A Comprehensive Technical Survey of Contemporary Cybersecurity Products and Solutions

Christos Tselios[1(✉)], George Tsolis[1], and Manos Athanatos[2]

[1] Citrix Systems Inc., Patras, Greece
[2] Foundation for Research and Technology - Hellas (FORTH), Heraklion, Greece
{christos.tselios,george.tsolis}@citrix.com

Abstract. As the complexity of applications and software frameworks increases, cybersecurity becomes more challenging.The potential attack surface keeps expanding while each product has its own peculiarities and requirements leading to tailor-made solutions per case.These are the primary reasons which render security solutions expensive, highly complex and with significant deployment delay. This technical survey intends to reveal the pillars of today's cybersecurity market, as well as identify emerging trends,key players and functional aspects. Such an insight will allow all interested parties to optimize the design process of a contemporary and future-proof cybersecurity framework for end-to-end protection.

Keywords: Cybersecurity · Optimization · Market analysis

1 Introduction

As the complexity of applications and software frameworks increases, cybersecurity becomes more challenging [5]. The attack surface keeps expanding while each product has its own peculiarities and requirements leading to tailor-made solutions per case. This is the primary reason which renders security solutions expensive, highly complex and with significant deployment delay. Larger companies are willing to pay the protection premium since a potential breach could have severe economical and reputational impact. Alas, small-medium enterprises (SMEs) and public administrations with limited budget are generally reluctant to invest in cybersecurity. They plan and operate without thinking about security, designing new services and products with two main objectives in mind: time to market and cost minimization.

The most important factor to boost cybersecurity in SMEs, public administrations and organizations with restricted budget in general, is to link it with its economic impact and the market that is forming around it. One must admit that, in most cases, cybersecurity is promoted with no economic impact. And even though all companies agree that boosting their security will eliminate service disruption and data recovery costs, the truth is that the majority would

A. P. Fournaris et al. (Eds.): ESORICS 2019 Workshops, LNCS 11981, pp. 3–18, 2020.
https://doi.org/10.1007/978-3-030-42051-2_1

be more interested in advancing their security methods if they could identify opportunities for additional economic profit (e.g. new services, clients, markets etc.). This technical survey intends to reveal the most important cybersecurity market pillars, identify emerging trends in cybersecurity and identify key players and performance capabilities. Such an insight will allow all interested parties to optimize the design process of a contemporary and future-proof cybersecurity solution and will also shed some light on how the integrated framework of the SMESEC Project [4] intends to deliver end-to-end cybersecurity protection.

Cyber-attacks become more and more sophisticated, rendering legacy solutions no longer adequate for today's systems and services. Cybersecurity solutions evolve and become more "intelligent" with technologies like machine learning, statistical analysis, user behavioral analysis etc. but these solutions are offered to closed standalone products. This consortium argues that the complexity of managing cybersecurity world cannot be one man's job. Not all products can address or have the optimal solutions for all the different cases of cyber-attacks (viruses, malware, ransomware, intrusion detection, DDoS etc.). A proper framework must be able to adopt the latest innovations by integrating products (not only from security) with focused solutions from different providers very fast and considerably easy.

2 Identifying Imperative Cybersecurity Market Segments

Cyber-protection is a constant circular process which can be described in the following high level steps: (i) perform a risk assessment, (ii) develop a security plan, (iii) deploy the right defenses, (iv) monitor and (v) re-perform risk assessment. It is clear that this process is expensive and time consuming. Current solutions offered by security companies are off-the-shelf products charged by the number of protected end-devices and cannot be easily modified to accommodate the specific needs of small businesses. In addition, steps like risk assessment and security plan deployment are not always included and SMEs need to (a) evaluate and integrate extra modules thus increasing the overall cost or (b) settle with a product which might not be the optimal solution for their use cases. It is therefore important to take a step back and identify, categorize and analyze some important existing and upcoming security market segments, along with the key players and dominant products in each case.

