

Cybersecurity Report

Agence Wallonne à l'Exportation et aux
Investissements Étrangers



EMBASSY OF BELGIUM


Wallonia.be

January 2022

Embassy of Belgium

Authored by: AWEX - Washington D.C.



Table of Contents

Executive Summary	3
Agencies	4
US Cyber Budget Allocation	6
American Cybersecurity Private Sector Market	8
Cybersecurity in the American Education System	11
Executive Order on Improving the Nation’s Cybersecurity	14
Most Common Types of Cyber-Attacks	16
Case Studies	21
Largest US Cybersecurity Firms	25
.....	

Executive Summary

Since the end of the Cold War, the United States has been the global superpower in terms of economic strength, political influence, and military dominance. The US remains the main stakeholder in most international organizations such as the World Bank, NATO, the UNSC, and more. However, in the contemporary political landscape, there are increasingly more domestic and international threats that experts claim may pose a hazard for American global preeminence. Perhaps one of the most overarching international and domestic threatening arenas is that of cybersecurity.

The US is known as one of the most technologically advanced nations as a result of the active participation and investment in the cybersecurity space by the Federal Government, the armed forces, civil society, the private sector, and academia. The US is home to the world's largest cyber firms, including Google, Amazon, Microsoft and Apple, as well as home to the most developed technological hubs that further drive innovation such as Silicon Valley. The US also retains the most technologically adept and incorporated military which is highlighted by the head of the US Cyber Command (USCYBERCOM), General Paul Nakasone, who stated that US international cyber strategy – in peace and war - is to “achieve and maintain cyberspace superiority.”

Since the realm of cybersecurity changes and adapts so quickly, the US has recently issued several reports and Executive Orders to combat the evolving threats within the cyberspace which may have severe palpable repercussions, including [the National Cyber Strategy of the United States](#), [the Department of Defense Cyber Strategy](#), and the [Executive Order on Improving the Nation's Cybersecurity](#). According to these documents, the US has a tri-pronged strategy in terms of cybersecurity: homeland defense, low-intensity conflict, and high-intensity conflict.

Homeland defense, in terms of cybersecurity, pertains to protecting the nation's critical infrastructure, such as the national power grid, domestic financial services, intellectual property, and food & agriculture infrastructure, from foreign threats that seek to cause harm to or destabilize the day-to-day operations of the US. In terms of low- and high-intensity conflicts, the US strategy aims to provide cyber-attack options in all phases of operations and at every level of command; on the defensive side, the aim is to ensure that cyber defenses are highly resilient, instantaneous, and unified among all areas affected.

This report delves into the myriad components of what makes up the cyber capabilities of the United States. Such aspects of the report include: the different governmental agencies working in cybersecurity, an overview of the US cyber budget allocation, an analysis of a cyber-driven Executive Order, a summary of the most prevalent types of cyber-attacks, case studies regarding several significant cyber-attacks, reviews of the major US companies working in cybersecurity, and lastly, the analysis of the cyber capabilities of the main US geopolitical rivals such as North Korea, Iran, China, and Russia.

Agencies

Cybersecurity is an increasingly omnipresent reality of domestic and international relations, as a result nearly every single federal agency within the US maintains a cybersecurity branch to effectively fulfill and defend their duties. In US cyber policy there are many channels of executive authority that flow from the president: the intelligence community (IC), the armed forces (USCYBERCOM), FCEB's (Homeland Security, Justice, Commerce, Energy and Transport), and other agencies (such as National Laboratories). These are all coordinated through the National Security Council (NSC), chaired by the president, and its Principals Committee, chaired by the National Security Advisor.

One of the main cybersecurity agencies is the Department of Homeland Security (DHS) which is the lead for coordinating the overall national effort to enhance the cybersecurity of US critical infrastructure, as well as ensuring protection of the civilian federal Government networks and systems (such as official Government websites). The key independent branch within DHS that specializes in cyber space is the Cybersecurity and Infrastructure Security Agency (CISA). CISA is tasked with protecting secure Government networks and with facilitating collaboration with the private sector to increase the cybersecurity of civilian networks.

The National Security Agency is an intelligence agency of the DOD responsible for the collection and analysis of foreign communications and foreign signals intelligence, as well as protecting US Government communications and information systems, especially in the realm of cyberspace. The NSA consists of several different branches with unique mandates, with the newly formed Cybersecurity Directorate, led by [Rob Joyce](#), formerly the DHS Acting Secretary, being tasked with integrating the NSA's cybersecurity mission to prevent and eradicate threats to the nation's most sensitive systems and critical infrastructure.

In order to update the White House's cyber strategy, in January 2021, President Biden established the position of Deputy National Security Advisor for Cyber and Emerging Technology, led by [Anne Neuberger](#), to bolster executive defense following the SolarWinds cyber-attack. This new position is distinct from other cybersecurity agencies on account of it not being subject to congressional red-tape since it falls under the authority of the President. This new position will be tasked with enforcing the cyber-related Executive Orders instituted by the respective President. It will also push to synthesize a more coordinated response from all relevant cyber agencies/branches to potential cyber-attacks.

Another critical agency that partakes in cybersecurity is the Federal Bureau of Investigation (FBI) which is responsible for the detection, investigation, prevention, and response within the domestic arena under its authorities for law enforcement, domestic intelligence, counterintelligence, and counterterrorism. For instance, when malicious cyber activity is detected in the domestic cyber space, the FBI's National Cyber Investigative Joint Task Force (NCIJTF), takes the lead to prevent, investigate, and mitigate it.

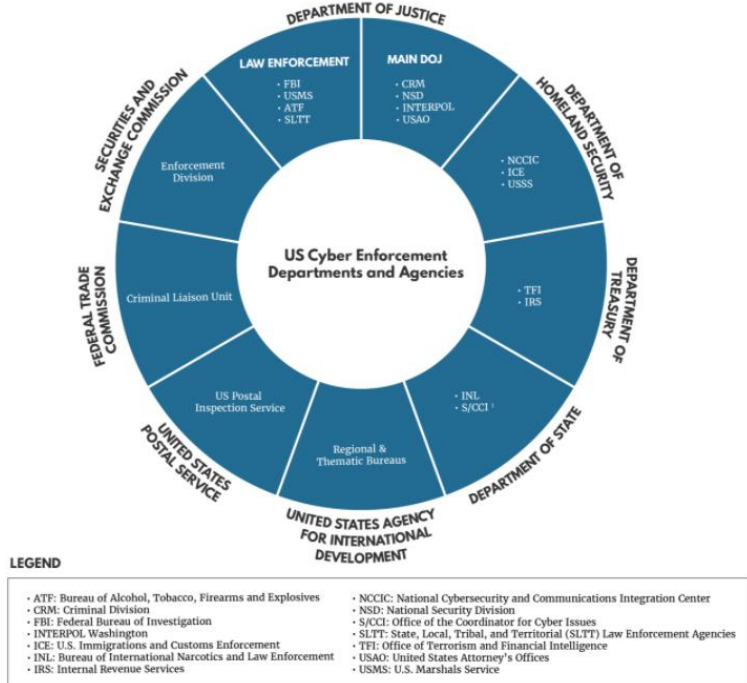
While the FBI operates in the domestic cybersecurity sphere, USCYBERCOM and the IC (CIA, NSA, ODNI) are responsible for detection, prevention, and defense in foreign cyber space, foreign cyber-threat intelligence and attribution, security of national security and military systems; and, in cases of high-intensity conflict, the defense of the country if the Nation comes under cyber-attack from an invasive actor.

Aside from the various cybersecurity offices within the Federal Government, there are also several civil-sector organizations that effectively collaborate with Federal Agencies to advance cyberspace goals. One such organization for this has been the President’s [National Infrastructure Advisory Council \(NIAC\)](#), which brings together senior executives from the private sector and state and local governments to advise on how to reduce physical and cyber risks and improve the security and resilience of the nation’s critical infrastructure sectors.

Another strategic initiative focusing on civil cybersecurity is the [Information Sharing and Analysis Centers \(ISACs\)](#) which are the coordinating bodies designed to maximize information flow across the private sector critical infrastructures and with the Government. ISACs enables the sharing of cyber threats and mitigation strategies among and with Government and private sector partners during both steady conditions and incidents requiring cross-sector responses. There are currently 26 different private-sector Centers including the aviation, real estate, education, media, and oil sectors.

An additional civil cybersecurity organization is the [National Initiative for Cybersecurity Education \(NICE\)](#) which is within the National Institute of Standards and Technology in the Department of Commerce. NICE is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing programs, facilitate change and innovation, and to increase the number of skilled cybersecurity professionals to protect the country.

Lastly, the [Cyberspace Solarium Commission](#), established in 2019, is a bicameral, bipartisan commission comprised of 10 commissioners including four legislators and five cyber experts from outside of Government that is tasked with developing an annual report recommending and outlining a coherent and proactive cybersecurity national strategy. Such recommendations indicated in the Commission’s report include: institutionalize international cyber engagement, investing in the resiliency of technological infrastructure, and to decree a clear policy of cost imposition to parties that initiate cyber-attacks against the US Government or its citizens.



This list of federal departments and agencies is not exhaustive. It is a compilation of key government entities with a core mission in cyber enforcement. There are many other federal entities who work in this area.
 1. Currently, the Office of the Cyber Coordinator for Cyber Issues has been folded into the Division of International Communications and Information within the Bureau of Economic and Business Affairs. There is Congressional legislation to establish an Office of International Cybersecurity Policy at the State Department, with the office reporting to the undersecretary of state for political affairs.

US Cyber Budget Allocation

According to the [2021 SonicWall Cyber Threat Report](#), since 2019, ransomware attacks on a global scale has increased by 62%, with a 158% spike in North America alone. In fact, in 2020, the Federal Bureau of Investigation (FBI) disclosed that there were [“over \\$4 billion in cybercrime losses reported to the US Government for the entirety of year.”](#) This growing cyber exploit threats have only been exacerbated by the progression of the 21st century by virtue of an increase in the variety and scope of non-traceable cryptocurrencies, the rise of more malicious non-state actor hacking groups, and the bolstering of cyber-attack operations by both nation-states and their sanctioned proxy units. From the devastating effects of the Colonial Pipeline hack in 2020 that showed the potential for hackers to completely, even temporarily, upend one of the most crucial energy sources of the US, to the 2017 SolarWinds hack that led to the infiltration and subsequent destruction of tens of thousands of private and public computer servers that contained sensitive material regarding national security – it is clear that the multitude and magnitude of cyber-attack is only set to increase in the near future.

