Ministry of Foreign Affairs

US and Washington DC Cyber Market Analysis 2021

Commissioned by the Netherlands Enterprise Agency

>> *Sustainable. Agricultural. Innovative. International.*

UNITED STATES AND WASHINGTON DC REGION CYBER MARKET ANALYSIS

Prepared for The Embassy of the Netherlands
in the United States

February 2021

GOOD
HARBOR
Cyber Security
Risk Management

Proprietary and Confidential

1. Scope and Methodology

The Embassy of the Netherlands in the United States retained Good Harbor to analyze the US market for Dutch cybersecurity companies, focusing specifically on opportunities in the Washington DC, Virginia, and Maryland region. Good Harbor focused analysis on Dutch strengths in the cybersecurity market, alignment with US market trends, major players in the US for Dutch companies to partner or work through, and barriers to entry for Dutch cybersecurity companies. The analysis highlights leading firms, integrators, research centers, and investors that lead trends in the US cyber industry in both the federal and commercial sectors. It also identifies emerging cybersecurity market segments that are likely areas of growth over the next five years.

Good Harbor carried out its analysis through review of key documents provided by Embassy staff as well as information collection from internal and external interviews. Good Harbor also drew on its understanding of the cybersecurity market developed through work with corporate CISOs, CEOs, and venture capital firms. Good Harbor conducted a workshop with members of the core Netherlands- and US-based Dutch team in addition to external interviews with a US technical expert, a venture capitalist investing in European companies, and Dutch cybersecurity entrepreneurs.

2. Dutch Commercial Cybersecurity Ecosystem

The Netherlands is seen as a leader in Europe on cybersecurity with a strong research, startup, and practitioner ecosystem. Along with Germany, Estonia, the Nordic countries, and the United Kingdom, one interviewee identified the Netherlands as one of the hotbeds for cybersecurity in Europe and a key area for growing companies that are poised for success in Europe and potentially the US market. American technology giants Microsoft, Amazon, and Google have all expanded their presence in the Netherlands, especially around cloud computing. The Netherlands government has taken an active role in promoting the sector including in fundamental research and assisting with market access and connections. As Dutch companies enter the US market, they can draw on strengths that have been identified by both interviewees and the Dutch government in its multiyear US cyber security roadmap. Some of these strengths overlap with current areas of market growth in the US cybersecurity market and future emerging areas.

2a. Operational Technology (OT)/Internet of Things (IoT) Security

The Netherlands has a strong industrial economy including in high-tech manufacturing, chemicals, and energy. The Netherlands has long been a trading economy with major port facilities like Rotterdam, the largest port in Europe. According to the Netherlands Roadmap for Cyber in the US and interviews, the industrial strength of the country has made Operational Technology (OT) and Industrial Control Systems (ICS) security an area of focus for entrepreneurs and researchers. The ICS/OT security market tends to be highly specialized and require specific backgrounds, as ICS/OT protocols and devices are distinct from traditional IT devices. OT/ICS security solutions require specifically built and implemented products and services based on in-depth knowledge of these environments, how they operate, and how teams within those environments conduct their jobs.

The Dutch government, cybersecurity industry, and universities have also started a major research program focused on securing the Internet of Things, comprised of non-IT devices that are increasingly connected to the Internet and corporate networks. The INTERSCT Consortium is a public-private research partnership including Dutch governmental entities, private companies, and universities focused on IoT security. With other emerging technologies like 5G expected to catalyze IoT device connectivity, IoT is likely to remain a priority research area for the Netherlands. Startups from Europe, including the Netherlands, and Israel have made inroads in the US OT and IoT security market.

2b. Penetration Testing/Vulnerability Scanning

The Netherlands has a strong hacker culture dating back to the late 1980s and 1990s according to multiple interviewees. Along with Berlin, Amsterdam was a center of vulnerability research and hacking activity. This history of offensive security and hacking communities has helped differentiate the Netherlands in “offensive” security, including penetration testing and vulnerability scanning services and technologies. The hacking culture in the Netherlands has created a strong talent pool for services firms to find vulnerability researchers and penetration testers. Services firms, including Fox-IT (acquired by NCC Group) and Secura, along with technology providers, like Guardian 360, are active in the vulnerability assessment and red-teaming market. HackerOne, a leading global bug bounty program provider, has a strong presence in the Netherlands. Penetration testing and vulnerability scanning is a core cybersecurity market for the United States companies, but there are large players like NCC that have a foothold in the US.