2.1 Contemporary Security Market Segments and Related Products

Encryption refers to the process of protecting sensitive data by converting to an encoded form that can be decrypted by means of a protected key. This method ensures that even if security is breached in other levels, data will still be highly protected and will be useless to any malicious user. In fact, encryption is one of the first requirements when it comes to protecting sensitive data. Apart from the key players and proprietary solutions presented in Table 1, there is a wide range of open source solutions which cover different aspects like file, filesystem, and

network encryption such as VeraCrypt[1] and CryptTool[2]. None of the SMESEC contributed products is now directly related to the encryption market, thus it makes this particular market attractive for adding the specific capabilities to the SMESEC.

Symantec[3] is a key player in the specific domain with an encryption portfolio that includes endpoint, file and folder and email encryption. Integration with Symantec Data Loss Prevention automatically encrypts sensitive data being moved onto removable media devices or residing in emails and files. Robust management features include individual and group key management, automated policy controls, and out-of-the-box, compliance-based reporting. Heterogeneous management capabilities include support for native OS encryption (FileVault2) and Opal compliant self-encrypting drives. Sophos[4] introduces the most complete data protection solution on the market today, protecting data on multiple devices and operating systems. Whether data resides on a laptop, a mobile device, or being collaborated upon via the cloud or other file sharing method, SafeGuard Encryption is built to match organizational workflow and processes without slowing down productivity.

Table 1. Encryption-related solutions

Kaspersky Lab	Kaspersky Endpoint Security offers data encryption with highly integrated security policies that can be aligned with application and device controls for data protection in case devices or files are lost or stolen
Symantec	Symantec's encryption portfolio includes endpoint, file/folder and email encryption. Integration with Symantec Data Loss Prevention automatically encrypts sensitive data being moved onto removable media devices or residing in emails and files
McAfee, Inc.	McAfee Complete Data Protection secures critical data on endpoint devices with powerful enterprise-grade drive encryption. This endpoint encryption suite also enables management of native encryption on Macs and Windows systems

Governance, Risk Management and Compliance (GRC) create an acronym often used to describe the organization efficiency to achieve its objectives, address uncertainty and act with integrity. In these three terms, (i) Governance refers to the processes involved to assure that the organization handles information properly across all workflows, (ii) Risk Management stands for predicting and handling possible risks that may slow the organization achieving the goals and (iii) Compliance includes all the processes to adhere with laws and regulations, as well as company policies.

[1] https://www.veracrypt.fr/en/Home.html.
[2] https://www.cryptool.org/en/.
[3] https://www.symantec.com/products/endpoint-encryption.
[4] https://www.sophos.com/en-us/products/safeguard-encryption.aspx.

This market segment covers some security aspects that usually SMEs neglect to address, for instance who has the rights to the obtained datasets, whether datasets adhere to company or other legal compliances, and how to deal with issues identified through the initial risk management process. This kind of services often comes on top of other first level security solutions, and SMESEC aims to address this space as well.By collecting traffic, usage, and other data from the underlying infrastructure (firewall, antivirus, etc.) the integrated framework can re-assess the risk periodically, whereas the overall architecture should take into account general governance and compliance constraints (Table 2).

Table 2. Key players in the GRC domain

RSA Security LLC (part of EMC)	RSA Archer eGRC Solutions allows developing an efficient, collaborative enterprise governance, risk and compliance (eGRC) program across IT, finance, operations and legal domains. These solutions include policy, risk, compliance, enterprise, incident, vendor, threat, business continuity and audit management
IBM Corporation	The IBM OpenPages GRC Platform delivers a modular platform for intrinsic GRC, enabling businesses to deploy scalable solutions for managing enterprise-wide risk and compliance. Designed for increasing overall productivity and efficiency, the platform supports agile implementation for rapid time to value
MetricStream	MetricStream offers an advanced and comprehensive IT GRC software solution for streamlining IT GRC processes, effectively managing IT risk, and meeting IT regulatory requirements. The MetricStream solution enables companies to implement a formal framework to rigorously measure, mitigate, and monitor IT risks
Galvanize	Galvanize's software helps organizations successfully manage risk, compliance, audit, and security needs effectively. The available platform provides the most intuitive and flexible solutions for GRC, security risk intelligence, vendor/third-party risk management, KPI/KRI metrics, and on-demand applications

Security Information and Event Management (SIEM) is a technology that enables the aggregation of data produced by multiple devices, network infrastructure, systems, and applications. Data logs may be the primary source of information but SIEM systems are able to absorb and identify other complex data structures as well. These characteristics, allow SIEM systems not only to monitor systems and users but also comply with policies and standards as well.