As a result, the Biden Administration has been undertaking major steps to strengthen US cyber defenses, capabilities, and preparedness. The FY2021 National Defense Authorization Act (NDAA) created the position of US National Cyber Director, tasked to lead the implementation of US cyber policy, strategy, and defense. In addition, the Department of Energy (DOE) and the Department of Homeland Security (DHS) [have both made cybersecurity a top priority in their latest initiatives.](#) President Biden called on DOE to launch a 100-day plan aimed at preventing disrupted services for electric utilities, and DHS announced a series of 60-day endeavors to support private and public partners against ransomware.

Table 12–2. ESTIMATED CIVILIAN FEDERAL CYBERSECURITY SPENDING BY AGENCY
(In millions of dollars)

Organization	FY 2020	FY 2021	FY 2022
Civilian CFO Act Agencies	\$7,383	\$8,184	\$9,402
Department of Agriculture	\$223	\$223	\$239
Department of Commerce	\$701	\$472	\$422
Department of Education	\$123	\$165	\$225
Department of Energy	\$590	\$711	\$793
Department of Health and Human Services	\$544	\$598	\$715
Department of Homeland Security	\$1,613	\$2,097	\$2,409
Department of Housing and Urban Development	\$73	\$81	\$76
Department of Justice	\$903	\$934	\$1,241
Department of Labor	\$101	\$109	\$105
Department of State	\$284	\$320	\$447
Department of the Interior	\$106	\$124	\$144
Department of the Treasury	\$556	\$653	\$829
Department of Transportation	\$267	\$334	\$345
Department of Veterans Affairs	\$426	\$472	\$450
Environmental Protection Agency	\$29	\$28	\$29
General Services Administration	\$77	\$80	\$78
National Aeronautics and Space Administration	\$162	\$155	\$187
National Science Foundation	\$241	\$244	\$256
Nuclear Regulatory Commission	\$28	\$27	\$25
Office of Personnel Management	\$47	\$44	\$44
Small Business Administration	\$16	\$17	\$17
Social Security Administration	\$216	\$243	\$266
U.S. Agency for International Development	\$57.7	\$54.2	\$58.1

Further, in President Biden’s FY22 Budget, [Federal civilian cyber spending increased about 14% to a total of approximately \\$9.8 billion for all 17 of the Departments](#), which is due to “secure Federal civilian networks, protect the Nation’s infrastructure, and support efforts to share information, standards, and best practices with critical infrastructure partners and American businesses.” This funding also includes \$110 million for the Cybersecurity and Infrastructure Security Agency (CISA), \$500 million for the Technology Modernization Fund, and an extra \$750 million to agencies affected by recent, significant cyber incidents to address exigent gaps in security capability. The Budget also provides \$15 million to support the Office of the National Cyber Director established in the FY21 NDAA. As a result of this drastic increase, the cyber budgets for all 17 civilian Departments now nearly equals the Department of Defense’s (DOD) cyber operations budget of approximately \$10.4 billion.

With the growing threat of cyber-attacks looming in the near future from rival nation-states, malicious proxy groups, or other non-state actors, it is imperative for the US to continue to modernize and fortify its cyber budgets in order to maximize cyber

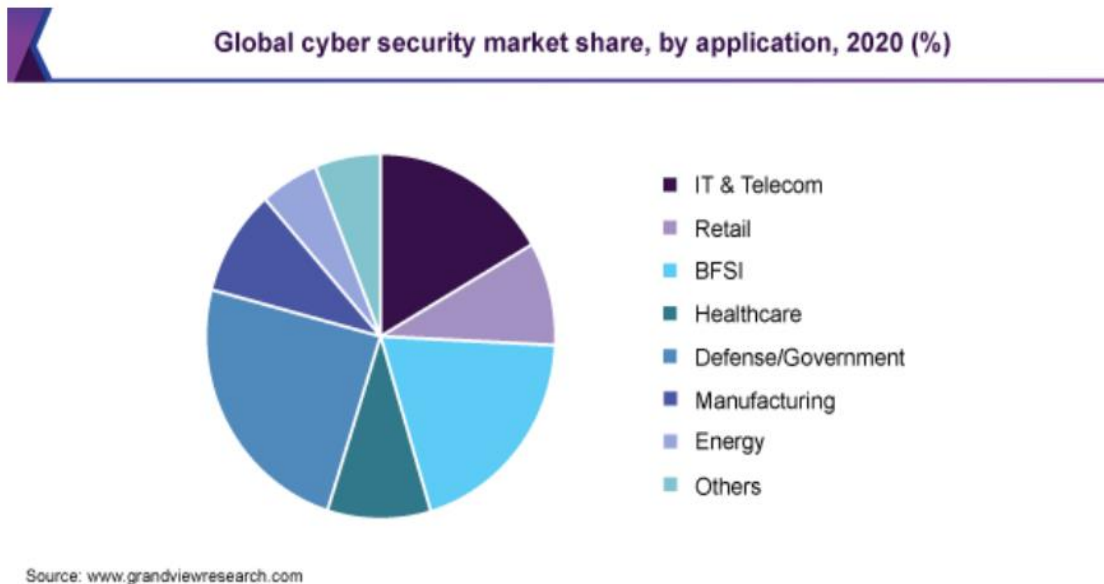
defenses, capabilities, and preparedness. The current Administration is indeed taking the appropriate steps to meet these future challenges, however, only the continued monetary allocation of cyber related investments within the Federal Government will ensure that the US will successfully meet the challenges of tomorrow.

In-Depth Analysis of US Cyber Capabilities Budget Allocation FY22

Agency and programs	2022 Total	Increase/decrease from 2021
CISA: Administrative Subpeona	\$5,000,000.00	\$5,000,000.00
CISA: Capacity building	\$124,951,000.00	\$3,207,000.00
CISA: Cyber excercises	\$10,022,000.00	\$1,800,000.00
CISA: Cyber response and recovery fund	\$20,000,000.00	\$20,000,000.00
CISA: CyberSentry	\$8,158,000.00	\$-??
CISA: Hunt and Incident Response Team	\$64,233,000.00	\$7,017,000.00
CISA: infrastructure security	\$175,300,000.00	Null
CISA: Joint Cyber Planning Office	\$10,600,000.00	\$10,600,000.00
CISA: National Risk Management Center	\$113,928,000.00	\$6,652,000.00
CISA: Operational planning and coordination	\$79,890,000.00	\$10,153,000.00
CISA: stakeholder engagement	\$58,180,000.00	\$12,455,000.00
CISA: Threat hunting	\$158,883,000.00	\$(1,568,000.00)
CISA: Vulnerability managment	\$144,537,000.00	\$(516,000.00)
Commerce: NIST-Cybersecurity and Privacy	\$81,900,000.00	\$
DHS: State Homeland Security Grant Program	\$44,601,450.00	\$(15,314,000.00)
DOE Cybersecurity, Energy Security, and Emergency Response..	\$25,000,000.00	\$25,000,000.00
DOE Cybersecurity, Energy Security, and Emergency Response..	\$25,000,000.00	\$25,000,000.00
DOJ: Criminal Division	\$215,173,000.00	\$17,919,000.00
DOJ: Economic, high-tech, white collar	\$13,000,000.00	\$1,000,000.00
DOJ: Intellectual Property Enforcement Program	\$2,500,000.00	\$-??
DOJ: Interpol Washington	\$40,993,000.00	\$5,401,000.00
DOJ: National Security Division	\$123,093,000.00	\$5,642,000.00
EPA	\$3,873,000.00	\$3,873,000.00
FBI: Cyber investigation resources	\$40,000,000.00	\$
ICE: Homeland Security Investations' Domestic investigation (..	\$1,877,754,000.00	\$21,821,000.00
IRS: Cybercrimes and applied data analytics	\$41,095,000.00	\$
IRS: enhance enforcement operations	\$32,340,000.00	\$
State: cyber dimplomacy and technology policy	\$9,832,000.00	\$9,832,000.00
State: INL Cybercrime and IPR	\$20,000,000.00	\$10,000,000.00
TSA	\$3,000,000.00	\$
USSS: Computer Forensics training	\$37,160,000.00	\$2,783,000.00
USSS: Domestic and international field operations	\$705,391,000.00	\$18,808,000.00
USSS: investigative operations	\$51,000,000.00	\$300,000.00
White House: National Cyber Director	\$15,000,000.00	\$15,000,000.00

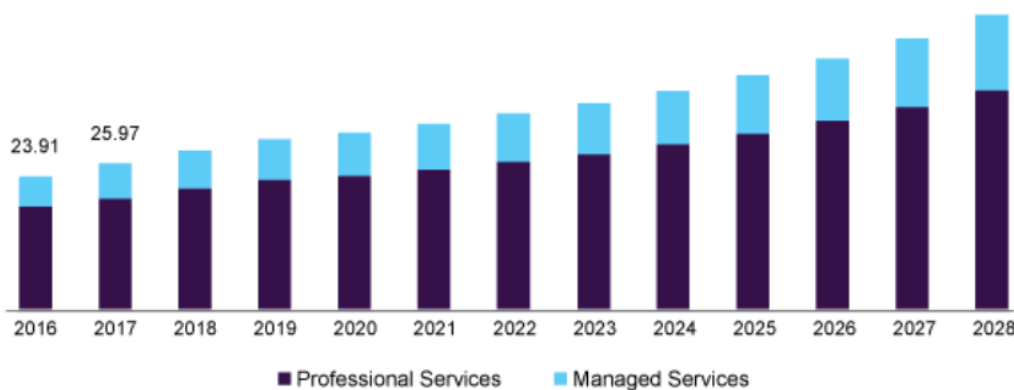
American Cybersecurity Private Sector Market

According to the Department of Labor’s Bureau of Labor Statistics, employment of information security – of which cybersecurity encompasses – is [projected to grow 33% year-over-year from 2020 to 2030](#), much faster than the average for nearly all other occupations. In fact, the global market share for cybersecurity in 2021 [amounted to approximately \\$180 billion dollars](#), up from \$167 billion the year prior in 2020, marking a 7.7% increase; and up from \$42 billion in 2017, signifying an overall increase of nearly 330%. Trends indicate that this market share is only going to increase with each passing year as the digital world becomes more enveloped in everyday life and society. The main sectors within cybersecurity private industry that are bound to exponentially grow are IT & telecom, retail sale, banking & financial services, insurance, healthcare, defense, manufacturing, and energy.