2c. Threat Intelligence

The Netherlands’ Roadmap for Cybersecurity in the US identifies threat intelligence as an area of focus and strength for the Netherlands. US companies have shown a willingness to acquire threat intelligence from non-US companies, especially from NATO allies and Israel, making threat intelligence a potential area for expansion into the US market. EclecticIQ is headquartered in Amsterdam, and leading firms including Intel471 and IntSights have offices in the Netherlands. Other European firms that are quickly expanding into the US market or already have a significant presence include Digital Shadows (UK, redomiciled in US), Blueliv (Spain), and CybelAngel (France). Large enterprise customers often purchase multiple threat feeds and rely on multiple vendors. Compared to other product categories, enterprise customers often have fewer concerns about threat intelligence providers with a minimal US presence given that these products are relatively easy for large enterprises to add and to replace without intensive professional services. The United States is a leader in threat intelligence, but international providers are often able to win US customers as well.

2d. Privacy

With the General Data Protection Regulation (GDPR), the EU has become a model for data privacy globally. New regulation in the United States, including California Consumer Privacy Act (CCPA), follows similar principles to GDPR. While privacy and security have traditionally been separate fields, data security and privacy are converging in both policy and technology. The Dutch experience with data privacy should be of benefit in the US market as privacy regulations are introduced in more states, creating a patchwork of regimes. In the United States, privacy is largely considered a governance, risk, and compliance (GRC) or legal issue and not a core technical market. That is beginning to change with emerging tech-focused privacy startups. European leadership in privacy should provide technical startups a position in the US market.

3. US Cybersecurity Market and Trends: Opportunities for the Netherlands

In these areas of strength for the Netherlands based on economy, history, and policy, there is overlap between the areas of focus and market trends in the United States. From its work with the "pain points" of corporate CISOs in the United States and research with top investment firms, Good Harbor has seen demand and market growth in managed security services, identity including the emerging Zero Trust solutions, and data security/privacy. These market segments are experiencing strong growth and disruption due to the improved functionality and usability in newer solutions, changing models of security, new regulatory requirements, and shortages of cybersecurity talent. The United States is a leader in these markets, but there are strong players from Europe in each segment and open space for leading solutions to fill demand in the United States. Over the next five years, technological advancement in 5G security, cloud, Secure Access Service Edge (SASE), and Artificial Intelligence/Machine Learning are likely to be dominant growth areas of the cybersecurity market of which Dutch companies should be aware.

3a. Current Growth Areas in the US Market

Managed security services constitute a mature market segment in which the Netherlands is strong as home to major global players like Fox-IT. Demand for managed security services is rising due to the challenges of staffing and running internal security operations centers (SOCs). For most organizations, an outsourced team to manage security technologies and detect intrusions is a cheaper and more effective solution than doing so in-house. The MSSP market is being disrupted by new entrants using automation, improved internally developed analytics, and stronger detection. These Managed Detection and Response (MDR) providers are focused not on running and monitoring legacy perimeter technologies, but rather on actively detecting and blocking threats within the network. Leading MDR providers that have emerged as fast-growing players in the market and are poised to gain share include eSentire, Artic Wolf, and Expel (Disclosure: Expel is a portfolio company of Paladin Capital Group, a Good Harbor affiliate). Product companies, including in the endpoint, data loss prevention, and cloud security spaces, are increasingly offering managed services for their specific products given the management and staffing challenges customer organizations often face. Managed services are likely to continue to consolidate globally, as the market is currently defined by numerous regional and local players. The MSSP market is expected to experience steady, strong growth in coming years. 451 Research estimates the market will grow at nearly 17% annually to $24B by 2022.[1] IDC estimates the MSSP market will grow at a 14.2% CAGR between 2018 and 2022.[2]

Identity is a broad but fundamental category for enterprise security. Identity market growth is being driven by changing security approaches, significantly the emergence of "Zero Trust" as a model, which assumes that no interaction with data or systems is to be allowed without meeting certain conditional steps. All users, through strong access control, privilege management, and multifactor authentication, are only granted access to the resources they need for specific tasks given specific security parameters. Work-from-home, where on-premise network security appliances including firewalls, intrusion detection, and network data loss prevention do not offer coverage, has increased the demand for identity offerings. Identity products increasingly act as a network perimeter rather than network security appliances. Major organizations including Google and Microsoft have adopted Zero

[1] Executive Readout - Managed Services, 451 Research, 1 August 2018, Pg. 17

[2] "Worldwide Spending on Security Solutions," IDC, 20 March 2019, https://www.idc.com/getdoc.jsp?containerId=prUS44935119

Trust models internally, helping push the concept into the mainstream. Dutch companies can take advantage of this growth in the identity sector as identity companies in Europe including Gemalto, Omada, and Onfido have had global market success.