Undoubtedly, SIEM is a key component in a security solution, especially when multiple products are involved. The ability of SIEM products to ingest large amounts of heterogeneous data from several sources, correlate, create and visualize insights, makes it indispensable component in a security architecture (Table 3).

Table 3. Key players in the Security Information and Event Management domain

Microfocus	The ArcSight SIEM by Microfocus is s comprehensive solution that enables cost-effective compliance and provides advanced security analytics for identifying threats and/or risk management
McAfee, Inc.	McAfee Enterprise Security Manager brings event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and compliance reporting–delivering the context required for adaptive security risk management
LogRythm Inc.	LogRhythm's security intelligence and analytics platform enables organizations to detect, prioritize and neutralize cyber threats that penetrate the perimeter or originate from within
Splunk Inc.	Splunk's Security Intelligence Platform, combines Splunk Enterprise and Splunk App for Enterprise Security, to offer an overview of all existing data threats
RSA Security LLC (part of EMC)	RSA NetWitness Logs and Packets goes beyond baseline SIEM capabilities. Designed for scale and heavy analytic loads, the product will spot sophisticated attacks and will prioritize alerts

Intrusion Detection and Prevention Systems (IDS/IPS) implement threat deterrent technologies which monitor live network traffic [2] to detect and prevent vulnerabilities [3], based on a given set of rules. Besides the proprietary solutions presented in Table 4 there are some popular open-source solutions such as Suricata[5] and Snort[6].

Table 4. Dominant IDS/IPS solutions and key players

Cisco Systems, Inc.	The Cisco FirePOWER Next-Generation IPS (NGIPS) solution offers advanced threat protection by integrating real-time contextual awareness, intelligent security automation and superior performance
IBM Corporation	IBM Security Network Intrusion Prevention System appliances are designed to stop constantly evolving threats before they impact your business. This means providing both high levels of protection and performance, while lowering the overall cost and complexity associated with deploying and managing a large number of point solutions
Trend Micro, Inc.	The TippingPoint Next-Generation Intrusion Prevention System (IPS) offers comprehensive threat protection against advanced and evasive targeted attacks with high accuracy. Using a combination of technologies such as deep packet inspection, threat reputation, and advanced malware analysis. It provides enterprises with a proactive approach to security

[5] https://suricata-ids.org/.
[6] https://www.snort.org.

Distributed Denial-of-Service (DDoS) refers to attacks from multiple sources to a single target in order to make it unable to provide a service by causing denial of service due to flooding by immense traffic. Such attacks directly affect the organization operations by denying access to legitimate users, therefore mitigation solutions have been developed, as shown in Table 5.

Table 5. Distributed DoS protection key players and products

Cloudflare Inc.	CloudFlare's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of DDoS threats and can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 attacks
Arbor (now part of NetScout)	Arbor Cloud is a DDoS service powered by the world's leading experts in DDoS mitigation, together with the most widely deployed DDoS protection technology
Verisign Inc. (now part of Symantec)	Verisign DDoS Protection Services help organizations reduce the risk of catastrophic DDoS attacks by detecting and filtering malicious traffic aimed at disrupting or disabling their internet-based services. Unlike traditional solutions, Verisign DDoS Protection Services filter harmful traffic upstream of the organizational network or in the cloud
Akamai	Kona Site Defender combines automated DDoS mitigation with a highly scalable and accurate WAF to protect websites from a wide range of online threats, including network- and application-layer DDoS, SQL injection and XSS attacks – without compromising the user experience. Kona Site Defender can stop the largest attacks and leverages Akamai's visibility into global web traffic to help organizations respond to the latest threats
Imperva	The Imperva Incapsula service delivers a multi-faceted approach to DDoS defense, providing blanket protection from all DDoS attacks to shield your critical online assets from these threats. Incapsula DDoS protection services are backed by a 24 $\times$ 7 security team, 99.999% uptime SLA, and a powerful, global network of data centers
F5 Networks Inc.	F5's DDoS Protection solution protects the fundamental elements of an application (network, DNS, SSL, and HTTP) against distributed denial-of-service attacks. Leveraging the intrinsic security capabilities of intelligent traffic management and application delivery, F5 protects and ensures availability of an organization's network and application infrastructure under the most demanding conditions