This clear trend of technological expansion and augmentation will be further fueled by the advent and honing of new technologies. Phenomena such as [artificial intelligence \(AI\), quantum computing, 5G bandwidth, and others](#) will inevitably disrupt existing digital paradigms which, as a result, will inextricably be linked with cybersecurity as it evolves to secure future information systems. This is evident by measuring the amount of funding by venture capitalist firms. For instance, according to [a recent cybersecurity market review](#), investors funded more than \$11.5 billion in total venture capital financing into cybersecurity startups in the first half of 2021, up from \$4.7 billion during the same period a year earlier, marking an increase of nearly 144%.

U.S. cyber security market size, by service, 2016 - 2028 (USD Billion)



Source: www.grandviewresearch.com

Unsurprisingly, the US spends more - both in terms of Federal Government and private sector investment – in cybersecurity. According to a [2020 report on the status of cybersecurity positions around the world by International Telecommunications Union \(ITU\)](#), the US ranked at the top in terms of cybersecurity legal measures, technical measures, organizational measures, capacity, development measures, cooperation measures.

What’s more, the US is also home to the largest and most significant cybersecurity companies in the world. Aside from the prodigious and wide-reaching technological companies who also partake in some aspects of cybersecurity (such as Microsoft, IBM, Apple, and others), the US harbors the leading global private cybersecurity vendors as well such as Cisco, Palo Alto Networks, and Fortinet. To reinforce, [in the first quarter of 2020](#), Cisco accounted for 9.1% of the market share in the cybersecurity industry, while Palo Alto Networks and Fortinet accounted for 7.8% and 5.9% respectively.

While it is clear that this sector is on the rapid rise and that there are no shortcomings on new technological advancements on a regular basis, one aspect of the market that is worrisome for the US cybersecurity market (and that of the world) is the widening gap of available cyber employment positions and actual cybersecurity-trained available workers.

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15

To reiterate, according to a newly-published [2021 International Information System Security Certification Consortium \(ISC\)2 Cybersecurity Workforce Study](#) which collected survey data from 4,753 cybersecurity professionals working with small, medium, and large organizations throughout North America, Europe, Latin America, and the Asia-Pacific, it is estimated that the US now has more than 1.1 million cybersecurity professionals, which is an increase from about 880,000 in 2020, a 13.6% increase, but still leaves an employment gap of approximately 377,000 in the totality of the US.

The report also states that there about 4.19 million cybersecurity professionals worldwide, which is 700,000 more compared to the year 2020, which essentially narrowed the global skills gap from 3.1 million to 2.7 million.

This substantial gap is among the sources for the constant flow of cyber-attacks to the US. Some of the major pitfalls that result from the gap include: the misconfiguration of systems, slower time to patch system exploits, not enough resources for proper risk assessment and management, oversights in processes and procedures, the inability for systems to remain aware of all threats against networks, and can lead to the rushed deployment of systems without taking all the necessary precautions to confirm the fortifications of respective systems.

All areas of cybersecurity are affected by this staff shortage. The report indicates that there are seven major categories that are most affected by the skill gap: securely provision systems (48%), analysis of systems (47%), protection & defense (47%), oversight and governing (43%), operation and maintenance (39%), investigative (39%), and collection & operation (32%). These statistical and tangible concerns are the reasons as to why two-thirds (60%) of study participants report that the cybersecurity staffing shortage is placing their organizations at risk.



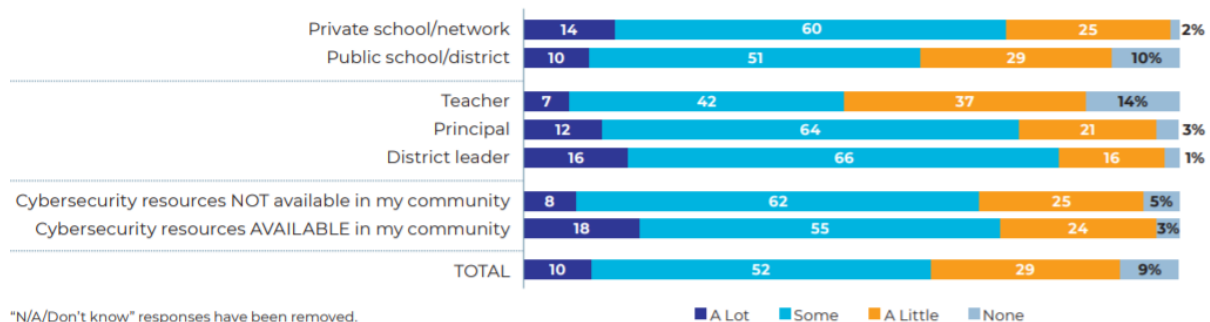
Cybersecurity in the American Education System

The increasing omnipresence of global cyber-threats, paired with the noteworthy skills gap within the cybersecurity sector, have led both the US Federal Government and academic institutions to adopt substantial and far-reaching initiatives and programs to overhaul the contemporary American educational system in order to cater to more cyber-related studies and domains.

IBM General Manager of Government and Education Courtney Bromley [stated in a recent interview](#) that “cybersecurity is one of the most in-demand skills across all industries... there’s a huge gap that exists between the continued high demand for cybersecurity professionals and the ongoing shortage of talent.” To that end, according to the US Department of Labor’s Bureau of Labor Statistics (BLS), jobs in information security and cybersecurity are projected to [grow by 31% by 2029 as demand for IT talent increases](#) in both the public and private sectors.

Currently, however, the US seems unequipped to meet the cyber-related challenges that the future will inevitably hold. For example, [a recent 2020 survey by a cyber think-tank discovered](#) that less than half of K-12 students were receiving any cyber education at school at all. Schools with lower-income students received even less cyber education than those with higher-income students. In fact, 91% of educators who responded to the survey say they know relatively little about the subject. Adding on, [solely 35% of high schools](#) teach some form of computer science nationwide while only 28 states have computer science standards written for the students.

How much do you know about cybersecurity education?



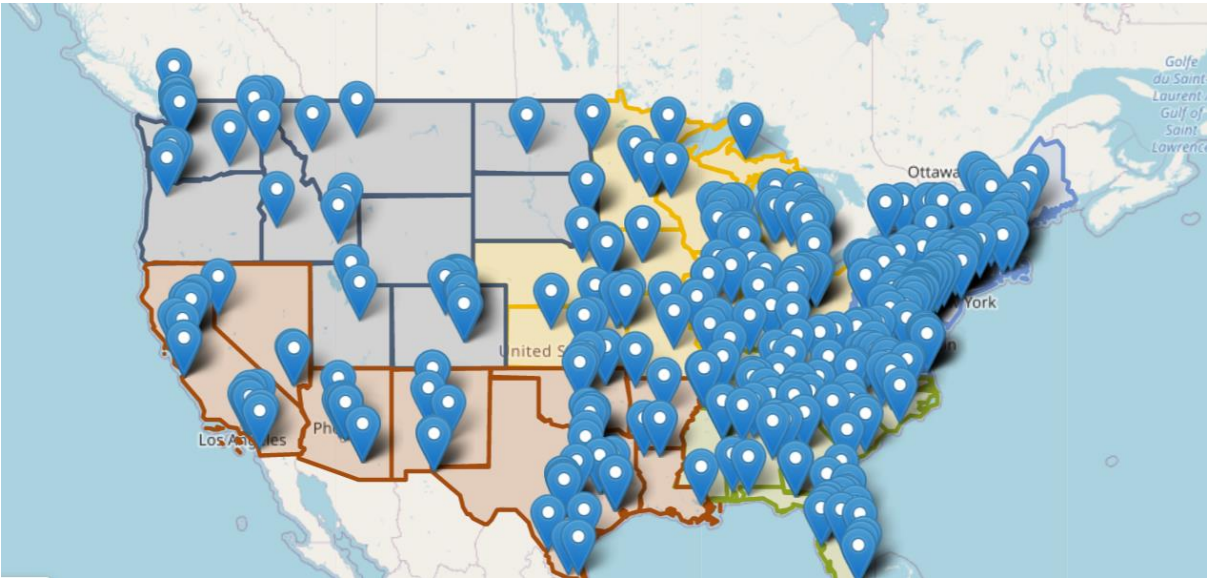
As a result, several US Federal agencies have begun to provide grants and initiatives to schools nationwide in order to bolster cyber wherewithal. For instance, the Department of Homeland Security (DHS) has partnered with various nonprofits, middle and high schools, universities and state school boards across the country to help incorporate cybersecurity concepts into educational curricula. DHS has also partnered with the [National Integrated Cyber Education Research Center \(NICERC\)](#) to provide an array of cyber curricula and hands-on training for teachers at no cost to the respective school district. The curriculum is focused on subjects like Cyber Fundamentals, Algebra I and Computational Thinking. As of 2018, DHS asserts that NICERC has taught over 13,500 teachers and reached more than 2.1 million students nationwide.

There are also a myriad of university-level programs and initiatives that aim to partner academia with the Federal Government. For example, the [National Initiative for Cybersecurity Education \(NICE\)](#) is a partnership between government, universities, and the private sector focused on supporting the nation’s ability to address current and future cybersecurity education and workforce challenges by advancing an integrated ecosystem of cybersecurity guidance, training, and workforce development. NICE is led by the National Institute of Standards and Technology (NIST) in the Department of Commerce.

