



FROM PERIMETER TO DATA:

The five layers of cyber security

With more and more devices, cars, homes and – not least – production and manufacturing processes being connected to the internet, businesses and individuals are increasingly exposed to cyber-risks and vulnerable to cyber-attacks. This growing need for protection means a requirement for more sophisticated approaches to cyber security – something that is providing attractive opportunities for investors to participate in the growth prospects of companies at the forefront of these developments. Indeed, the layered approach that this article discusses has proven to be the most effective as malefactors only need to be right once, while security professionals – and the organisations they protect – need to be right all the time.



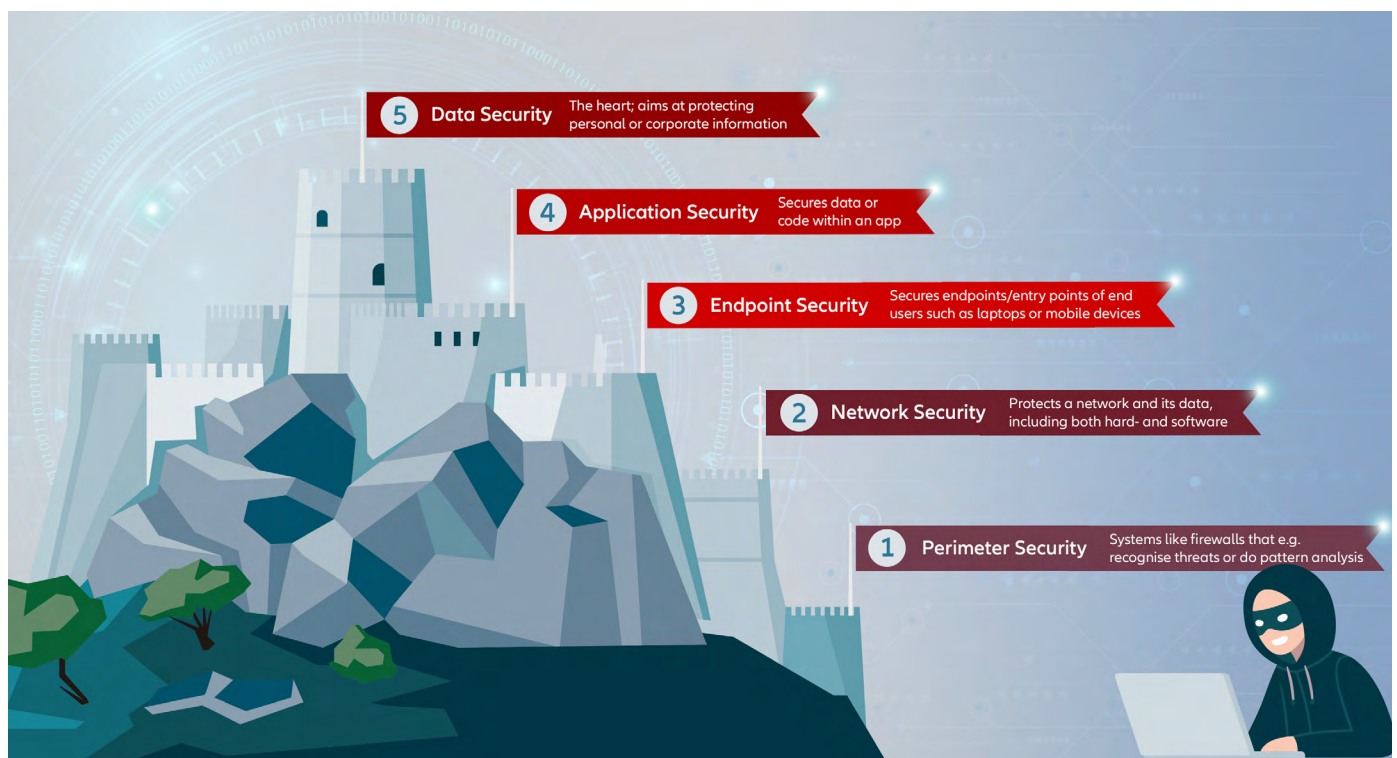
Johannes Jacobi
Senior Product
Specialist
Global Investment
Platform

Perimeter security: the first line of defence

Perimeter security has traditionally been synonymous for firewalls; i.e., the protection of data and systems by filtering out potentially dangerous or unknown traffic. With the growing ubiquity of the cloud and remote access, perimeter security solutions – once designed to locally manage and protect local networks - must now adapt to this new and more complex landscape.

The transformation of network security defence

Network security covers both hardware and software technologies, and processes and devices that protect a network and its data from harm. Again, the expansion of the cloud and working from home/anywhere are fundamentally changing the landscape here; networks now also include the path to the cloud and hybrid infrastructures that may consist of on-premises data centres, public/private cloud instances, and SaaS applications.