Web Application Firewall (WAF) differ from the typical firewall as they focus mainly on protecting the web traffic (HTTP protocol) from a variety of attacks, such as Cross-Site Scripting (XSS) or SQL injection. WAFs are able to inspect the payload of the HTTP traffic, decide if this is legit, and provide input to other tools like SIEMs.

Several businesses today depend on web applications due to platform independency, easy-of-deployment which together with the evolution of cloud computing [6] generated a whole new market. It is WAFs which protect these valuable applications and nullify attacks targeting other dependant assets (Table 6).

Table 6. Web Application Firewall solutions

Citrix Systems Inc.	Citrix ADC prevents inadvertent or intentional disclosure of confidential information and aids in compliance with information security regulations such as PCI-DSS[a]
F5 Networks Inc.	BIG-IP Application Security Manager is an on-premises web application firewall (WAF) with relatively advanced firewall. It secures applications against layer 7 distributed denial-of-service (DDoS) attacks and application vulnerabilities
Barracuda Networks Inc.	Barracuda Web Application Firewall is a solution for organizations looking to protect web applications from data breaches and defacement. With the Barracuda Web Application Firewall, administrators do not need to wait for clean code or even know how an application works to secure their applications. Organizations can ensure robust security with a Barracuda Web Application Firewall hardware or virtual appliance, deployed either on-premises or in the cloud

[a] https://www.pcisecuritystandards.org/

Secure Web Gateways (SWG) protect company assets while surfing and enforce the policy companies to the network traffic. They may offer a range of capabilities, including URL filtering, antivirus/antimalware protection, SSL traffic inspection, etc.

Secure Web Gateways can offer a wide range of protections for web traffic, covering not only incoming but outgoing traffic as well. Characteristics such as URL filtering or anti-malware protection can help into preventing malicious content and code entering the organization. The ability to inspect secure traffic makes it also attractive as much of the malware can be transported over secure web connections that otherwise pass uninspected (Table 7).

Table 7. Key players delivering Secure Web Gateway solutions

Symantec	Symantec Secure Web Gateway (previously Blue Coat SWG) consolidates a broad set of features to authenticate users, filter web traffic, identify cloud application usage, provide data loss prevention, deliver threat prevention, and ensure visibility into encrypted traffic
Zscaler	Zscaler Web Security provides security, visibility and control, going beyond the basics of web content filtering. Delivered in the cloud, Zscaler includes web security integrated with a robust network security platform that features advanced threat protection, real-time analytics and forensics
Cisco Systems Inc.	Get advanced threat defense, advanced malware protection, application visibility and control, insightful reporting, and secure mobility. The Cisco Web Security Appliance (WSA) combines all of these forms of protection and more in a single solution

Endpoint Security and Protection Platforms (EPP) intend to protect endpoints such as workstations, servers or mobile devices from viruses, trojans, spyware, malware, or phishing attacks.

EPP is one of the traditional markets in terms of awareness, as antivirus solutions used to be present in SME environments several years ago. The increasing complexity of viruses and malware today, rendered these solutions even more necessary, and the integration with other security products is definitely an advantage when it comes to the prevention of this kind of threats (Table 8).