In addition, the DHS and the National Security Agency (NSA) jointly sponsor the [National Centers of Academic Excellence \(CAE\) program](#), designating specific colleges and universities as top schools in Cyber Defense Education (CAE-CDE), otherwise known as ‘Centers of Excellence.’ Schools are selected based on their close alignment to particular cybersecurity-related [knowledge units \(KUs\)](#), validated by top cybersecurity professionals. CAE graduates are streamlined into a career path that enables them to protect commercial networks, national security information systems, and critical information infrastructure in the private and public sectors.








As of 2020, there are 200 CAE-CDE programs at the Associate, Bachelor’s, Master’s and Doctoral levels. There are also 21 undergraduate and graduate level CAE in Cyber Operations (CAE-CO) programs, which are more technically-based than the CDE programs. Additionally, the NSA has designated 77 CAE in CD Research (CAE-R) programs as of 2020. The increasing propensity of these programs is indeed a clear indication that the US deems it critical to increase the understanding of cyber defense technology and policy among the entire spectrum of university education.

National Centers of Academic Excellence University Map



What’s more, the DHS also co-sponsors the [CyberCorps: Scholarship for Service \(SFS\)](#), which provides scholarships for bachelors, masters and graduate degree programs focusing on cybersecurity in exchange for service in Federal, state, local or tribal governments upon graduation. The scholarship has the ability to partially or completely cover all tuition expenses for eligible full-time cyber students. The scholarships are funded through grants awarded by the National Science Foundation (NSF) in partnership with DHS and the Office of Personnel Management (OPM).

According to the BLS, the average salary for cybersecurity analysts, also known as information security analysts, is approximately \$103,590 in 2020. This median pay is expected to increase as the demand for these jobs gradually increases with each passing year. To that end, the US is home to among the best universities that offer degrees in cybersecurity. According to a [2022 survey conducted by a cyber nonprofit](#), the top universities include: Stanford University, Carnegie Mellon University, Johns Hopkins University, the University of Texas at Austin, the University of Southern California, the Georgia Institute of Technology, Purdue University, the University of Massachusetts Amherst, and the University of Pennsylvania.

Quick Facts: Information Security Analysts	
2020 Median Pay 	\$103,590 per year \$49.80 per hour
Typical Entry-Level Education 	Bachelor's degree
Work Experience in a Related Occupation 	Less than 5 years
On-the-job Training 	None
Number of Jobs, 2020 	141,200
Job Outlook, 2020-30 	33% (Much faster than average)
Employment Change, 2020-30 	47,100

As a result of these joint developments, coupled with an increase in cyber readiness, it is approximated that there are about [187 American universities that now offer cybersecurity degrees](#). The majority of them are centered on standardized frameworks for cybersecurity defense or focused on basic criminal forensics. These degrees are generally not warfare-related (unlike those of adversarial countries such as North Korea and China) which leads some experts to assert that this leaves the US at a general disadvantage unless more cybersecurity programs are shifted to include more offensive-based curricula. This issue has only been [exacerbated by the increase in teleworking and virtual schooling](#) as a result of the pandemic which propelled leadership in education and government to ramp up training and implementation of digital security.

Executive Order on Improving the Nation's Cybersecurity

On May 12, 2021, [President Biden released an Executive Order \(EO\)](#) aimed at improving the nation's collective cybersecurity preparedness and response among Federal Agencies and Federal contractors. The Order's 18-pages focuses primarily on obliging deadlines to all Federal Agencies, including Federal Civilian Executive Branch (FCEB) Agencies, the Intelligence Community (IC) Agencies, and the Department of Defense (DOD) in developing guidelines, standards, and requirements pertaining to the efforts of the Federal Government to identify, deter, protect against, detect, and respond to cyber-threats and attacks by malicious actors.

The EO recognizes that in order for the Government to counter the myriad cyber-threats facing the country, the Federal Government must partner with applicable organizations from the private sector. The EO outlines plans to transform the cybersecurity capabilities of the country's Federal Agencies to conduct and implement significant investments and changes to "protect and secure its [Federal Government] computer systems, whether they are cloud-based, on-premises, or hybrid."

The EO is separated into four main portions: *i. preventing intrusion* (cloud services; multi-factor authentication; software supply chain standards; "Internet of Things" (IoT) transparency), *ii. minimizing impact of intrusion* (data encryption; zero trust environment), *iii. detecting and responding to intrusion* (notification requirements; required vendor cooperation; additional information sharing; uniform incident response playbook; endpoint detection and response; centralized threat-hunting; logging requirements), and *iv. lessons learned* (Cyber Safety Review Board).

i. Preventing intrusion: A principal aspect of the EO relates to the removal of barriers to sharing threat information from Government service providers and Federal Agencies. The service providers, such as cloud service providers, possess unique access to and insight into cyber threat and incident information vis-à-vis Federal Agencies' information systems. The EO will remove the contractual terms and obligations that may currently limit the sharing of such threat or incident information with applicable agencies. The removal of such contractual barriers will consequently increase the sharing of information about cyber-threats, incidents, and risks in efforts to accelerate incident deterrence, prevention, and response to enable more effective defense of agencies' information systems. To that end, the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT (informational technology) and OT (operational technology) service providers and recommend updates to such requirements and language to the FAR Council and other appropriate agencies. The revisions will be made by the Director of Office Management and Budget (OMB), the Attorney General, Secretary of Homeland Security (DHS) and the Director of National Intelligence (DNI).

ii. Minimizing impact of intrusion: Another key aspect of the EO is that of modernizing approaches and responses to cyber threats of the Federal Government, while ensuring the protection of privacy and civil liberties of citizens. The EO makes it clear that the Federal Government must adopt security best practices such as the

advancement towards Zero-Trust Architecture which allows users (potential service providers) full access but only to the bare minimum they need to perform their jobs; if a device is compromised, Zero-Trust can ensure that the damage is contained to only the portions that the user was given access to. Other steps to modernize the Government's approach in dealing with cyber-threats include accelerating informational movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), centralizing access to cybersecurity data to drive analytics for identifying cyber risks, and investing in both technology and personnel to correspond with these modernization goals.

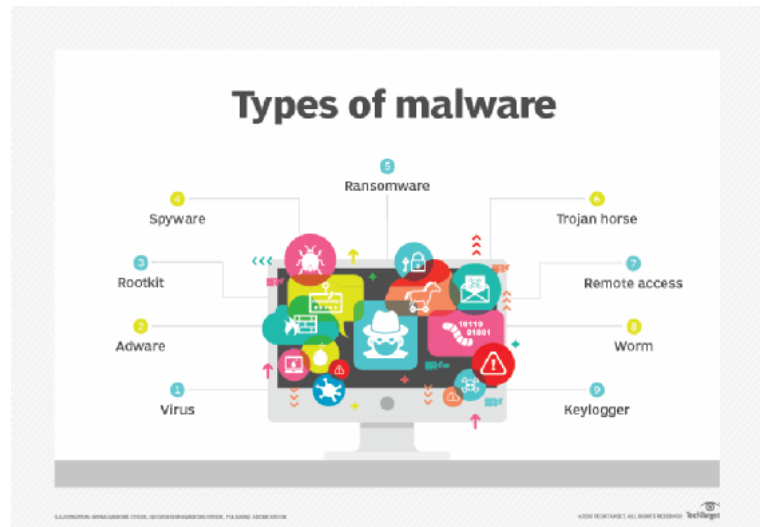
iii. Detecting and responding to intrusion: In addition, the EO orders the establishment of a collective framework to collaborate on cybersecurity and incident response activities related to FCEB cloud technology in order to guarantee effective information sharing among and between agencies and cloud service providers. The EO also calls for the Federal Government to rapidly improve the security and integrity of its software supply chain, with a priority on addressing critical software, which the EO defines as a "software that performs functions critical to trust (such as affording or requiring elevated system privileges of direct access to networking and computing resources." The Government will accomplish this by soliciting input from Federal Agencies, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools and best practices for complying with the standards, procedures, or criteria deemed necessary.

iii. Detecting and responding to intrusion: In terms of investment, the EO directs the Department of Commerce and the National Institute of Standards and Technology (NIST) to initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of IoT devices and software development practices, as well as consider ways to incentivize manufacturers and developers to participate in these programs. The new planned criteria is expected to reflect the increasingly comprehensive levels of testing and assessment that a product may have undergone, and will be compatible with existing labeling schemes that manufactures use to inform consumers about the security of their products. This is significant because it signals that the Federal Government intends to overhaul its approach to private sector cybersecurity products in order to keep consumers involved and informed about the security capabilities of available products. It also indicates that the Government wants to collaborate more with technologically superior manufacturers and producers to equip itself with the most up-to-date cyber technology available in both the private and public sectors.

iv. Lessons learned: The EO also requires the establishment of a Cyber Safety Review Board which is expected to review and assess significant cyber incidents affecting FCEB Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses. The Board will consist of Federal officials from DHS, NSA, CISA, FBI, and other pertinent Agencies in order to provide recommendations for offering a more unified approach to cybersecurity and incident response practices.

Most Common Types of Cyber-Attacks

Malware: Otherwise known as malicious software, is any program or file that is harmful to a computer user. Such malicious programs can perform a variety of functions such as stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity. There are several types of malware such as computer viruses, worms, Trojan horses and spyware. All types of malware are designed to exploit devices at the expense of the user and to the benefit of the perpetrator source.



Phishing: The cyber-crime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.

The infographic, titled "The Bait", is set against a light blue background. On the left, there is a cartoon blue character with a brain for a head, a password field with four asterisks, a mouse cursor pointing at it, and a shark fin. On the right, there are three white text boxes with blue borders. The first box says: "Scammers use familiar company names or pretend to be someone you know." The second box says: "They ask you to click on a link or give passwords or bank account numbers. If you click on the link, they can install programs that lock you out of your computer and can steal your personal information." The third box says: "They pressure you to act now — or something bad will happen."

