future tech

Next Digital Cybersecurity

Cybersecurity encompasses the set of procedures and tools that are implemented to protect information assets that are generated and processed through computers, servers, mobile devices, networks and electronic systems. Information assets can include data, software and hardware, and threats to these assets are varied and can originate from both outside and inside an organization.

Both cybersecurity and cyberattacks have evolved as communication technology has evolved. It has come a long way from simple encryption to highly sophisticated algorithms to protect data and communication. **Embedded multi-factor authentication procedures, better encryption techniques and the use of virtual private networks** have become more common every day. **Artificial intelligence (AI) and machine learning** have enabled real-time threat detection and automated incident responses, as well as continuous learning and procedural improvement.

COVID-19 caused a massive adoption of remote work in record time at the expense of the protocols and computer security perimeters of companies. The increase in technological dependence, not only at the work level, but also in education, health, commerce, banking or social life itself, resulted in an increase in the use of remote work in record time at the expense of corporate IT security protocols and perimeters.

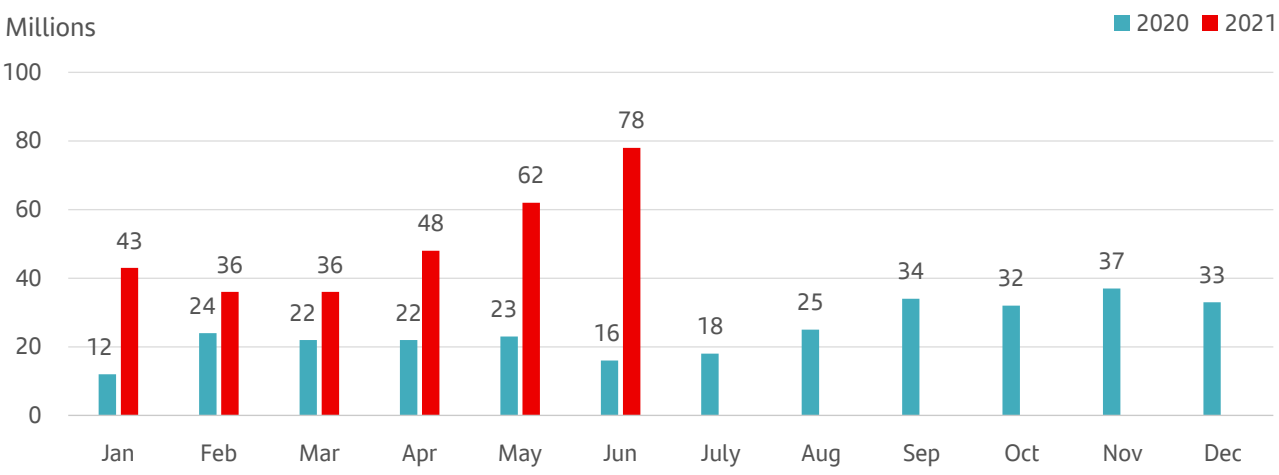
vulnerabilities, data loss and targeted ransomware attacks. ransomware (data hijacking) attacks. According to SonicWall's "Mid-Year Update: 2021 SonicWall Cyber Threat Report" **in the first six months of 2021 attack attempts already exceed the 2020 total.** (see graph)

According to data from the "Cost of a Data Breach Report 2021" study produced by the Ponemon Institute and sponsored by IBM, **in 2020, the average cost of a data breach was $3.86 million worldwide, and $8.64 million in the United States.** These costs include breach discovery and response (breach) expenses, the cost of downtime and lost revenue, and long-term reputational damage to a company and its brand. According to the same study, in the last year (2020-2021) the average cost per breach has increased by 10% and 20% of those breaches are initially due to compromised credentials.

As the cyber-space is international and relatively new, rules or norms are yet to be established and boundaries are barely existent. In that sense, **investing in cybersecurity has become more critical than ever** to protect governments, organizations and individuals, as well as their physical, digital and financial assets and even their own brands. According to Canalys, a company specializing in the analysis of the technology sector, in the United States in **2020 investments in cybersecurity recorded a growth of 10%, reaching 53 billion USD.** The CAGR for the next of this sector remains at around 10%.