Perimeter and network security

With an increasing use and a deeper integration of cloud technologies into business processes and with the establishment of flexible work models (on-site, remote and hybrid), many organizations are struggling with more complex network and data vulnerability issues. Innovators in this sector are thus rethinking established security concepts and developing new models. For instance, Zscaler and CrowdStrike have developed a solution based on the idea of “zero trust”, where user identity, device posture (i.e., a device’s security credentials), and access policies are used to grant or withhold access rights. These risk-based conditional access solutions help steering a multitude of individual access requirements from users by detecting in real time possible threats which may arise when identities don’t match with corresponding access rights. This, in turn, protects complex and thus more vulnerable IT environments from breaches.

Endpoint security: where a network’s safety begins

The growing use of the cloud is also resulting in profound changes in how endpoints – i.e., any device that is connected to the network and can communicate both ways – should be protected from cyberattacks. Indeed, malicious actors now often target the vulnerability of endpoint devices to get access to a network while, until relatively recently, they would have focused on breaching perimeter security.

Given the increasing proliferation of devices connected to organization’s networks, the growth of the “internet of things” (IoT), and the unique risks associated with “bring your own device” (BYOD) policies, endpoint security is likely to represent a particularly strong growth area for the foreseeable future. Indeed, some estimates suggest that the endpoint security market will grow at a CAGR of 8.3% by 2028, reaching a value of USD 24.58 bn.¹

Endpoint security

Formed in 2011, CrowdStrike has developed a comprehensive endpoint security offering comprising of a range of unified modules to prevent breaches. Their Falcon platform collects cyber security data – processing over 6 trillion events per week² – and leverages AI to constantly improve its performance and deliver one of the highest detection and efficacy rates in the industry.

The company’s annual recurring revenue grew by 48% year-on-year to exceed 2.5 billion, as of January 31, 2023.³

Endpoint security market: projected market CAGR of 9.4% by 2026, reaching a value of USD 22 billion⁴

Application security: defending apps and users

Application security is as multifaceted as applications themselves. It includes not only the procedures used to protect websites and apps while in use, but also those used during their development and design.

Again, the rise of the cloud is changing the game here. With more and more organizations hosting resources in this way, application security is becoming ever more complex. Recent research suggests that the global application security market will experience a CAGR of 18.30% by 2028 reaching a value of USD 22.54 bn, up from USD 6.95 USD bn in 2021.⁵

Application security

One of the leaders in a range of cyber security areas and disciplines, Zscaler's "Private Access" (ZPA) solution applies the principles of zero trust and segmentation to give users secure and direct connectivity to apps while eliminating unauthorized access via "zero trust network access" (ZTNA). ZPA is currently the world's most deployed ZTNA platform⁶, and this model is expected to become dominant in the coming years – Gartner predicts that, by 2025, over 70% of remote access deployments will use ZTNA⁷.

Application security – projected market CAGR of over 18% by 2028, reaching a value of USD 22.54 billion⁸

Data security: the heart of protection

The protection of data across platforms and applications connected to an organization's network is often considered the paramount discipline of cyber security. The safeguarding of data is vital for every enterprise as many companies base their processes and business models on the storage, transmission, and, not least, the monetarization of gathered internal and external data. Indeed, the consequences of breaches in this respect present one of the greatest risks to companies and other organisations in terms of potential liability and reputational damage.

Data security

According to Cowen Research and Boston Consulting Group, the "human element" is responsible for at least three quarters of cyber breaches. Issues here include, for example, users failing to follow security protocols or becoming victim to deceptive communications or other forms of social engineering. For this reason, security awareness training and technologies that identify and detect threats more efficiently remains key to limiting such breaches. Microsoft offers a variety of security solutions that help its customers keep data safe from attacks. One of the company's new solutions is the Copilot product, which allows security teams to detect hidden patterns and respond to incidents faster with generative AI. Microsoft is a leader in cyber security and continues to develop innovative solutions to secure critical data. We see this segment as an important driver to the company's long-term growth.

Allianz Global Investors identifies first movers in cyber security

When it comes to cyber security, it is vital for companies to stay a step ahead of malicious actors. Cybercrime is, and will continue to be, a difficult-to-assess risk. Leading companies providing solutions in this area are thus likely to benefit from the growing need for holistic cyber security approaches – a need that will only become more pertinent, and complex to address, in the coming years.

Allianz Global Investors identifies innovators and first movers in cyber security across the full range of cyber security solutions, especially those that provide innovative solutions to protect applications, organizations, and users in complex cloud environments.