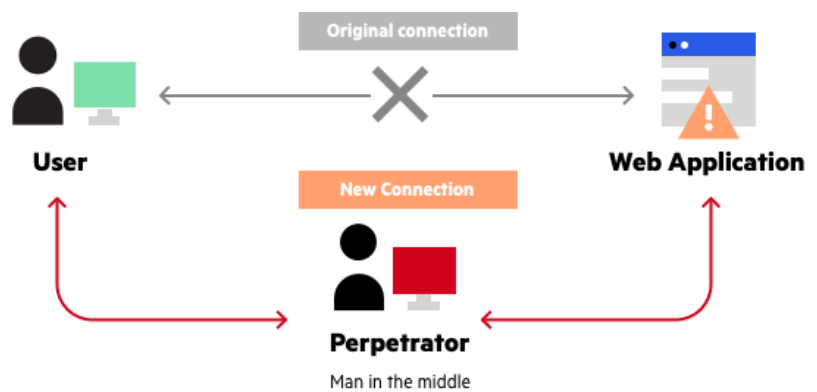
Ransomware: Ransomware is a prominent subgroup of malware that essentially encrypts a victim's digital files. The perpetrator subsequently demands a ransom from the victim to restore access to the data upon payment. Users are often shown instructions for how to pay a ransom fee to get the decryption key or code. The ransom fees are often ordered to be paid through cryptocurrency such as Bitcoin or Ethereum.



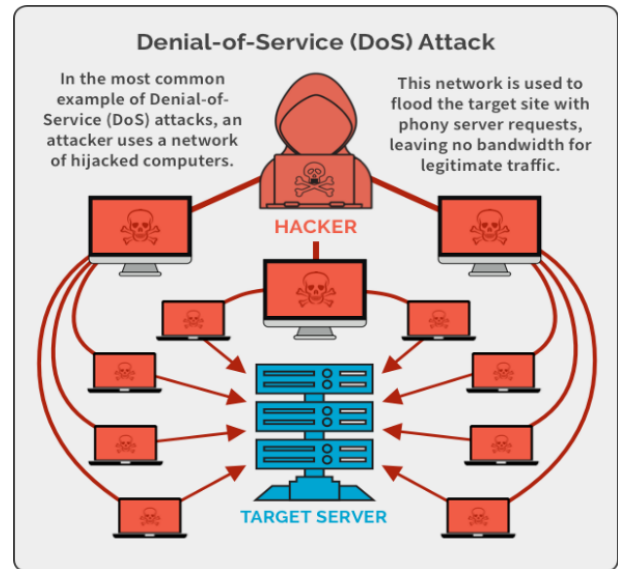
Ransomware pop-up page from the 2017 worldwide cyber-attack “WannaCry” which spread to more than 230,000 computers.

Man-in-the-Middle Attacks (MITM):

MITM is a general term for when a perpetrator positions themselves in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers.

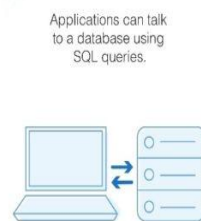


Denial-of-Service (DoS): DoS attacks are cyber-acts meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users of the service or resource they expected. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. A crashing service attack takes advantage of bugs in the target that subsequently crash or severely destabilize the system in order to render the site or network inaccessible.



SQL Injections: SQL is a standardized language used to access and manipulate databases to build customizable data views for each user. SQL queries are used to execute commands, such as data retrieval, updates, and record removal. SQL Injections, commonly referred to as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

What Is SQL Injection



SQL injection occurs when the application does not protect against malicious SQL queries..



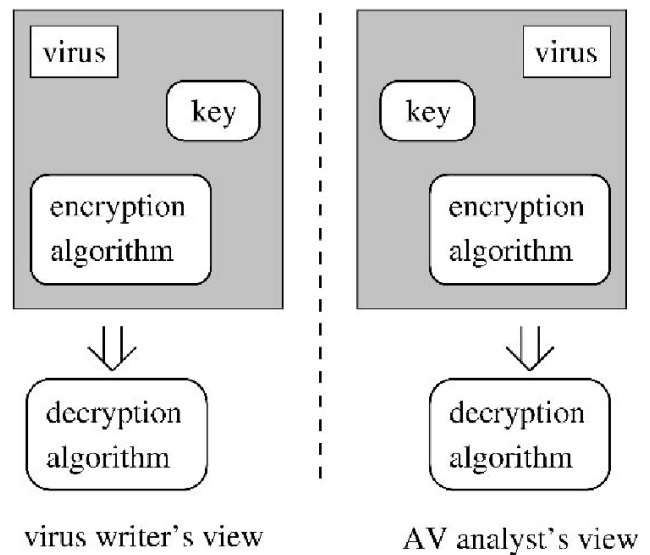
An attacker can use malicious SQL queries to trick the database into providing sensitive information.



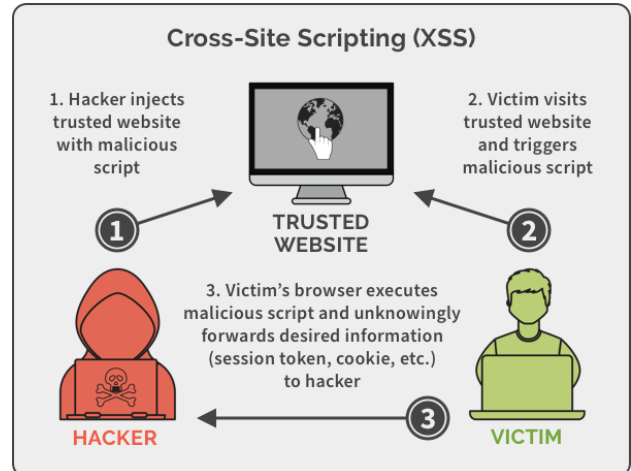
Zero-Day Exploits: A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. Vulnerabilities can be the result of improper computer or security configurations and programming errors. If left unaddressed, vulnerabilities create security holes that hackers can exploit. Hackers can potentially write malicious code to target a specific security weakness. The malicious software then takes advantage of a vulnerability to compromise a computer system or cause an unintended behavior.



Cryptovirology: Field of cybersecurity that studies how to use cryptography (the practice of writing code to send secured communications) to design malicious software. The field was born with the observation that public-key cryptography can be used to break the symmetry between what an antivirus analyst sees regarding malware and what the attacker sees. The antivirus analyst sees a public key contained in the malware whereas the attacker sees the public key contained in the malware as well as the corresponding private key (outside the malware) since the attacker created the key pair for the attack. The public key allows the malware to perform trapdoor one-way operations on the victim's computer that only the attacker can undo.



Cross-Site Scripting: Otherwise known as XSS, is a type of attack in which malicious scripts are injected into websites and web applications for the purpose of running on the end user's device. During this process, unvalidated inputs (user-entered data) are used to change outputs. XSS attacks can exploit vulnerabilities in a range of programming environments, including VBScript, Flash, ActiveX, and JavaScript. This ability to exploit commonly used platforms makes XSS attacks both dangerous and common.



Rootkits: A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit allows a perpetrator to maintain command and control over a computer without the computer user/owner knowing about it. Once a rootkit has been installed, the controller of the rootkit has the ability to remotely execute files and change system configurations on the host machine. A rootkit on an infected computer can also access log files and spy on the legitimate computer owner's usage.

Rootkits: What is a Rootkit?

- A rootkit is a set of tools used for (covertly) maintaining root access to a system
- Rootkits allow attackers the ability to circumvent protection mechanisms limiting root access
- Provide a much higher layer of stealth than normal "Trojan programs" by hiding processes and files

Case Studies

Orion Systems SolarWinds Hack

The SolarWinds hack [refers to the supply-chain cyber-attack against SolarWinds](#), a 3rd party software company. The attack has been deemed by US Intelligence agencies, in conjunction with private cyber detection companies, as orchestrated by a Russian hacking group called 'APT29' (Advanced Persistent Threat), otherwise known as 'Cozy Bear,' which has strong ties and suspected funding to the Russian Foreign Intelligence Service (SVR). The attack was first confirmed in March 2020, though the initial commencement of the hack might have begun weeks or even months before it was officially identified.

The SolarWinds Hack is known as a Trojan-Horse attack, in which malicious malware is injected into the victims' central system through a regular system update that remains dormant and hidden in the system before it activates, which then gives it remote control of any computer that had SolarWinds Orion installed. According to a [December 2020 analysis conducted by FireEye](#), the private cybersecurity company that first detected the hack, the Trojan virus would wait 12 to 14 days, then communicate with a command-and-control server, where it could install additional software and perform other tasks, including accessing an Active Directory service or monitoring network traffic.

At the time of the hack, SolarWinds had about 300,000 customers, consisting of more than 425 of the US Fortune 500, including Microsoft, Cisco, Intel, Deloitte, and other organizations such as the California Department of State Hospitals, Kent State University, the Pentagon; as well as US agencies such as the State Department, the National Security Agency, the Department of Energy, Department of the Treasury, the National Nuclear Security Administration, the Department of Justice, and the White House. The hack, however, [affected the approximately 33,000 customers who used the Orion system](#), subsequently perturbing nearly 18,000 different servers, leading to hundreds of thousands of computers becoming compromised and susceptible for mass data theft and destruction. What's more, since the hack was done so stealthily, and went undetected for months, security experts assert that some victims may never know if they were hacked or not.

The attack, which had gone a full 9 months undetected, had according to many cybersecurity experts, blindsided the preeminent USCYBERCOM. In fact, General Nakasone, Commander of USCYBERCOM, told Congress in March 2021 "what I'm identifying right now is that our adversaries understand that they can come into the US and rapidly utilize an ISP (internet service provider), come up and do their activities, and then come down before a warrant can be issued, before we can actually have surveillance by a civilian authority here within the US. That's the challenge that we have right now."

Former Director of CISA, Chris Krebs, [stated that the "indiscriminate nature"](#) of targeting the supply chain in a way that potentially compromised thousands of companies was "outside of the bounds of at least what we have seen recently of espionage activities." In addition, former NSA Deputy Director and current head of the White House's National Cyber Directorate, Chris Inglis, said the SolarWinds hack "focused sufficiently sharply that it

hovers in the mind's eye for quite some time," and called for espionage-specific rules of international law to counter these rapid and unyielding cyber-attacks, saying the hack violated principles of proportionality and necessity.

In response to the SolarWinds hack, the Biden administration levied sanctions against Russia and took executive action to bolster US cybersecurity capabilities such as implementing strict security standards that supply chain software companies like SolarWinds must meet in order to do business with the federal government. The new standards also require those companies to maintain a vulnerability disclosure program and make automated security checks public to ensure that another cyber-attack does not go undetected for months at a time.