Table 8. Leading Endpoint Security and Protection Platforms

Sophos	Sophos Endpoint Protection makes it simple to secure Windows, Mac, and Linux systems against malware and advanced threats, such as targeted attacks
Trend Micro	Trend Micro endpoint security provides the necessary threat protection and data security to users and corporate information across every device and application
Webroot Inc.	Webroot SecureAnywhere Endpoint Protection leverages cloud-based real-time intelligence to protect organizations against ever-evolving threats
BitDefender	Bitdefender's GravityZone Endpoint Security provides the highly scalable endpoint security solution that businesses require to protect against malware and web threats
Symantec	Symantec Endpoint Protection: Proactively detect and block today's most advanced threats with an endpoint protection solution that goes beyond antivirus
Kaspersky Lab	World-class security for all your endpoints – including laptops, desktops, file servers and mobile devices. Advanced security for workstations & File servers. Multi-layer mobile security and management. Application Control, Device Control & Web Control. Centralized management console for all functions

Application Security Testing (AST) helps developers, administrators, and enterprises to identify security vulnerabilities by performing exhausting testing on various aspects of the software. AST is usually an operation that does not run in the front-line, but a careful testing of a hardware or software applications before deployment can prevent future attacks. Testing can take place even before deployment, but also while a product has been deployed, providing continuously feedback. Another possible benefit will be enriching tests with even more attack scenarios and consuming this information in an automated manner (Table 9).

Table 9. Application Security Testing

IBM Corporation	IBM Security AppScan Standard helps organizations decrease the likelihood of web application attacks and costly data breaches by automating application security vulnerability testing. IBM Security AppScan Standard can be used to reduce risk by permitting you to test applications prior to deployment and for ongoing risk assessment in production environments
WhiteHat Security	WhiteHat Sentinel is a Software-as-a-Service (SaaS) platform that enables your business to quickly deploy a scalable application security program across the entire software development lifecycle (SDLC). Combining advanced scanning technology with a large application threat research team, WhiteHat Security accurately identifies the enterprise vulnerabilities and scale to meet any demand
Microfocus	Fortify on Demand is an application security testing and program management solution that enables customers to easily create, supplement and expand a software security assurance program through a managed service dedicated to delivery and customer support

2.2 Emerging Security Market Sectors and Key Players

A number of emerging markets that will expand significantly in next few years is those including certain characteristics such as: (i) intelligent methods of detecting/mitigating attacks, rather than a rule or signature-based approach (ii) advanced behaviour analysis and user profiling (iii) a centralized way of collecting, correlating and extracting intelligence from multiple endpoints, providing higher level of confidence for the risks than individual indications. Some of the key players in these markets and a short description of their products follow in the following sections.

Deception Technology is an emerging market segment in cybersecurity. The main goal of deception technology solutions is the deployment of several decoys in parts of the infrastructure that are indistinguishable with the real servers. If an attacker gains access, these decoys act as an easy target and quickly notify as well as trigger appropriate actions against the intruder (Table 10).

Table 10. Deception Technology key players

TrapX	TrapX is a cyber security company founded in 2010 and headquartered in California, US. TrapX "Deception grid" platform provides deception based advance threat defense solution. TrapX has a number of out-of-box use cases for detecting zero-day malware, ransomware and attacks through compromised accounts
Cymmetria	Cymmetria, founded in 2014 and headquartered in California, US, has a deception platform called "Mazerunner", which intercepts the attacker during the reconnaissance phase and carefully lead them to a monitored deception network where they are analyzed for their tactics, techniques and procedures employed for attacking the enterprise
Acalvio	Acalvio provides Advanced Threat Defense (ATD) solutions to detect, engage and respond to malicious activity inside the enterprise networks. Acalvio holds patents in deception and data science and have developed their product "Deception2.0" around that. Acalvio is founded in 2015 and headquartered in California, USA

Endpoint Detection and Response. Endpoint Detection and Response (EDR) is the evolution of EPP. Typically, EDR involves the detection and mitigation to a more sophisticated process including detection, analytics and prioritization of incident response.Currently there is some confusion over the exact borders of each market. However, the characteristics of the EDR products can be a driver for extending the capabilities of the EPP ones, either directly, or through the development of synergies between modules that will render existing frameworks capable of eventually providing EDR services (Table 11).

