ARCTIC WOLF

The State Of The European Cybersecurity Product Market

FEATURING RESEARCH FROM FORRESTER

Forrester Infographic: The State Of The European Cybersecurity Product Market

Whilst many high-profile cyberattacks involve businesses located in the United States, companies in Europe are not immune—far from it. Recent studies conducted by the European Union Agency for Cybersecurity (ENISA) and the governments of the United Kingdom and Germany confirm that European companies face a significant and growing risk of cybercrime activity and data breaches.

For example, the Cyber Security Breaches Survey 2020 prepared by the UK government reported that 46% of businesses experienced a cybersecurity breach or attack in the previous 12 months. Some businesses suffered more than others. In fact, 68% of medium-sized businesses and 75% of large businesses surveyed endured an attack. The German government paints a similar picture, with 33% of surveyed organisations having experienced a cybersecurity incident in 2018, with 87% of those incidents resulting in outages or disruptions to their operations.

More broadly, ENISA's report on the threat landscape identified 10 trends that emerged in 2020. These include expansion of the attack surface as society enters a new and accelerated phase of digital transformation, as well as the emergence of new social and economic norms as a result of the COVID-19 pandemic

Every sector of the economy can become a target, but the legal sector is a perennial favourite for attackers due to its vast amount of data and the value it offers to cybercriminals and nation-states. For example, in June 2021, UK law firm Gateley revealed a breach of its IT environment in which some of the firm's data was downloaded by attackers, necessitating the firm to contact clients whose data was compromised during the leak. Law firms with a global presence that includes Europe can also find themselves victimised, as was the case in October 2020, when Seyfarth Shaw announced it suffered a ransomware attack.

For the data and funds in its possession, the financial sector is often connected to sophisticated and pervasive attacks and breaches. In April 2021, the European Banking Authority announced that attackers breached its defences and may have gathered personal data via emails housed on Microsoft Exchange servers. In the UK alone, some estimates peg the share of financial services companies that suffered cyberattacks in 2020 as high as 70%.

In addition to the risk of a cyberattack, the financial sector in Europe faces a complex and evolving regulatory landscape. This makes the creation of an effective cybersecurity program even more challenging, as it must also help ensure associated regulatory compliance.

The healthcare and government sectors also are magnets for ongoing attacks for a multitude of reasons. In fact, hospital systems in the UK, Germany, France, and Spain have experienced all kinds of cyberattacks with varying degrees of damage. ENISA announced that cyberattacks more than doubled in 2020, from 146 to 304. That included a 47% spike in cyberattacks against the healthcare sector.

IN THIS DOCUMENT

1 The State Of The European Cybersecurity Product Market

5 Forrester Infographic: The State Of The European Cybersecurity Product Market

16 About Arctic Wolf

SKILLS SHORTAGE LEAVES COMPANIES AND CRITICAL INFRASTRUCTURE EXPOSED

Beyond the challenges the threat landscape already provides, the cybersecurity talent shortage presents a significant roadblock for most companies. For the UK government, the lack of suitably qualified cyber talent is "verging on a crisis" as it relates to the need to secure critical national infrastructure.

Unfortunately, bridging the gap between the demand and supply of cybersecurity experts could take decades to accomplish. The 2020 (ISC)^2 Cybersecurity Workforce Study, which surveyed 3,790 security professionals in North America, Europe, Latin America, and the Asia-Pacific region, predicts that the global security workforce must grow by a staggering 89% to protect critical assets. Furthermore, 56% of those surveyed said that cybersecurity shortages are putting their organisations at risk.

Nonetheless, the global shortage of professionals according the ISC2 report stands at 3.12 million. To combat the shortage of talent, organisations have begun to look for tools, programs, and services that can reduce the strain and demands on their existing operational IT staff, and can help their limited crew of security-focused employees become more productive and develop a higher degree of job satisfaction.

Depending on where an organisation's staffing shortages lie, a managed security services provider, managed detection and response provider, or endpoint detection and response provider, can provide critical support and expertise.

WHAT'S NEXT FOR THE UK AND EUROPEAN CYBERSECURITY LANDSCAPE?