Identity is a large and growing market. According to Gartner, identity access management is a $10.6B market in 2019 and has grown at a 9.5% annual CAGR between 2017 and 2019.[3] Brandessence Market Research estimates that identity management market was a $10.4B market in 2018 and will grow at a 13% CAGR until 2025[4]

There is also growing demand for integrated data security offerings. Traditional data security products including encryption, data loss prevention, and data classification have been difficult to use and often a cause of business disruption, leading to only partial implementation of these technologies throughout organizations. As organizations have moved to assuming that breaches will happen, protecting data through a "data-centric" security model has gained popularity. Data-centric security builds on these technologies to include context like identity and business risk to dictate access to data, put in place controls around data, and monitor use. While demand for integrated data-centric security tools continues to grow in its own right, data security processes are increasingly integrating privacy controls, driving additional growth of the data security market. Data identification, classification, monitoring, and response all have both security and privacy use cases, and technologies for both often overlap. Privacy regulation is helping drive adoption of data security technologies.

These demand drivers are poised to continue to spur growth in the data security market. According to a white paper by Optiv and Momentum Cyber, data protection was one of five security segments that realized an increase in spending of 25% or more in 2018.[5] According to Gartner, data security as a segment grew at a rate of 17% between 2017 and 2019 to a $3.5B

[3] "Gartner Forecasts Worldwide Information Security Spending to exceed $124B in 2019," Gartner, 15 August 2018. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-informationsecurity-spending-to-exceed-124-billion-in-2019

[4] "At 13.02% CAGR, Identity and Access Management Market Size to Surpass USD 24.52 Billion by 2025," Brandessence Market Research, 20 August 2018. https://www.marketwatch.com/press-release/at-1302-cagr-identity-and-accessmanagement-iam-market-size-to-surpass-usd-2452-billion-by-2025-2019-08-20

[5] "2019 Security Technology Spend Insight Report," Optiv Inc and Momentum Cyber, 2019. https://momentumcyber.com/docs/White_Papers/2019_Security_Technology_Spend_Insights_Report_White_Paper.pdf

industry.[6] Markets and Markets estimates that the whole of the data-centric security market will be a $5.8B market by 2022, growing at a 23% CAGR from 2017.[7]

3b. Future Growth Areas in the US Market

The future of the technology stack is impacting which segments of the market will likely rapidly expand over the next five years. According to an interviewee, for example, the security of 5G equipment and thus higher data processing requirements for edge devices, including IoT devices, is likely to become more critical and spawn new security companies. The ability to deploy devices that are constantly connected at high data rates will increase data volume, move data away from the corporate core, and ensure that the data processing itself is secure. While 5G is just coming online in the United States and does not yet have an associated security market independent of IoT security, it will continue to emerge as a distinct area of focus.

Similarly, the move to the cloud is already driving new security functionality and models. First, there is market demand for securing cloud applications, workloads, and data across infrastructure. Organizations, even those heavily reliant on a single cloud platform provider, are multi-cloud environments with multiple vendors for critical applications, infrastructure, and platforms. There is demand in the market for solutions that work across vendors to offer visibility into and control of cloud environments. Representative US vendors covering all or parts of SaaS, IaaS, and PaaS security include Palo Alto Prisma, Aqua Security, Hytrust, Threat Stack, and Illumio.

Concurrently, security companies are moving traditional security and networking products to hosted environments, offering cloud-based security for now increasingly remote workforces. Known as Secure Access Service Edge (SASE) solutions, these vendors integrate network security technologies, including firewall, intrusion detection, secure web gateway, data loss prevention, and secure access, with networking capabilities like SD-WAN. There is a convergence of networking and security technologies as these solutions move towards cloud environments. Representative vendors include Palo Alto Networks, ZScaler, and Cato Networks. Incumbent networking and security appliance players including Cisco, Fortinet, and Forcepoint are quickly trying to develop their own solutions.

[6] "Gartner Forecasts Worldwide Information Security Spending to Exceed $124B in 2019," Gartner.

[7] "Data-Centric Security Market Worth $5.8B by 2022," Markets and Markets, May 2017. https://www.marketsandmarkets.com/PressReleases/data-centric-security.asp

Finally, there has been significant hype around artificial intelligence and machine learning already in the market yet increasing disillusion with the efficacy of current products and approaches. While reality may not ever live up to hype surrounding the ability to use AI to automate security and detect previously unknown attacks, the technology will likely continue to advance over the next five years. Issues with false positive rates and frequency of missed detections identified in current offerings are likely to continue to diminish, and adoption will be widespread both as standalone offerings and as part of other security technologies.