Colonial Pipeline Ransomware

In May 2021, the US's largest domestic oil pipeline was targeted by a ransomware attack which led it to shut down its operations on the East Coast. The attack, which lasted a few days, [had the potential to greatly disrupt and threaten the US's supply of domestic gas and the disruption of global gas prices and distribution](#). The pipeline, owned by Georgia-based Colonial Pipeline, is a key passage for the eastern half of the U.S. It's the main source of gasoline, diesel and jet fuel for the East Coast with capacity of about 2.5 million barrels a day (105 million gallons) on its system from Houston as far as North Carolina, and another 900,000 barrels a day to New York; totaling to approximately 45% of the East Coast's oil supply and reaching more than 50 million Americans. US energy and cyber officials alike labeled this cyberattack as the "most significant and successful [known] attack on US infrastructure."

While there was no direct evidence linking the Russian Government to the cyber-attack on the Colonial Pipeline, the Federal Bureau of Investigation and the Department of Homeland Security [officially confirmed that DarkSide](#) was responsible for compromising the network. DarkSide is a nascent Russian-based cyberattack group that, since August 2020, has used ransomware cyberattacks to hack various companies throughout the world such as Japanese-based Toshiba Corp and German-based Brenntag. DarkSide follows a "ransomware-as-a-service" model, in which hackers develop and sell their ransomware attack tools to those wishing to carry out an attack. DarkSide also adheres to a "double extortion" trend, where the hackers not only encrypt and lock the user's data, but also threaten to make the data public if the ransom is not paid – as was the case with Colonial Pipeline.

The cyber-attack [targeted the billing system of Colonial](#) which led the company to completely halt all its operations out of concern that it would not be able to track how much gas is owed and allocated. DarkSide gained entry into the Colonial's networks in late April 2021 through a virtual private network (VPN) account, which allowed employees, and subsequently, DarkSide, to remotely access the company's computer network with the use of a leaked password spotted in a mass data leak. The main issue that permitted hackers to strike was on account of the Colonial billing system not having multifactor authentication (which requires multiple verification steps in order to login), allowing DarkSide to breach the Colonial Pipeline network with relative ease.

DarkSide ordered that Colonial pay a ransom of 75 bitcoin (\$4.4 million) in return for a software application to restore the network. With guidance from the FBI, Colonial paid the ransom and received the software, which allowed it to continue its crucial distribution operations; of which the Department of Justice successfully recovered \$2.3 million of the payment.

The Colonial Pipeline ransomware attack [reinforced the federal government's sense of urgency](#) in bolstering the nation's cybersecurity capabilities. Prior to the ransomware attack, prominent bipartisan Congressmembers including Senator Ed Markey (D-MA) and Senator Ben Sasse (R-Neb) had voiced that the federal Government has long failed to devote the needed attention to pipeline security and that the attack was the latest indication that the Government isn't ready for potentially debilitating cyber strikes.


WannaCry Ransomware

WannaCry was a [ransomware cyber-attack that took place in May 2017 that targeted more than 230,000 computers around the world](#) that were running on the Microsoft Windows operating system. The attack essentially locked the victims' respective computer and held their digital files hostage while demanding the user pay \$300-\$600 in Bitcoin to have access returned to them. The attack lasted about four days and is estimated to have cost anywhere between hundreds of millions to billions of dollars in damages.

The WannaCry ransomware virus was [designed to infiltrate and disseminate through a flaw in a hacking system](#) developed by the US National Security Agency (NSA) called EternalBlue that targeted computers running on the Windows operating system. EternalBlue was stolen and leaked by a hacking group called Shadow Brokers in April 2017 which subsequently caused Microsoft to patch up the weaknesses that the NSA initially detected. However, not all computers that were operating on Windows were properly updated with the data that patched up the vulnerability which is the reason how the WannaCry virus was able to affect a plethora of computers from nearly 150 countries.

The Shadow Brokers is a hacker group that first emerged in 2016. They are known to publish leaks containing hacking tools, such as zero-day exploits, from a suspected cybersecurity branch of the NSA called the Equation Group. These leaked exploits and vulnerabilities are used to target enterprise firewalls, antivirus software, and, in the case of WannaCry, Microsoft products. In December 2017, cyber experts from both US and the UK have formally deemed that the Shadow Brokers group is based in North Korea, since the code that was used had already been identified as being a recurring code once perpetrated by the Kim Jong Un regime.

[The WannaCry ransomware consists of several components.](#) One such component is the primary delivery program that contains other programs, including encryption and decryption software. Once WannaCry is on a computer system, it searches for dozens of specific file types, including Microsoft Office files and picture, video and sound files, which it then executes a routine to encrypt the files, which can only be decrypted using an externally delivered digital key.



This led to hundreds of thousands of victims paying the requested sum in Bitcoin to retrieve their locked data. The WannaCry virus targeted computers to critical governmental agencies including: the UK National Health Service (NHS), the Russian railway systems & the Russian Ministry of Internal Affairs, the Chinese Public Security Bureau, the Saudi Arabian Telecom Company, and the regional Indian governments of West Bengal, Kerala, Gujarat, and Maharashtra; as well as influential private/public companies including: the Taiwan Semiconductor Manufacturing Company (TSMC), Nissan, FedEx, Renault, Petrobras, PetroChina, Deutsche Bahn, and an array of hospitals and universities in Indonesia, Brazil, India, Canada, Spain, China, and many others.

Largest US Cybersecurity Firms

Cisco Systems, Inc.

Description: Cisco Systems, Inc. designs, manufactures, and sells Internet Protocol (IP) based networking and other products related to the communications and information technology throughout the world, with a footprint on every continent. The company provides infrastructure platforms, including networking technologies of switching, routing, wireless, and data center products that are designed to work together to deliver networking capabilities, and transport and/or store data. The company also offers collaboration products comprising unified communications, as well as the Internet of Things and analytics software. In addition, it provides security products, such as network security, cloud and email security, identity and access management, advanced threat protection, and unified threat management products. It serves businesses of various sizes, public institutions, governments, and service providers. The company sells its products and services directly, as well as through systems integrators, service providers, other distributors.



Main Products:

- SASE (Secure Access Service Edge): Secure access service edge combines networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users work. Core functions include software-defined wide area network, secure web gateway, firewall as a service, cloud access security broker, and zero-trust network access.
- Cisco XDR: A system designed to extend the capabilities of Cisco's detection and response solutions where users can use it to collect and correlate data across email applications, endpoints, cloud resources, servers, and networks.

2021 Total Revenue of Cisco Cyber: \$714M

Market Cap: \$233B

Founded: 1984

Total Employee Count: 79,000

Contact Information:

170 West Tasman Drive
San Jose, California 95134-1706
Phone: (408) 526-4000

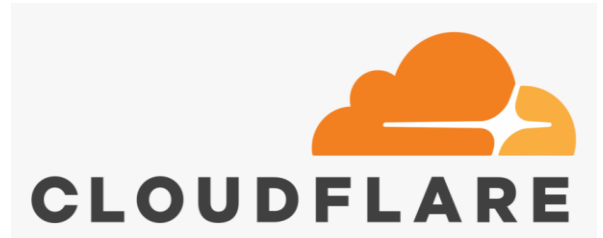
www.cisco.com

Recent Year Company Market Growth:



CloudFlare, Inc.

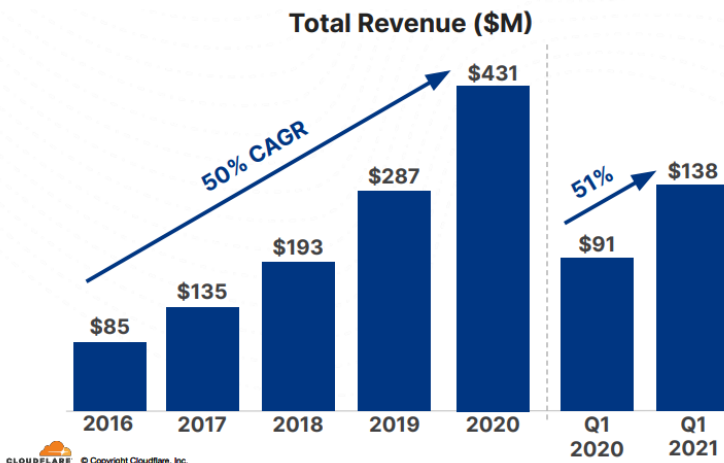
Description: CloudFlare, Inc. operates a cloud platform that delivers a range of network services to businesses worldwide. The company provides an integrated cloud-based security solution to secure a range of combination of platforms, including public cloud, private cloud, on-premise, software-as-a-service applications, and IoT devices. Its security products comprise cloud firewall, bot management, distributed denial of service, IoT, SSL/TLS, secure origin connection, and rate limiting products. The company also offers performance solutions, which include content delivery, intelligent routing, and mobile software development kit, as well as content, mobile, and image optimization solutions. In addition, it provides reliability solutions comprising load balancing, anycast network, virtual backbone, DNS, DNS resolver, and always online solutions that enhances Internet experience and allows customers to run their digital operations efficiently. Further, the company provides Cloudflare internal infrastructure solutions, including on-ramps, which connect users, devices, or locations to Cloudflare's network; and filters, which are the products that protect, inspect, and privilege data.



Main Products:

- Cloudflare One: A Zero Trust network-as-a-service platform that simultaneously connects users to enterprise resources, with identity-based security controls delivered close to users.
- WAF: (Web Application Firewall) protects the user's Internet property from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests with no changes to the user's existing infrastructure.

Recent Year Company Market Growth:



2021 Total Revenue: \$633M

Market Cap: \$55.83B

Founded: 2009

Total Employee Count: 2,050

Contact Information:

101 Townsend Street
San Francisco, California 94107
Phone: (650) 319-8930
www.cloudflare.com

CrowdStrike Holdings, Inc.