Whilst there's clearly considerable demand for cybersecurity support around the globe, there's a problem in Europe as it relates to the providers that support the market. For quite some time, European vendors have fallen short of expectations in terms of defending against targeted attacks and the common opportunistic threats such as phishing, ransomware, and business email compromise.

In some cases, European managed security service providers (MSSPs), have attempted to bridge the growing talent and tools gap, promising to ease the burden of proactive threat hunting, alert management and incident triage. More often, European customers find that their MSSP partners are only capable of delivering a reactive approach to security, with gaps in coverage in critical areas, including cloud telemetry visibility, proactive threat hunting, and real-time incident response.

There is a rapidly expanding disconnect between customer expectations of MSSP vendors, including the demand for enhanced remediation support and response capabilities, and the level of service they're able to deliver has led to an increased desire to partner with the established Managed Detection and Response (MDR) vendors who have proven themselves across the entire security operations discipline. Unfortunately, few MDR vendors with robust client bases and enterprise-grade service are currently headquartered in the UK or EU, leading to increased interest in and adoption of North American solutions.

FORRESTER OFFERS AN EVALUATION

To understand the current cybersecurity vendor landscape in the UK and Europe and how the environment might evolve, Forrester conducted extensive research to hear directly from European companies about their experiences with international cybersecurity vendors.

Its research determined that UK and European companies need the assistance of providers to mitigate the growing number of threats they face. Since the skills gap may take years to close, more vendors will add new offerings to help organisations thwart attacks. Consequently, organisations will find themselves forced to choose between multiple point products or comprehensive solution that combine the processes, people and technology that many of today's businesses need.

Today, Arctic Wolf has customers in the UK and Europe that leverage our security operations solutions to address their most pressing cybersecurity challenges while taking the burden of doing so off their outstretched internal teams. To learn more, go to arcticwolf.com/uk.

Forrester Infographic: The State Of The European Cybersecurity Product Market

European Security Leaders Trying To Buy Local Will Struggle To Meet Their Needs

by Paul McKay
with Martin Gill, Melissa Bongarzone, and Peggy Dostie

July 8, 2020

Why Read This Report

Developing a thriving European cybersecurity product market is a key EU digital single market priority in 2020 and beyond. European security leaders would love to buy locally but don't always have many viable options to meet their needs. Use data from this infographic to understand European security leaders' current usage of security products, satisfaction levels, and the level of choice they have to buy local European cybersecurity products.

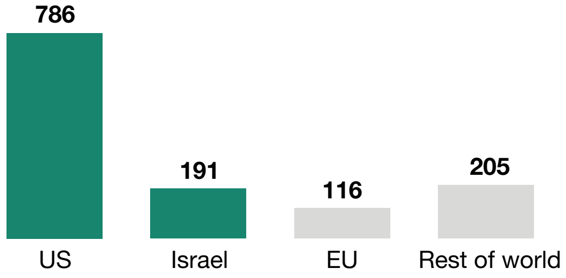
FORRESTER INFOGRAPHIC

The state of Europe’s cybersecurity product market

The EU has signaled that developing Europe’s market for cybersecurity products is a key digital single market priority for 2021 to 2027.[1] This infographic explores the state of the European cybersecurity product market and examines the buying preferences of European security leaders.

The US and Israel dominate the global cybersecurity market[1]

Cybersecurity firms by current primary HQ location and tax home[2]



CISOs looking to buy European-only would struggle to source in this way

🟩 Extensive selection of EU-based security vendors

🟩 Good selection of EU-based security vendors

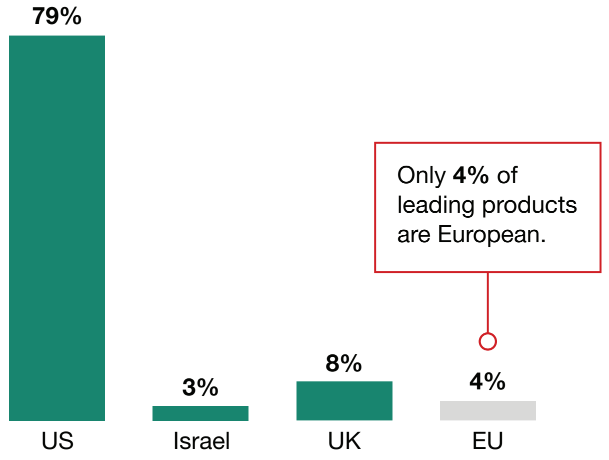
⬛ Limited selection of EU-based security vendors