4. Major Players in the US Market for Dutch Cybersecurity Companies

The US cybersecurity market is the largest and most mature research, partnership, and venture capital market globally. The DC region specifically, with ties to government including NSA, Cyber Command, and other government agencies; strong educational organizations; incumbent cybersecurity companies; and a budding venture capital ecosystem, is one of the most dynamic areas in the US for cybersecurity activity. According to market analyst Richard Stiennon, DC, Maryland, and Virginia are home to over 170 cybersecurity companies, ranking the region second only to Silicon Valley and far ahead of other regions.[8] Major incumbent technology firms, including Amazon's future HQ2 expansion in Northern Virginia, Microsoft, and Google have made the DC region even more of a hub for security.

4a. Venture Capital and Private Equity

Venture capital and private equity investment can be a pathway for European cybersecurity firms to enter the United States market. Successful firms including AlienVault, Darktrace, and Yubico all raised venture capital from American VC funds and successfully entered the US market. Major US VC funds can help make introductions to American partners, assist with governance and corporate structure for targeting the US market, and help structure US-based sales teams. However, according to a US VC interviewee who is currently investing in the European cybersecurity market, there are few major US VC firms that are active in Europe, especially in early stages.

Leading firms including Accel, Insight, Sequoia, and TPG have active investments in European cyber companies, but most of their activity has been with UK-based startups in later stage deals. Some major VC and private equity firms in the US has covenants around

[8] Richard Stiennon, *Security Yearbook 2020: A History and Directory of the IT Security Industry*, IT Harvest 2020.

only investing in North American-based companies, but these requirements are beginning to change. Another interviewee noted that it was easier in earlier stages of growth to raise from active European funds, but funding rounds tend to be smaller than those led by American VCs. According to data from Crunchbase, of Dutch cybersecurity startups funded in the past two years, only two were funded by US firms and both were comparatively small funds. VC funding is often a signal to the market on the potential of a product. Assisting with introductions to major VC firms and hosting events to introduce Dutch companies to prominent VCs could be an area of expanded activity for the Embassy.

Table 1: Funding of Dutch Cyber Startups since 2018 (Data via Crunchbase)

Lead Investors	Investor HQ Country	Investment Name	Announced Date	Funding Type
ACE Management	France	EclecticIQ	12/1/20	Series C
DN Capital	US (San Francisco)	Zivver	10/28/20	Series B
The FIS FinTech Accelerator in Partnership with The Venture Center	US (Little Rock)	Surfly	6/30/20	Venture - Series Unknown
No lead investor listed	–	Fraudio	6/30/20	Seed
Alma Mundi Ventures	Spain	Surfly	11/15/19	Venture - Series Unknown
Walvis Participates	The Netherlands	Onegini	9/26/19	Series B
Eleven Ventures	Bulgaria	LogSentinel	8/1/19	Seed
No lead investor listed	–	SEGRON	6/27/19	Series A
Johan Mastenbroek	The Netherlands	Tykn	5/20/19	Venture - Series Unknown
Chivas Venture	UK	Tykn	12/10/18	Venture - Series Un
Vortex Capital Partners	The Netherlands	Cybersprint	11/27/18	Series A
Dawn Capital	UK	Zivver	10/16/18	Series A
Pecunio	UAE	Lynked. World	10/15/18	Venture
No lead investor listed	–	Ligo	8/29/18	Seed
World Startup Factory	The Netherlands	Paztir	4/14/18	Seed
No lead investor listed	–	Fourthline	3/14/18	Series A

No lead investor listed	–	Vision Tech Lab	2/8/18	Seed

In the DC region, there is a blossoming venture capital ecosystem focused on both commercialization efforts from national security organizations and traditional venture investing. Paladin Capital Group (Disclosure: Paladin is a Good Harbor affiliate), based in Washington DC, has an active presence in Europe. With eight active investments in European cybersecurity startups, Paladin is one of the few major US cyber investment firms actively seeking out early-stage investments in Europe. For cybersecurity startups, part of the value of such an investor is assistance with entering the US market.

Other leading investors of interest in the DC region active in the cybersecurity market include Data Tribe, NextGen Ventures, Updata Partners, Columbia Capital, Grotech Ventures, and New Atlantic Ventures. Active private equity firms headquartered in the DC area include Carlyle Group and Arlington Capital Partners. Data Tribe, a firm focused on commercializing technology emerging from the National Security Agency (NSA), is led by Bob Ackerman, an influencer in the DC region's VC community. Ackerman has been key in driving the growth of the area's venture ecosystem and sees the dynamism coming from national security organizations as a pivotal differentiator for the area. He also runs Allegis Cyber, which is a later-stage, more traditional VC fund based in Palo Alto, CA.