Description: CrowdStrike Holdings, Inc. is a cybersecurity company which engages in the provision of cloud-delivered solution for next-generation endpoint protection that offers cloud modules on its Falcon platform through SaaS subscription-based model. It operates through domestic and international geographical segments. The firm's services include incident response services; proactive services, tabletop exercises, adversary emulation, cloud security assessment, and blue team exercises. CrowdStrike's cybersecurity technology specializes in next-generation endpoint protection, delivering as a single integrated cloud-based solution. CrowdStrike's Falcon platform stops breaches by detecting all attack types, even malware-free intrusions, providing five-second visibility across all current and past endpoint activity while reducing cost and complexity.



Main Products:

- Falcon Endpoint Protection: System that unifies the technologies required to successfully stop breaches: next-generation antivirus, endpoint detection and response, IT hygiene, 24/7 threat hunting and threat intelligence. Falcon combines these to provide continuous breach prevention in a single agent.
- Falcon Prevent: A defensive system that combines an array of powerful methods to provide prevention against the rapidly changing tactics, techniques and procedures (TTPs) used by adversaries to breach organizations – including commodity malware, zero-day malware and even advanced malware-free attacks.

2021 Total Revenue: \$874.4M

Market Cap: \$55.83B

Founded: 2011

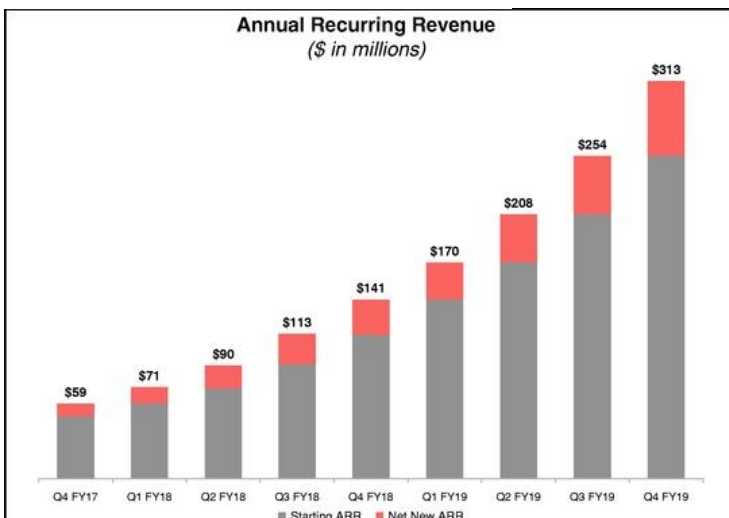
Total Employee Count: 4,200

Contact Information:

150 Mathilda Place
Suite 300
Sunnyvale, California 94086
Phone: (888) 512-8906

www.crowdstrike.com

Recent Year Company Market Growth:



Fortinet, Inc.

Description: Fortinet, Inc. provides broad, integrated, and automated cybersecurity throughout the world. It offers FortiGate hardware and software licenses that provide various security and networking functions, including firewall, intrusion prevention, anti-malware, virtual private network, application control, web filtering, anti-spam, and wide area network acceleration. The company also provides FortiSwitch product family that offers secure switching solutions for connecting customers their end devices; FortiAP product family, which provides secure wireless networking solutions; FortiExtender, a hardware appliance; FortiAnalyzer product family, which offers centralized network logging, analyzing, and reporting solutions; and FortiManager product family that provides central and scalable management solution for its FortiGate products. The company provides security subscription, technical support, professional, and training services. It sells its security solutions to channel partners and directly to various customers in telecommunications, technology, government, financial services, manufacturing, and healthcare industries.



Main Product:

- FortiGate NGFW: Delivers enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into the hybrid IT architecture and build security-driven networks to achieve ultra-fast security, end to end, consistent real-time defense with FortiGuard Services, security processing units, and operational efficiency and automated workflows.

2021 Total Revenue: \$3.210B

Market Cap: \$54.46B

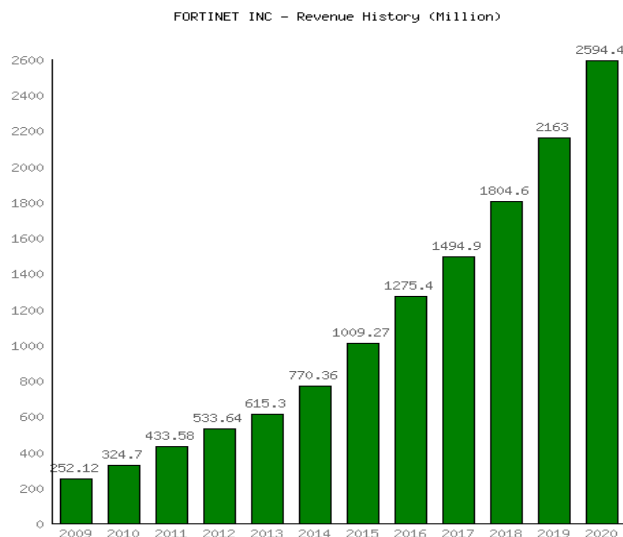
Founded: 2000

Total Employee Count: 9,000

Contact Information:

899 Kifer Road
Sunnyvale, California 94086
Phone: (408) 235-7700
www.fortinet.com

Recent Year Company Market Growth:



IBM Corporation

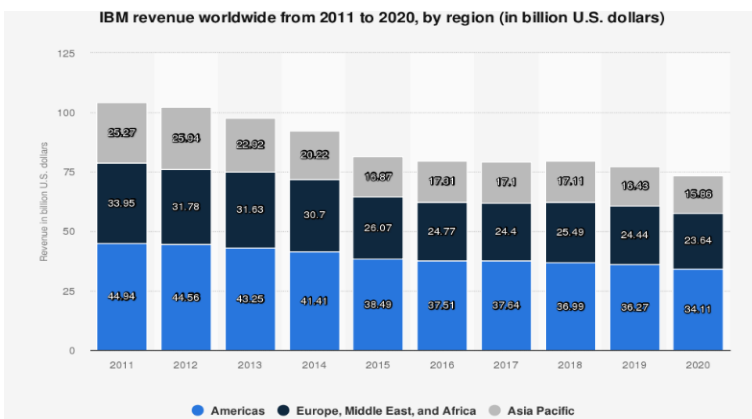
Description: IBM (International Business Machines) Corporation is an information technology company, which provides integrated solutions that leverage information technology and knowledge of business processes. It operates through the following segments: Cloud and Cognitive Software, Global Business Services, Global Technology Services, Systems, and Global Financing. The Cloud and Cognitive Software segment provides integrated and secure cloud, data, and solutions to the clients. The Global Business Services segment provides clients with consulting, application management, and business process outsourcing services. The Global Technology Services segment provides comprehensive IT infrastructure and platform services that create business value for clients. The Systems segment provides clients with innovative infrastructure platforms to help meet the requirements of hybrid cloud and enterprise AI workload. While the Global Financing segment provides client financing, commercial financing, and participates in the remanufacturing and remarketing of used equipment.



Main Products:

- **Cloud Pak for Security:** AI-powered software, designed to accelerate application modernization with pre-integrated data, automation and security capabilities. IBM Cloud Paks deliver the industry's only hybrid cloud platform experience, enabling business and IT teams to build and modernize applications faster across any cloud or IT infrastructure.
- **Security Guardium Insights:** provides centralized data security across the hybrid multicloud. Adapt and scale with modern architecture, streamline compliance and audit processes and share contextual risk insights across security teams to support zero trust.

Recent Year Company Market Growth:



2021 Total Revenue: \$36.5B

Market Cap: \$127.19B

Founded: 1911

Total Employee Count: 346,000

Contact Information:

One New Orchard Road
Armonk, New York 10504
Phone: (914) 499-1900

www.ibm.com

Mandiant, Inc.

Description: Mandiant, Inc., formerly known as FireEye Inc., operates as an intelligence-led security company. The firm engages in intelligence-based cybersecurity solutions that allow organizations to prepare for, prevent, respond to and remediate cyber-attacks. It operates through the following geographical segments: United States; Europe, the Middle East, Africa, and the Asia Pacific. Its most popular solutions include: Enterprise Security; Managed Security; Threat Intelligence; and Industry Solutions.



Main Products:

- Mandiant Advantage: A multivendor XDR (extended detection and response) platform that utilizes several comprehensive modules including: automated defense, threat detection, security validation, and attack surface management through the Mandiant Intel Grid.
- Mandiant Intel Grid: The core enabling technology that fuels our products with Mandiant's relevant, instantaneous moment breach intelligence and expertise to allow the prioritization of efforts by responding to the threats that matter to an organization.

2021 Total Revenue: \$480M

Market Cap: \$4.4B

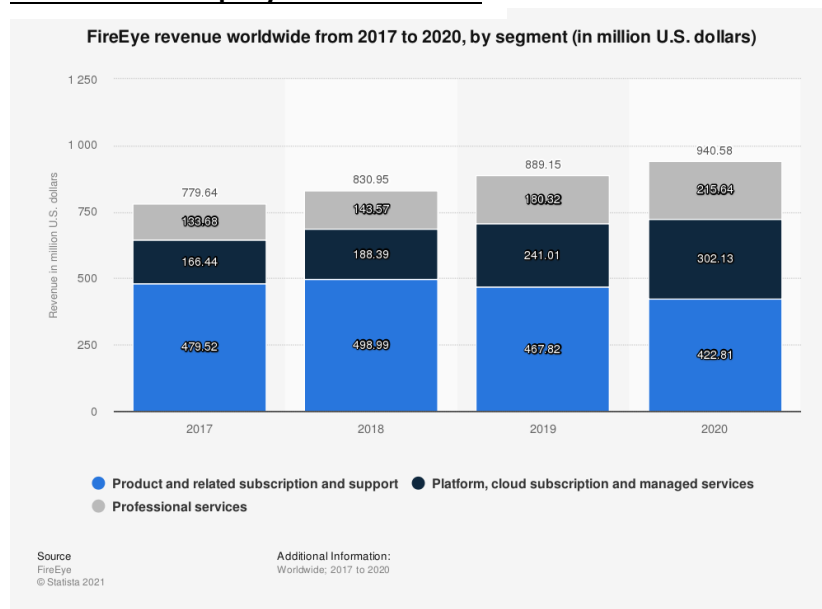
Founded: 2004

Total Employee Count: 3,400

Contact Information:

601 McCarthy Boulevard
Milpitas, California 95035
Phone: (408) 321-6300
www.mandiant.com

Recent Year Company Market Growth:



Microsoft Corp.