◼ No credible EU-based security vendors in this space

	EU security technology market selection
Endpoint security	⬛
Endpoint detection and response	▒
Data security suites (including DLP)	⬛
Threat intelligence	⬛
Governance, risk, and compliance	🟩
Security analytics	▒
Enterprise firewalls	🟩
Distributed denial of service	🟩
Email security	🟩
Industrial control system security	⬛
Network security (including NAV and microsegmentation)	⬛
IoT security	⬛
Privileged identity management	▒
Customer identity and access management	⬛
Identity-as-a-service	⬛
Cloud security solutions	⬛
Native public cloud capability	▒
Mobile security	⬛
Server security	⬛
Privacy management	🟩
Cybersecurity risk ratings	▒
Access recertification	▒
Application security testing solutions	⬛
Web application firewalls	▒

European security leaders rely heavily on US security products

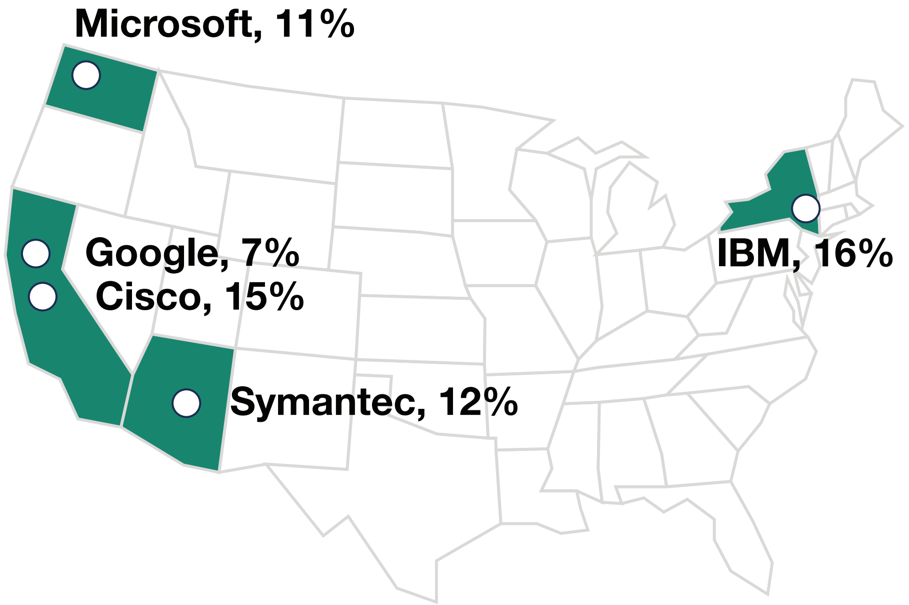
Domicile of firms whose security products were named a Leader or Strong Performer in Forrester Wave™ evaluations[3]



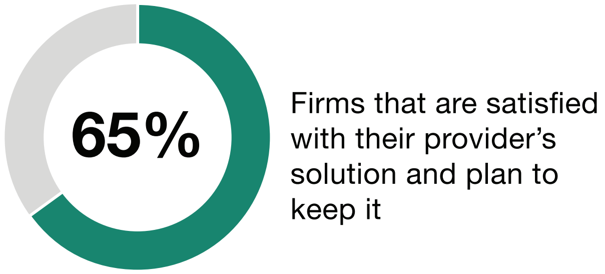
Only **4%** of leading products are European.

Note: The total for the US includes companies that are started elsewhere but transferred their listing to the US. This shows the US's dominance both in creating leading security companies and being an attractive place for startups looking to list or attract investment.