1. <https://www.globenewswire.com/news-release/2023/01/20/2592453/0/en/endpoint-security-market-size-worth-usd-24-58-billion-by-2028-report-by-fortune-business-insights.html>
2. <https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/>
3. <https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-fourth-quarter-and-fiscal-year-2023/>
4. <https://www.prnewswire.com/news-releases/endpoint-security-global-market-report-2022-sector-to-reach-22-billion-by-2026-at-a-cagr-of-9-4-301712341.html>, as of March 2023
5. <https://www.vantagemarketresearch.com/industry-report/application-security-market-1406>, as of June 2022
6. <https://www.zscaler.com/products/zscaler-private-access>
7. <https://www.datacenterknowledge.com/security/gartner-zero-trust-will-replace-your-vpn-2025>, as of October 2022
8. <https://www.vantagemarketresearch.com/industry-report/application-security-market-1406>, as of June 2022
9. <https://www.knowbe4.com/en/products/enterprise-security-awareness-training/>

Investing involves risk. The value of an investment and the income from it will fluctuate and investors may not get back the principal invested. Past performance is not indicative of future performance. This is a marketing communication. It is for informational purposes only. This document does not constitute investment advice or a recommendation to buy, sell or hold any security and shall not be deemed an offer to sell or a solicitation of an offer to buy any security.

The views and opinions expressed herein, which are subject to change without notice, are those of the issuer or its affiliated companies at the time of publication. Certain data used are derived from various sources believed to be reliable, but the accuracy or completeness of the data is not guaranteed and no liability is assumed for any direct or consequential losses arising from their use. The duplication, publication, extraction or transmission of the contents, irrespective of the form, is not permitted. This material has not been reviewed by any regulatory authorities. In mainland China, it is for Qualified Domestic Institutional Investors scheme pursuant to applicable rules and regulations and is for information purpose only. This document does not constitute a public offer by virtue of Act Number 26.831 of the Argentine Republic and General Resolution No. 622/2013 of the NSC. This communication's sole purpose is to inform and does not under any circumstance constitute promotion or publicity of Allianz Global Investors products and/or services in Colombia or to Colombian residents pursuant to part 4 of Decree 2555 of 2010. This communication does not in any way aim to directly or indirectly initiate the purchase of a product or the provision of a service offered by Allianz Global Investors. Via reception of his document, each resident in Colombia acknowledges and accepts to have contacted Allianz Global Investors via their own initiative and that the communication under no circumstances does not arise from any promotional or marketing activities carried out by Allianz Global Investors. Colombian residents accept that accessing any type of social network page of Allianz Global Investors is done under their own responsibility and initiative and are aware that they may access specific information on the products and services of Allianz Global Investors. This communication is strictly private and confidential and may not be reproduced. This communication does not constitute a public offer of securities in Colombia pursuant to the public offer regulation set forth in Decree 2555 of 2010. This communication and the information provided herein should not be considered a solicitation or an offer by Allianz Global Investors or its affiliates to provide any financial products in Brazil, Panama, Peru, and Uruguay. In Australia, this material is presented by Allianz Global Investors Asia Pacific Limited ("AllianzGI AP") and is intended for the use of investment consultants and other institutional /professional investors only, and is not directed to the public or individual retail investors. AllianzGI AP is not licensed to provide financial services to retail clients in Australia. AllianzGI AP is exempt from the requirement to hold an Australian Foreign Financial Service License under the Corporations Act 2001 (Cth) pursuant to ASIC Class Order (CO 03/1103) with respect to the provision of financial services to wholesale clients only. AllianzGI AP is licensed and regulated by Hong Kong Securities and Futures Commission under Hong Kong laws, which differ from Australian laws.

This document is being distributed by the following Allianz Global Investors companies: Allianz Global Investors GmbH, an investment company in Germany, authorized by the German Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin); Allianz Global Investors (Schweiz) AG; in HK, by Allianz Global Investors Asia Pacific Ltd., licensed by the Hong Kong Securities and Futures Commission; in Singapore, by Allianz Global Investors Singapore Ltd., regulated by the Monetary Authority of Singapore [Company Registration No. 199907169Z]; in Japan, by Allianz Global Investors Japan Co., Ltd., registered in Japan as a Financial Instruments Business Operator [Registered No. The Director of Kanto Local Finance Bureau (Financial Instruments Business Operator), No. 424], Member of Japan Investment Advisers Association, the Investment Trust Association, Japan and Type II Financial Instruments Firms Association; in Taiwan, by Allianz Global Investors Taiwan Ltd., licensed by Financial Supervisory Commission in Taiwan; and in Indonesia, by PT. Allianz Global Investors Asset Management Indonesia licensed by Indonesia Financial Services Authority (OJK).