Table 11. Endpoint Detection and Response key players and products

Carbon Black	Carbon Black Enterprise Response is the most complete endpoint detection and response solution available to security teams who want a single platform for hunting threats, disrupting adversary behaviour and changing the economics of security operations. Only Carbon Black Enterprise Response continuously records all endpoint activity, centralizes and correlates that data with unified intelligence sources, and reveals a complete kill chain that pinpoints attack root cause to power live threat containment, banning and remediation activities. Built entirely on open APIs, Carbon Black Enterprise Response pushes and pulls data through the security infrastructure to automate and enhance adaptive threat response processes, helping to make it the dominant EDR solution among global enterprises
Cisco Systems Inc.	Cisco Advanced Malware Protection (AMP) is a security solution that addresses the full lifecycle of the advanced malware problem. It can not only prevent breaches, but gives you the visibility and control to rapidly detect, contain, and remediate threats if they evade front-line defences - all cost-effectively and without impacting operational efficiency
CrowdStrike	CrowdStrike is a leading provider of next-generation endpoint protection, threat intelligence, and pre- and post incident response services. CrowdStrike Falcon is the first true Software as a Service (SaaS) based platform for next-generation endpoint protection that detects, prevents, and responds to attacks, at any stage - even malware-free intrusions. Falcon's patented lightweight endpoint sensor can be deployed to over 100,000 endpoints in hours providing visibility into billions of events in real-time. CrowdStrike operates on a highly scalable subscription- based business model that allows customers the flexibility to use CrowdStrike-as-a-Service to multiply their security team's effectiveness and expertise with 24/7 endpoint visibility, monitoring, and response
FireEye	The FireEye Endpoint Threat Prevention for the FireEye Security Platform - HX Series was developed by Mandiant consultants for use during an incident response or compromise assessment. The management system consists of a hardware appliance that is installed in the primary network and an optional appliance that can be installed into the DMZ for managing off network endpoints

(*continued*)

Table 11. (*continued*)

Guidance Software (now part of OpenText)	EnCase Endpoint Security: Mitigate Threats, Maximize Productivity Enterprises demand EDR products to offer scalability, strong detection and incident response workflows, and open integrations to operate more efficiently. EnCase Endpoint Security v6 was designed to not only meet these needs, but then exceed them with a beautifully redesigned front-end user interface. The completely redesigned EnCase Endpoint Security v6 delivers improved performance, better usability, and enhanced capabilities. Moving to the newest version of EnCase Endpoint Security has never been easier or more exciting
RSA	RSA ECAT is a continuous endpoint solution providing contextual visibility beyond a single alert to provide incident responders and security analysts a full attack investigation platform to detect and respond in real-time against advanced attacks, known and unknown as well as malware and non-malware threats
Symantec	Symantec Advanced Threat Protection: Endpoint is a new solution to uncover, prioritize, and remediate advanced attacks across all of your endpoints, leveraging existing investments in Symantec Endpoint Protection. With one click of a button, you can search for, discover, and remediate any attack artifacts across all of your endpoint systems. And, if you have Symantec Advanced Threat Protection: Network or Symantec Email Security.cloud, Symantec's Synapse correlation technology will automatically aggregate events across all Symantec-protected control points to prioritize the most critical threats in your organization

Cloud Access Security Brokers (CASB) have appeared in an era where cloud applications become more and more an integral part of the organization workflow, manage corporate data but do not operate on private infrastructure. CASB is entity which provides common access policies from any corporate device to any cloud application (Table 12).

Identity and Access Management (IAM) is the process of managing digital identities, and access rights to enterprise resource and auditing in an automated manner. From a technical standpoint, IAMs are centralized management systems that consolidate the processes of authentication and auditing providing a single framework for access. Main goals in IAM are (i) Multi-factor authentication schemes, (ii) Integration with directory services (LDAP, Active Directory, etc.), (iii) Single Sign-On (SSO), (iv) Credentials management, (v) Auditing, (vi) Analytics.

Table 12. Cloud Access Security Broker key players and products

CipherCloud	Available as a service or virtual appliance, CipherCloud delivers a comprehensive set of protection controls across all cloud applications, including encryption, tokenization, activity monitoring, data loss prevention (DLP) and malware detection that can overcome cloud security concerns
Cisco Systems, Inc.	Cisco CloudLock focuses on the shadow IT challenge which matter: those cloud and third-party apps that directly connect into a corporate environment. CloudLock provides adequate control to decide which apps lead to productivity gains and which ones are a security risk in any organization
Adallom (now part of Microsoft)	Cloud access security broker Adallom announced that its cloud application security platform is now available as part of the HP Enterprise Security Products and HP Enterprise Services portfolios
Palerra LORIC (now part of Oracle)	Palerra enables organizations to protect business-critical cloud infrastructure and data with LORICTM, the cloud security automation platform. LORIC is delivered as a service and can be deployed in minutes
Palo Alto Networks	Aperture extends the visibility and granular control of our security platform into SaaS applications themselves – an area traditionally invisible to IT. Aperture solves this problem by looking into SaaS applications directly, providing full visibility into the day-to-day activities of users and data. Granular controls ensure policy is maintained to eliminate data exposure and threat risks
Skyhigh Networks	Skyhigh Cloud Security Manager enables IT to embrace and accelerate the adoption of cloud services while ensuring privacy, security, and compliance
Blue Coat (now part of Symantec)	The Blue Coat Cloud Data Protection Gateway is a software solution that delivers critical data privacy and security capabilities to users of public cloud applications

The core idea of IAM is the existence of some common user authentication service that not only allows access, but also audits the use of assets and reports possible malicious events. It also allows the correlation of events from multiple sources to single users through the common directory service. SMESEC does not have an offering in this field, however the study of the capabilities of IAM offerings can help SMESEC understand what should be needed to effectively handle the identifications of users and the correlation to specific access events (Table 13) .

Table 13. Identity and Access Management key players and products

IBM Corporation	IBM Security Identity and Access Manager provides automated and policy-based user lifecycle management and access controls throughout the enterprise. Available as an easy-to-manage virtual appliance, it pairs IBM Security Identity Manager with IBM Security Access Manager Platform for more secure user authentication and authorization to applications and data
Oracle Corporation	Oracle's complete, integrated next-generation identity management platform provides breakthrough scalability with an robust suite of identity management solutions
Sailpoint	IdentityIQ is SailPoint's governance-based identity and access management (IAM) software solution that delivers a unified approach to compliance, password management and provisioning activities for applications running on-premises or from the cloud. IdentityIQ meets the needs of large organizations with complex identity management processes who prefer to tailor their solution to align with unique business needs
Okta	The Okta identity management service provides directory services, SSO, strong authentication, provisioning, workflow, and reporting, all delivered as a multitenant IDaaS though some components reside on-premise
RSA Security LLC	RSA offers both RSA Identity Management and Governance (RSA IGA), a full-fledged identity management suite built from separately licensed components, and RSA VIA, an IDaaS suite composed of separately licensed SAAS point solutions

3 Towards a Holistic Cybersecurity Framework for SMEs

The previously mentioned security market analysis identified some key market segments along with the technical requirements of each one. Apart from the traditional segments, emerging ones are also presented since they are going to play a key role in the cybersecurity ecosystem over the next few years. It is imperative that any properly-designed framework must embrace some of the new features or provide the hooks to connect with third-party products there.