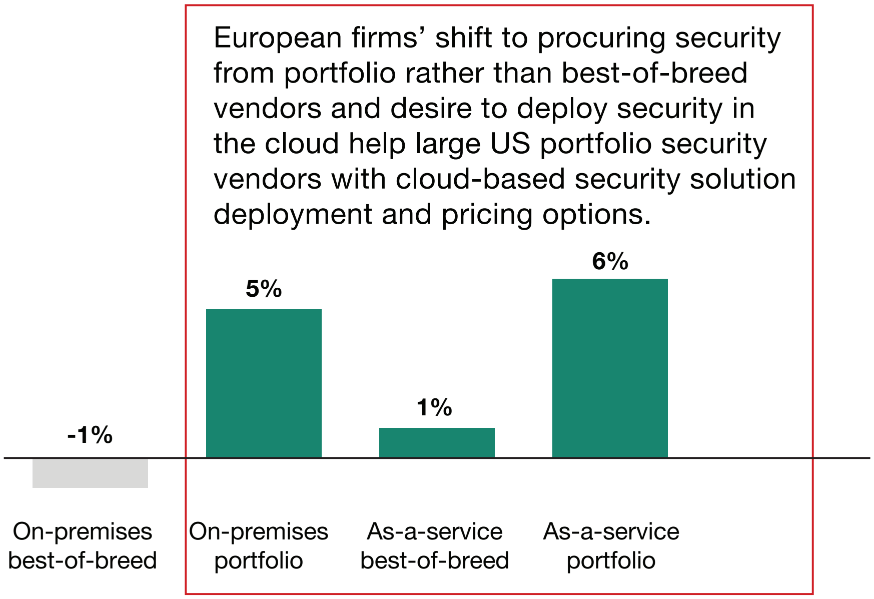
European security leaders use one of the following five companies as their primary security solution provider, showing the current dominance of US security firms.[4]



High satisfaction levels reduce the likelihood that firms will displace their current US-based vendors.[5]



Average shift in buying preferences for on-premises and as-a-service security technologies, in percentage points[6]


European firms' shift to procuring security from portfolio rather than best-of-breed vendors and desire to deploy security in the cloud help large US portfolio security vendors with cloud-based security solution deployment and pricing options.

The EU wishes to create a thriving local cybersecurity industry to better compete with the US. However, current efforts could lead to trade barriers. EU security leaders should continue to prioritize functionality and security need over country of origin when buying security software.

Notes and sources

1. The European Cybersecurity Act introduces the idea of a Europewide certification framework for technology processes and services. Source: “The EU Cybersecurity Act,” European Commission

2. Based on Venture Scanner data on active cybersecurity firms and their country of domicile. Data current as of March 31, 2020. “EU” refers to 27 EU member states with a cybersecurity firm with data in Venture Scanner. We include Switzerland and members of the European Economic Area in the EU for the purposes of this analysis. The UK is included in the “rest of the world,” as the UK is no longer an EU member. Source: Venture Scanner

3. Analysis of all companies assessed in currently published (i.e., not yet retired) Forrester Wave™ evaluations by Forrester’s security and risk team. We based this analysis on the company’s main domicile, i.e., where company HQ is located and where the firm is formally listed for regulation and tax purposes

4. We asked 854 European security technology decision makers: “Which of the following companies is your primary provider of security solutions?” Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

5. Base: 833 European security technology decision makers whose firm has a primary provider of security solutions. Source: Forrester Analytics Global Business Technographics Security Survey, 2019

6. Base: 697 to 753 European security technology decision makers. Source: Forrester Analytics Global Business Technographics Security Survey, 2017 and 2019

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

SURVEY METHODOLOGY

The Forrester Analytics Global Business Technographics® Security Survey, 2019, was fielded between April and June 2019. This online survey included 3,890 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Dynata fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics' Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Related Research Documents

Security Budgets Europe, 2020: SaaS Security Is In Vogue

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals
CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals
CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
› **Security & Risk**
Sourcing & Vendor Management

Technology Industry Professionals
Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

ABOUT ARCTIC WOLF:

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection, and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture.