found that 41% of the workforce works in the technological sector, a number expected will continue to grow in the next five years. According to Addiscot, "corporate leaders now recognize amply that the risk of IT security is a key business risk when dealing with technology".

Supporting and accelerating business results is an absolute priority for IT security, but it remains an absolute priority. The Ciso must change their operational computer security model to integrate the way work is done. Employees must know how to balance the various risks, including those related to computer, financial, reputational, competitive or legal security.



Computer security must also be connected to the corporate value by measuring and reporting success with respect to the results and company priorities. Trend 4: management of the impact of threats. The attack surface of today's companies is complex and exhausting. Ciso must improve their evaluation practices to understand the threat through continuous CTEM (Three Exposure Management) programs. Gartner provides for it by 2026, the organizations that give priority to investment safely through the CTEM program will undergo two thirds of violations less. Cisos must continuously evolve his methods of assessing threats to keep up with his own organization, using a CTEM approach to evaluate beyond technology.So," Adiscott said. Trend 6: Cybersecurity Confirmation combines methods, processes and tools used to confirm how potential attackers use the threat. Cybersecurity Approved Measures Make Great Progress in Automating Repetitive Assessment Aspects and expected ones that enable regular attacks, security controls and processes. By 2026 More than 40% of organizations, including two-thirds of medium-sized enterprises, will have consolidated revenue cybersecurity approval platforms. Trend 7: Platform consolidation For organizations that are looking to streamline operations, vendors combine platforms in one or more cybersecurity areas. For example, Identity Security Services can be offered through a common platform that combines audit, privileged access, and management functions. of access. SMM drivers must constantly record security audits to understand where there are coincidences and reduce duplication with established platforms. Trend 8: Connected businesses need security.

Organizations must move from relying on monolithic systems to modular opportunities to develop their programs to respond to rapid business changes. Security stacking is a method in which cybersecurity controls are integrated into architectural models and are used to implement technology at the module level. By 2027 More than 50% of core core programs will be created using composite architecture and will require a new approach to delivering these programs. "Folding protection is designed to protect the folding business," Addiscott said. When developing applications, м with composite components, indecisive dependencies arise. CYRs are an important opportunity to integrate privacy and security into the creation of a security object based on reusable components."When deciding on cyber security," Addiscott said. "To serve as a strategic advisor and give recommendations on the activities that the Governor's Council is to perform, including budget allocation and security resources." Gartner clients can read more in "Top Cyber Security Trends 2023". Read about the main priorities of security and risk workers in 2023. The free e-mail book of Gartner: Visions for leadership for 2023 for leaders in risk and risk management. Gartner Security & Risk Management Summitics Gartner Peak will provide the latest surveys and councilors to the Gartner Security & Risk Management Summit Summit & Risk Management, which will take place on June 5 to 7. In National Harbor, Maryland, 26/26-28 July. in Tokyo and from 26 to 28 September. in London.

Follow news and updates from the Twitter conference using #gartners. Gartner information for cyber security leaders provides cyber security executives to managers in the field of role transformation, harmonization of security strategies with business objectives, and creating programs that harmonize security with the needs of the organization. For more information, visit . Follow the Gartner and Twitter and LinkedIn and get updates from the leaders in the Cyber Security area using the #gartnersec hashtag. Visit Gartner Newsroom to find more information and insights. Observation.