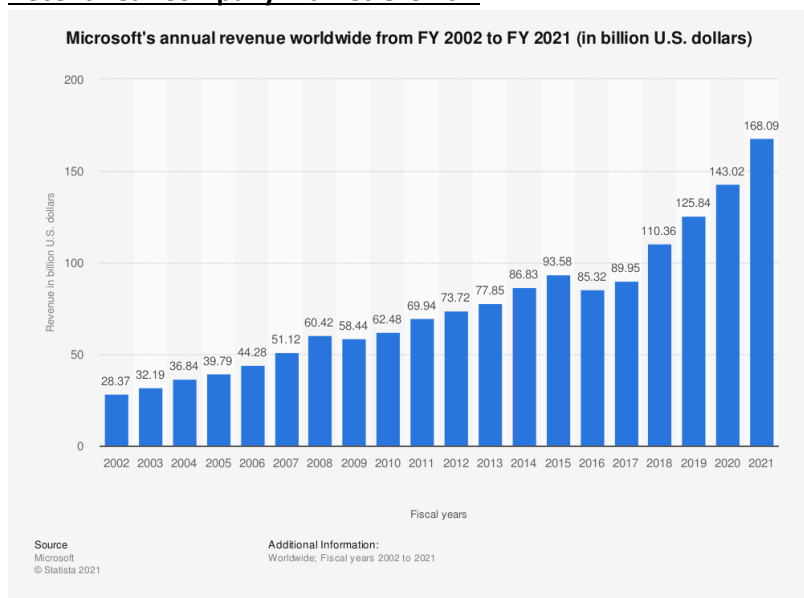
Description: Microsoft's cybersecurity department, the Cyber Defense Operations Center brings together security response experts from across the company to help protect, detect, and respond to threats in real-time. The Center has direct access to thousands of security professionals, data scientists, and product engineers throughout Microsoft to ensure rapid response and resolution to security threats. Informed by trillions of data points across an extensive network of sensors, devices, authentications, and communications, the Center employs automated software, machine learning, behavioral analysis, and forensics to create an intelligent security graph. Microsoft invests nearly \$1B per year in its cybersecurity infrastructure.



Main Product:

- Azur Active Directory (AAD): Microsoft's cloud-based identity and access management service, which helps employees sign in and access resources in external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Internal resources, such as apps on a corporate network and intranet, along with any cloud apps developed by an organization.

Recent Year Company Market Growth:



2021 Total Revenue: \$168.1B

Market Cap: \$2.3B

Founded: 1975

Total Employee Count: 181,000

Contact Information:

One Microsoft Way
Redmond, Washington 98052-6399
Phone: (435) 882-8080
www.microsoft.com

Palo Alto Networks

Description: Palo Alto Networks, Inc. provides cybersecurity solutions worldwide. The company offers firewall appliances and software; Panorama, a security management solution for the control of firewall appliances and software deployed on an end-customer's network and instances in public or private cloud environments, as a virtual or a physical appliance; and virtual system upgrades, which are available as extensions to the virtual system capacity that ships with physical appliances. It also provides subscription services covering the areas of threat prevention, malware and persistent threat, uniform resource locator filtering, laptop and mobile device protection, and firewall; and DNS security, Internet of Things security, SaaS security API, and SaaS security inline, as well as threat intelligence, and data loss prevention.

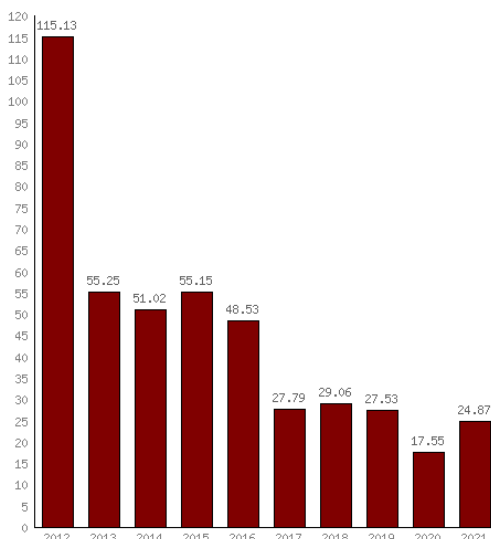


Main Products:

- **Cortex XDR:** Delivers enterprise-wide protection by analyzing data from any source to stop sophisticated attacks, eliminate blind spots with complete visibility, simplify security operations to cut mean time to respond (MTTR), and harness the scale of the cloud for AI and analytics.
- **Panorama:** A network security platform that empowers consolidated policy creation and centralized management features, sets up and controls firewalls centrally with functionality and an efficient rule base, and gain insight into network-wide traffic and threats.

Recent Year Company Market Growth:

PALO ALTO NETWORKS INC - Revenue Growth By Year (%)



2021 Total Revenue: \$4.3B

Market Cap: \$49.4B

Founded: 2005

Total Employee Count: 10,400

Contact Information:

3000 Tannery Way
Santa Clara, California 95054
Phone: (408) 753-4000
www.paloaltonetworks.com

Rapid7, Inc.

Description: Rapid7, Inc. offers a cloud-native insight platform that enables customers to create and manage analytics-driven cyber security risk management programs. Its platform includes InsightVM, a vulnerability risk management solution that is designed to provide a way to collect vulnerability data, prioritize risk, and automate remediation; InsightIDR, an incident detection and response solution; InsightAppSec, which provides application security testing that analyzes web applications for security vulnerabilities; and InsightConnect, a security orchestration and automation response solution that is used by security professionals. The company's other products include DivvyCloud, a cloud security posture management solution; Nexpose, an on-premise version of company's vulnerability risk management solution; AppSpider, an on-premise version of company's application security testing solution; Metasploit, a penetration testing software solution; and InsightOps that enables organizations to store and search data in real time.



Main Products:

- **InsightVM:** Provides not only visibility into the vulnerabilities in your modern IT environment—including local, remote, cloud, containerized, and virtual infrastructure—but also clarity into how those vulnerabilities translate into business risk and which are most likely to be targeted by attackers.
- **InsightConnect:** Rapid7's security orchestration, automation and response (SOAR) solution that streamlines and accelerates highly manual, time-intensive, processes 24 hours a day. With more than 300 plugins to connect an IT and security systems — and a library of customizable workflows.

2021 Total Revenue: \$455.8M

Market Cap: \$6.7B

Founded: 2000

Total Employee Count: 1,500

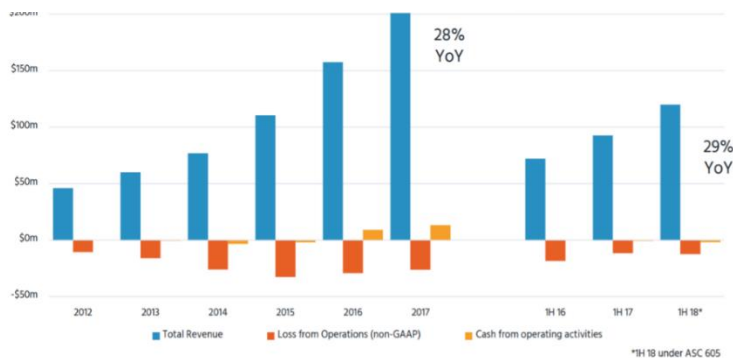
Contact Information:

120 Causeway Street
Boston, Massachusetts 02114

Phone: (617) 247-1717

www.rapid7.com

Recent Year Company Market Growth:



Rapid7 Proprietary

RAPID7

Zscaler, Inc.

Description: The company provides Zscaler Internet Access solution that provides users, servers, operational technology, Internet of Things device secure access to externally managed applications, including software-as-a-service (SaaS) applications and Internet destinations; and Zscaler Private Access solution, which is designed to provide access to managed applications hosted internally in data centers, and private or public clouds. It also offers Zscaler Digital Experience that measures end-to-end user experience across business applications, as well as provides an easy-to-understand digital experience score for each user, application, and location within an enterprise. In addition, the company provides workload segmentation solutions comprising Zscaler Cloud Security Posture Management that identifies and remediates application misconfigurations in SaaS, infrastructure as a service, and platform as a service to reduce risk and ensure compliance with industry and organizational benchmarks; and Zscaler Cloud Workload Segmentation, which is designed to secure application-to-application communications inside public clouds and data centers to stop lateral threat movement, as well as prevents application compromise and reduces the risk of data breaches.

Main Products:

- Zscaler Internet Access: A secure internet and web gateway delivered from the cloud. Offered as a service from the world's largest security cloud, Zscaler Internet Access provides a full security stack with comprehensive in-depth protection for an organization.
- Zscaler Private Access: a cloud service that provides seamless, zero trust access to private applications running on public cloud or within the data center. With ZPA, applications are never exposed to the internet, making them completely invisible to unauthorized users.

2021 Total Revenue: \$197.1M

Market Cap: \$16B

Founded: 2007

Total Employee Count: 3,000

Contact Information:

120 Holger Way

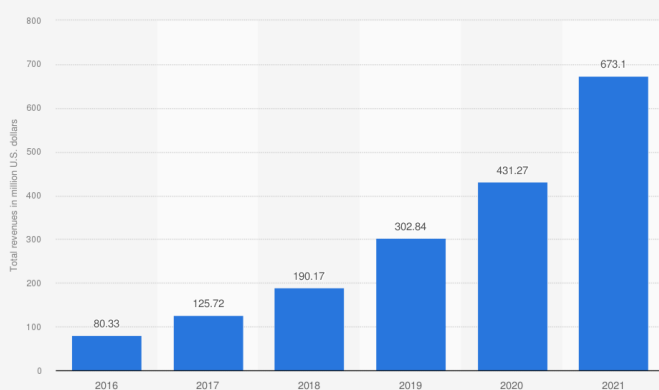
San Jose, California 95134

Phone: (408) 533-0288

www.zscaler.com

Recent Year Company Market Growth:

Zscaler total revenue worldwide from 2016 to 2021 (in million U.S. dollars)



Source:
Zscaler
© Statista 2021

Additional Information:
Worldwide; 2016 to 2021