4b. Strategic Partners

In the US cybersecurity market, partner, channel, and Original Equipment Manufacturing (OEM) are often efficient ways to quickly enter the US market while developing local direct sales forces. Cybersecurity consulting firms, systems integrators, and value-added resellers (VAR) are major channels through which US enterprises, government agencies, and some medium-sized businesses purchase cybersecurity products and services. These intermediaries have existing trusted relationships, contracting vehicles, and the ability to integrate technologies. Major consulting firms and integrators through which cybersecurity companies often sell products include Deloitte, Accenture, PwC, IBM, DXC, Booz Allen Hamilton, and EY. In the federal market, Leidos, Northrop Grumman, Raytheon, General Dynamics, CACI, ManTech, and SAIC are all major integrators that often help bring smaller companies to government customers. There are a number of smaller cybersecurity-specific consulting firms: Coalfire is the most notable, and the British firm NCC Group also has a well-established presence following its acquisition of iSec Partners. Value-added resellers are a strong channel for many organizations and access to them is competitive between technology providers. Optiv is the most prominent cybersecurity VAR. While smaller than Optiv, Guidepoint, a Northern Virginia-based VAR, has especially strong ties to federal government customers.

Strategic partnership and OEM relationships with other cybersecurity, network, cloud, and identity firms can be a way to enter the US market. There are some cybersecurity companies that only OEM their products, allowing them to rely on the salesforces and go-to-market engines of their partners. Partnerships can also help drive customers of an existing security product to evaluate complementary technology, as technology integration is critical to a mature cybersecurity program and remains exceedingly difficult to achieve. Major companies that often OEM products in the US cybersecurity market include network security players like Cisco and Watchguard. Managed security service providers often OEM technologies including threat intelligence and external monitoring services. In the DC area, large cybersecurity companies that may be of interest for partnership opportunities include Thycotic (Identity), Dragos (OT), Neustar (DDOS), Cofense (Email), Virtru (Data Security), ThreatConnect (Intelligence), Tenable (Vulnerability Scanning), ZeroFox (Social Media), and Sonatype (Application Security).

The analyst community in the United States is highly influential with CISOs and helps drive market trends and purchasing habits. Gartner, Forrester, and 451 are the major IT security analyst firms. In the US market, these firms help guide CISOs towards certain providers and types of technology as well as providing market research for investment firms. Engaging with these analyst groups is critical for firms looking to grow engagement in and access to the US market. Analyst suggestions of technology providers often determine which firms receive RFPs from CISOs. Many CISOs choose 3-4 firms recommended by analysts to test when purchasing a specific product or filling a need in their security program. Engaging with these analyst groups can ensure that they are aware of Dutch firms, their offerings, and differentiation in the market when analysts speak to CISOs.

4c. Research Institutions

The DC region is a hotbed for university and federally funded research institutions. These organizations often liaise with foreign governments and private companies on areas of research interest. They may also be a vehicle for identifying talent or interesting emerging technology in the market. The below chart outlines some of the major research organizations in the DC region. In cybersecurity, MITRE and its associated programs has become a leader in the cybersecurity space. The MITRE ATT&CK Framework has become a common means for communicating threat and technical mitigations within the US cyber industry. The US national labs are also known leaders in the cybersecurity market.

Partnership with DC area research organizations is less likely to be a major source of revenue or funding, but can be important in tracking trends, influencing standards, and for marketing purposes. NIST regularly publishes influential standards on cybersecurity both for government and private industry in the United States that influence cybersecurity practices and buying patterns. Tracking NIST guidance is important for ensuring alignment of technical solutions to emerging standards in the US. Non-profits that provide information, training, and advocacy for cybersecurity including the Internet Security Alliance, National Cyber Security Alliance, OWASP and Cloud Security Alliance have active participation from European entities and can help drive product and feature awareness in the market. These entities have corporate sponsorships as part of their core model.

Table 2: DC Area Research Organizations

🟥 ** Notes organizations thought to be most widely referenced*

Organization	Location	Classification	Administration	Funding
Center for Information Technology (CIT)	Washington, DC	FFRDC	National Institute of Health (NIH)	National Institute of Health (NIH)
Center for Communications and Computing	Alexandria, VA	FFRDC	Institute for Defense Analyses (IDA)	
Networking & Information Technology Research and Development Program (NITRD)	Washington, DC	FFRDC	National Coordination Office (NCO)	
Homeland Security Operational Analysis Center (HSOAC)	Washington, DC	FFRDC	RAND	Dept. of Homeland Security (DHS)
Homeland Security Systems Engineering and Development Institute (HSSEDI)	Washington, DC	FFRDC	MITRE Corporation	DHS
National Cybersecurity FFRDC	Rockville, MD	FFRDC	MITRE Corporation	NIST
MITRE Corporation	McLean, VA & Bedford, MA	FFRDC operator, Non-profit		Government, independent
Cyber Security & Privacy Research Institute (CSPRI)	Washington, DC	Education, Non-profit		George Washington University

Center for Public Policy and Private Enterprise (CPPPE)	College Park, MD	Education, Non-profit		University of Maryland
Kogod Cybersecurity Governance Center (KCGC)	Washington, DC	Education, Non-profit		Kogod School of Business, American University
CyberSMART (**S**cience, **M**anagement, **A**pplications, **R**egulation, and **T**raining) Center	Washington, DC	Education, Non-profit		Georgetown University
SANS Institute	Fredericksburg, VA	For-profit		
Internet Security Alliance (ISA)	Arlington, VA	501(c)(3)		
Electronic Privacy Information Center (EPIC)	Washington, DC	501(c)(3)		
National Cyber Security Alliance	Washington, DC	501(c)		
Cloud Security Alliance (DC Chapter and Netherlands Chapter)	Washington, DC & Europe	Non-profit		
Open Web Application Security Project (OWASP) Foundation	Bel Air, MD	501(c)(3)		
Cyber, Space & Intelligence Organization	McLean, VA	Trade association, Non-profit		

5. Challenges and Barriers to Entry for Dutch Cybersecurity Companies

Because the Netherlands is a trusted NATO ally and member of the EU, Dutch companies face fewer reputational, legal, and regulatory barriers to accessing the US market than those of even other US allies like Israel. However, there are barriers both in the commercial and public sector that may create challenges for Dutch companies looking to sell to US private and governmental customers. Dutch companies do not have the advantages that members of the Five Eyes alliance do in accessing US national security-related markets, for example, but there are few institutional barriers in the commercial space. In addition to legal and regulatory barriers, Dutch experts interviewed by Good Harbor observed cultural barriers in the federal and commercial sectors that may slow growth for other Dutch companies.

5a. Commercial Barriers

While there are few legal or regulatory barriers to Dutch companies entering the US commercial market, there may be cultural barriers of which Dutch companies should be aware. First, having American business and customer success leadership in the company, even if the development of technology and headquarters remains in the Netherlands, is important for targeting US customers. For example, in the managed security services space, having a SOC in the US with staffed by American analysts who interact with clients in the US is important for success. US customers want to speak to local analysts and at least feel like they are being serviced by an American company. Many large foreign cybersecurity providers have US-based customer support and SOC operations while headquarters, finance, and development remain overseas.

Second, the US cybersecurity market has a highly competitive sales culture, and personal relationships between sales representatives and security buyers are valued in the market. The US startup sales and marketing culture tends to be aggressive and fast-driving, which one interviewee said tends to cut against some Dutch cultural traits. Having a US presence with US salespeople who have existing relationships in the market is critical to entering the US market successfully. Many Israeli firms, for example, have at least a major US sales office and often hire an American into sales leadership positions, including Chief Revenue Officer or Global Head of Sales to target the US market. Many security buyers work with trusted salespeople across multiple companies. These trust relationships are highly important in the crowded and confusing US security market. The sales cycle for cybersecurity products is long and arduous, which Dutch firms should take into account. Cybersecurity sales take time and frequent touch points for success.

Finally, some firms choose to redomicile in the United States to provide a true American presence for the firm. Firms that have successfully used this model include Imperva, CyberArk, AlienVault, and Digital Shadows (Disclosure: Digital Shadows is a portfolio company of Paladin Capital). Often these firms keep development in the home country. Some US investors have covenants in their funds that require that they invest in North American-based companies and may ask that a legal entity be established in the United States as a precondition for investment. One interviewee whose Dutch firm counted the US as 60% of its revenue created a separate legal entity in the United States for tax and regulatory purposes but kept the intellectual property of the firm in the Netherlands. growth in the US market. There may be economic drawbacks for the Netherlands if Dutch cybersecurity companies redomicile in the US including tax implications, slower domestic innovation, and the potential for expertise to drift away from the Dutch market.

Whether Dutch companies choose to follow the model to remain fully incorporate in the Netherlands, have a separate legal entity in the US/North America, or fully redomicile in the United States, having a local, American-driven sales presence in the United States is the common link in companies that have successfully entered the US market. This requires local US sales and marketing that understands the sales cycle, landscape, and relationships in the US. While there are challenges for Dutch firms, entrance to the US market has been successful for a variety of European companies.

5b. Public Sector Barriers

The US public sector is a large and mature cybersecurity market, but there are barriers for Dutch firms to sell to federal agencies. First, according to an interviewee, US national security organizations including the Department of Defense and Intelligence Community are increasingly wary of foreign-developed cybersecurity technology, even from trusted allies like the Netherlands. This skepticism extends to companies that are domiciled in the United States but were originally foreign firms. In these cases, certifications including Common Criteria are prerequisites for federal sales success. There is also a trend towards a "Cyber Bill of Materials" in the federal space, which would require providers to list all software that are incorporated into a software build. While the Cyber Bill of Materials is still an emerging concept, it is valuable for Dutch firms to be aware of as customers develop greater conscientiousness of supply chain risks in IT and cybersecurity systems.

Even in civilian agencies, there are regulations and certifications that cybersecurity vendors must meet to sell to these agencies. The two major certifications required for federal security vendors are FedRAMP, which applies specifically to cloud vendors, and Authority to Operate (ATO), which lays out similar requirements for on-premises vendors. These certifications are based on NIST 800-53, which sets standards for federal agencies' cybersecurity. FedRAMP and ATO certifications can take multiple years and multiple millions of dollars to complete. For startups with novel solutions, federal agencies may grant an interim Authority to Operate for which the agency takes on the risk added by the vendor. Proof of concepts may also not require full certification until after they are complete and a purchase decision is to be made. Working through partners or contractors that have existing federal contracts and certifications is an easier method to enter the federal market than a direct sales model.

State and local governments are often an easier target in the public sector. State and local governments do not have the same stringent certification requirements that federal agencies do and often are more open to working with foreign firms than would be the US federal government. The sales cycle for state and local government is also typically faster and the contracting process less onerous than for federal agencies. While state and local governments usually operate with lower budgets than those of federal agencies, these entities consistently face major IT and security challenges. Winning contracts in states and localities may provide opportunities for Dutch firms to showcase the value of their products and services as well as build trust with public sector officials across the US.

5c. Other Legal and Regulatory Barriers

There are not traditional economic barriers for Dutch cyber firms entering the US, but the United States government has become increasingly aggressive at tracking foreign investment in firms that may touch national security. The Committee of Foreign Investment in the United States (CFIUS) reviews the national security risks of foreign investments in US companies or operations. CFIUS has assumed greater authority under the Trump administration and will likely retain it under the incoming Biden administration. For a Dutch company domiciled in the United States or with significant operations abroad, funders such as VC firms and their limited partners are under increased scrutiny. European VC and private equity firms have been the target of CFIUS action. In 2019, CFIUS forced a divestment from email security firm Cofense by Pamplona Capital Management because of Russian investment in Pamplona’s fund. CFIUS review may be a relatively unlikely risk, but important to bear in mind because of potential foreign investment in Dutch firms seeking to operate in the US.

Dutch firms that are operating in the US or have American employees/contractors should also be aware that they could be party to US export control laws. This is important in security given the dual-use nature of certain security products, including but not limited to vulnerability assessment software, penetration testing tools, and certain encryption products. Even with Americans working on certain products, Dutch firms could face requirements for sign-off prior to international sales or even internal transfer of certain technologies.

References & Resources

Section 2: Dutch Commercial Cybersecurity Ecosystem

- "Cyber security: European emerging market leaders," PwC, 2017. https://www.pwc.co.uk/deals/assets/cyber-security-european-emerging-market-leaders.pdf
- "Threat Intelligence Market by Application, Deployment Mode, Organization Size, Vertical, and Region - Global Forecast to 2025," Markets & Markets, 2020. https://www.marketsandmarkets.com/Market-Reports/threat-intelligence-security-market-150715995.html
- "Threat Intelligence Market Worth $20.20 Billion, Globally, by 2027 at 18.95% CAGR: Verified Market Research," Verified Market Research, April 2020. https://www.prnewswire.com/news-releases/threat-intelligence-market-worth-20-20-billion-globally-by-2027-at-18-95-cagr-verified-market-research-301107598.html
- "Data privacy as a strategic priority," Deloitte, 2019. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-data-privacy-as-a-strategic-priority.pdf
- "Data Privacy Law Tracker," Ballard Spahr LLP, 2020. https://www.cyberadviserblog.com/wp-content/uploads/sites/18/2019/06/State-Privacy-Law-Tracker-06-19.pdf
- "The consumer-data opportunity and the privacy imperative," McKinsey & Company, April 2020. https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

Section 3: *US Cybersecurity Market and Trends: Opportunities for the Netherlands*

- "Zero Trust Security Market - Growth, Trends, Covid-19 Impact, and Forecasts (2021 - 2026)," Mordor Intelligence, 2020. https://www.mordorintelligence.com/industry-reports/zero-trust-security-market
- "Data-Centric Security Market - Industry Analysis, Market Size, Share, Trends, Application Analysis, Growth and Forecast 2020-2025," Industry Arc, 2019. https://www.industryarc.com/Research/Data-centric-Security-Market-Research-500764
- "Rise of Advanced Cyber Threats Spurs Demand for Managed and Response Solutions," Frost & Sullivan, June 2020. https://ww2.frost.com/news/rise-of-advanced-cyber-threats-spurs-demand-for-managed-and-response-solutions-says-frost-sullivan/

- Why SASE is the in-time market disruption. Why now?" with Raj Gulani of Cisco, LightReading, December 2020. https://www.lightreading.com/why-sase-is-in-time-market-disruption-why-now/v/d-id/766344
- "Gartner: SASE Poised to Transform Cybersecurity," Security Boulevard, October 2019. https://securityboulevard.com/2019/10/gartner-sase-poised-to-transform-cybersecurity/
- "5 SD-WAN and SASE Predictions for 2021," SDxCentral, December 2020. https://www.sdxcentral.com/articles/news/5-sd-wan-and-sase-predictions-for-2021/2020/12/

Section 4: *Major Players in the US Market for Dutch Cybersecurity Companies*

- "How technology OEMs can guide channel partners to XaaS," Deloitte, October 2019. https://www2.deloitte.com/us/en/insights/industry/telecommunications/xaas-technology-oem-channel-partners.html
- "The top 11 VC investors in cybersecurity," PitchBook, June 2019. https://pitchbook.com/news/articles/the-top-11-vc-investors-in-cybersecurity
- "Washington DC Metro Area Cyber Security Companies," Crunchbase, 2021. https://www.crunchbase.com/hub/washington-dc-metro-area-cyber-security-companies/hub_overview_default/top?tab=top_orgs

Section 5: *Challenges and Barriers to Entry for Dutch Cybersecurity Companies*

- "Flipping up, not out: navigating the path to introducing a US holdco," Landers & Rogers, October 2019. https://landers.com.au/legal-insights-news/flipping-up-not-out-navigating-the-path-to-introducing-a-us-holdco
- "Evaluation Process (NIAP CCEVS) and Common Criteria Testing Laboratory Services - FAQ," National Information Assurance Partnership (NIAP). https://www.niap-ccevs.org/Ref/FAQ.cfm#cat27
- "Software Bill of Materials (SBoM) - Does It Work for DevSecOps?" AT&T Security, January 2019. https://cybersecurity.att.com/blogs/security-essentials/software-bill-of-materials-sbom-does-it-work-for-devsecops
- "2021 DevOps Predictions for the Software-Powered World," Forbes, February 2021. https://www.forbes.com/sites/forbestechcouncil/2021/02/08/2021-devops-predictions-for-the-software-powered-world/?sh=99573b53bba9

- "Top Five Cybersecurity Requirements for Government Contractors," Winvale, September 2020. https://info.winvale.com/blog/top-five-cybersecurity-requirements-for-government-contractors

- "FedRAMP Agency Authorization Playbook (PDF)." https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf

- "New CFIUS Rules – Eight Key Points," JDSupra, January 2020. https://www.jdsupra.com/legalnews/new-cfius-rules-eight-key-points-33495/

- "New CFIUS regulations change mandatory filing requirements and increase the importance of US export controls," DLA Piper, September 2020. https://www.dlapiper.com/en/us/insights/publications/2020/09/new-cfius-regulations-change-mandatory-filing-requirements/#:~:text=Under%20the%20existing%20CFIUS%20regulations,either%20used%20by%20the%20US

This is a publication of
Netherlands Enterprise Agency
Prinses Beatrixlaan 2
PO Box 93144 | 2509 AC The Hague
T +31 (0) 88 042 42 42
E klantcontact@rvo.nl
www.rvo.nl

This publication was commissioned by the ministry of Foreign Affairs.

Publicationnumber: RVO-083-2021/RP-INT

NL Enterprise Agency is a department of the Dutch ministry of Economic Affairs and Climate Policy that implements government policy for Agricultural, sustainability, innovation, and international business and cooperation. NL Enterprise Agency is the contact point for businesses, educational institutions and government bodies for information and advice, financing, networking and regulatory matters.

Netherlands Enterprise Agency is part of the ministry of Economic Affairs and Climate Policy.