When the project started, the SMESEC consortium members [4] conducted a thorough technical analysis of the independent products contributed to be integrated in the overall platform. This analysis, as shown in Table 14, revealed that these products indeed provide a wide range of capabilities to cover the high-level requirements derived from the security market analysis. Some products can produce reports that go beyond the raw data and reveal more insights. The existence of processed data means less burden and traffic to other architecture components that will perform the data analysis. In addition, the integration effort should ensure that these requirements also stay on top during the design

Table 14. SMESEC products by market segment

Product name	Security areas	Market
ATOS XL-SIEM	Security information and event management	SIEM
BD GravityZone	Anti-virus/anti-malware	EPP, EDR
CITRIX ADC	SSL interception, URL filtering	WAF, DDoS
EGM test-as-a-service	Testing	AST
FHNW	Security readiness evaluation	GRC
FORTH EWIS & cloud	Intrusion detection/prevention systems	IDS/IPS
IBM angel-eye	Virtual patching	AST
IBM ExpliSAT	Software formal verification tool	AST
IBM anti-ROP	Anti-ROP solution	Moving target defence

and implementation of the unified framework. This analysis also investigated possible integration strategies in regards to architecture, platform deployment and cloud readiness, all of paramount importance for delivering a robust and noteworthy cybersecurity framework.

Not all products can address or have the optimal solutions for all the different cases of cyber-attacks. Efficient combination of existing feature is the key to successful cyber-attack mitigation, regardless of how sophisticated this may be. In addition, a proper framework must be able to adopt the latest innovations by integrating products (not only from security) with focused solutions from different providers very fast and considerably easy. These two elements are considered of paramount importance for the SMESEC consortium members and will be an integral part of the overall design, implementation and integration phase of the project. There is currently no contributed product focused on behaviour analysis, other than BD GravityZone which rather examines software behaviour. On the contrary, few products support risk assessment from raw events. This is an interesting point architecturally, as the collection of more events from all other products to them, can potentially reinforce their risk assessment capabilities.

4 Conclusions

There is no cybersecurity product capable of addressing every different case of cyber-attacks (viruses, malware, ransomware, intrusion detection, DDoS etc.), nor worthy of being considered as a holistic cybersecurity solution. Any framework must be able to adopt the latest innovations by integrating a variety of products and focused solutions from different providers, very fast and considerably easy.

Cybersecurity solutions are becoming more “intelligent” with technologies like machine learning [1], statistical and user behavioral analysis, in a struggle to mitigate the constantly more sophisticated and perplexed cyber-attacks. However, Not all products can address or have the optimal solutions for all the different cases of cyber-attacks, therefore it should be flexible and modular enough

to adopt the latest innovations by integrating products (not only from security) with focused solutions from different providers very fast and considerably easy .

Based on the technical analysis of the contributed products and the market segment analysis, focus is given on placing the SMESEC framework in the security landscape. In the first phase, only as a sum of the products, but it is anticipated that the integration will produce some extra value to the overall solution. Some product extensions, as identified by partners, point to new features that would help SMESEC strengthen its position as a unified security framework, provide added-value to all individual products, and greatly improve the benefits for SMEs.

Acknowledgment. This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927 (CONCORDIA). This work is also partly supported by the European Commission under the auspices of SMESEC Project, Horizon 2020 Research and Innovation action (Grant Agreement No. 740787). The views and opinions expressed are those of the authors and do not necessary reflect the official position of Citrix Systems Inc.

References

1. Buczak, A.L., Guven, E.: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. **18**(2), 1153–1176 (2016). https://doi.org/10.1109/COMST.2015.2494502. Secondquarter
2. Butun, I., Morgera, S.D., Sankar, R.: A survey of intrusion detection systems in wireless sensor networks. IEEE Commun. Surv. Tutor. **16**(1), 266–282 (2014). https://doi.org/10.1109/SURV.2013.050113.00191. First
3. Gendreau, A.A., Moorman, M.: Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 84–90, August 2016. https://doi.org/10.1109/FiCloud.2016.20
4. SMESEC Project Consortium. https://smesec.eu/
5. Thakur, K., Qiu, M., Gai, K., Ali, M.L.: An investigation on cyber security threats and security models. In: 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing, pp. 307–311, November 2015. https://doi.org/10.1109/CSCloud.2015.71
6. Tselios, C., Politis, I., Tselios, V., Kotsopoulos, S., Dagiuklas, T.: Cloud computing: a great revenue opportunity for telecommunication industry. In: 51st FITCE Congress (FITCE), Poznan, Poland, vol. 6 (2012)