Global ransomware volume (number of attempted attacks)

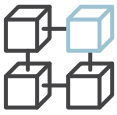
Source: Mid-Year Update: 2021 SonicWall Cyber Threat Report



Main innovations in Cybersecurity

Digital Signatures and Certificates

Due to the rapid advances in e-commerce, there is a growing need for online security and authentication. Many advanced technologies are being developed to secure authentication on the Internet. A **digital signature is a cryptographic mechanism that, when applied to a document, allows the recipient to identify the signer unambiguously and to guarantee the integrity of the signed document.** It enables organizations to authenticate and secure the identity and records of the customer and offers valuable possibilities for organizations to formalize contracts. There are electronic signature platforms that allow contracts to be sent and signed electronically in a secure way. The **digital certificate, on the other hand, is a certification or electronic document issued by a certification authority that links a person with a public key and confirms their identity.** This allows you to carry out online procedures, including signing documents digitally. According to data from Statista, an online statistics portal, in 2019 the digital signature market was valued at $957.24 million and is expected to grow to $4.8 billion by 2026.



Digital network infrastructure

Web security consists of **every action or tool used to prevent information from being exposed or prone to attacks by cybercriminals.** It protects not only companies but also users. **Among the main tools are the firewall, proxy server, antivirus software, endpoint encryption and vulnerability scanner.** The **firewall** monitors incoming and outgoing traffic and decides whether to allow or block traffic based on a set of pre-defined security restrictions. The **proxy server** is an intermediary between the connections of a client and the server filtering all the packets between both that prevents the server from knowing the identity of the client allowing a private and anonymous navigation. **Antivirus software** aims to detect, remove and block computer viruses. **Endpoint encryption** ensures that a message is turned into a secret message on its original delivery and decrypted only by the final recipient. Finally, the web **vulnerability scanner** is a software that constantly performs automatic scans of any application, system or network for any possible vulnerabilities. Estimates from Statista indicate that the network security market, which includes applications, software and cloud-based services, was valued at USD 29.5 billion in 2020 and is expected to exceed USD 4.6 billion in revenue by 2021.

Automatic learning

The growing adoption of machine learning in businesses across industries reflects the effectiveness of its algorithms, frameworks, and techniques to quickly solve complex problems. **Machine learning (ML) is a type of artificial intelligence (AI) that gives computers the ability to learn without being explicitly programmed. It consists of developing patterns and, through algorithms, modifying those patterns as new data becomes available.** To develop these patterns, large volumes of data are needed because the data must represent all potential outcomes of all possible scenarios.

With machine learning, **cybersecurity systems can analyze patterns and learn from them to help prevent similar attacks and respond to changes. It** can help cybersecurity teams be more proactive in preventing threats and **responding to active attacks in real time.** It can reduce the amount of time spent on routine tasks and enable organizations to use their resources more strategically. In short, machine learning can make cybersecurity simpler, more proactive, less costly, and more effective.

Innovators in Cybersecurity

VMware, Inc. is a Palo Alto, California-based company that develops **software used to create and manage virtual machines - computing functions spread across multiple systems. Companies use their cloud-based and on-premises applications to more efficiently integrate and manage server, storage, and network functions, reducing their IT costs**. VMware also offers software maintenance and support, training, consulting and hosted services. The company's overall cloud strategy contains three key components: continuing to expand beyond compute virtualization into the private cloud; extending the private cloud into the public cloud; and connecting and securing endpoints across a range of public clouds.

Palo Alto Networks, Inc. is a global cybersecurity provider that enables enterprises, service providers, and government entities to protect all users, applications, data, networks, and devices with complete visibility and context on a continuous basis across all locations**. It offers cybersecurity products that cover a broad range, enabling end customers to secure their end customers to secure their networks, remote workforce, branch offices, public and private clouds, and advance their Security Operations Centers ("SOCs").** Its products include appliances and firewall software and virtual system upgrades, which are extensions of the appliances. It has more than 80,000 customers in 150 countries around the world. It derives 65% of its revenues from the United States.

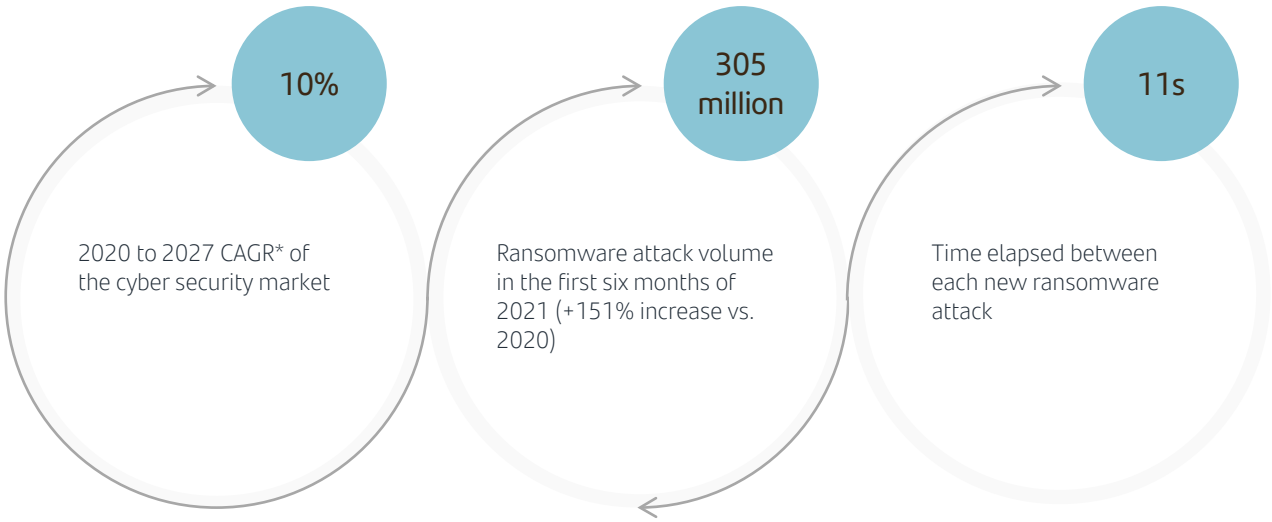
CrowdStrike Holdings, Inc**.** is a leading cybersecurity company that provides *endpoint* **and cloud workload security, threat intelligence, and cyberattack response services**. Since 2011, when the company was founded, they have specialized in cloud security. They designed the **Falcon** platform on a cloud-based architecture to detect threats and stop breaches without compromising the speed or performance of computers. **The platform features Threat Graph, which is a machine learning system that is continuously processing and contextualizing data, correlating it with different events to enrich its knowledge and be able to predict threats better and faster.**

Splunk Inc. developed software that collects and indexes machine-generated data produced by nearly all hardware and software that contains a time-stamped record of transactions, user actions, security threats and other activities. **With Splunk's software, users can drill down into the data, analyzing, monitoring and reporting for operational intelligence, application management, and security and compliance and analytics.** The company partners with companies such as Microsoft Visual Studio and Eclipse to include its software in their products. Splunk has more than 19,000 corporate and government customers in more than 130 countries. The company relies on U.S. customers for about 70% of its revenue.

DocuSign, Inc. **has been a pioneer in the development of electronic signatures. Today it offers the world's #1 eSignature solution as a core part of its broader platform for automating the agreement process.** They eliminate paper and automate the process, allowing companies to measure turnaround time in minutes instead of days, substantially reduce costs and greatly eliminate errors. Its cloud-based platform enables businesses of all sizes and industries to quickly and easily convert almost any agreement, approval process or transaction to digital, from almost anywhere in the world and on virtually any device. It has more than one million customers and one billion users worldwide.

Fortinet, Inc. is a global leader in cybersecurity solutions for a wide variety of organizations, including enterprises, communications service providers, government organizations and small businesses. **The company manufactures network security appliances (sold under its FortiGate line) and software that integrate anti-virus, firewall, content filtering, intrusion prevention systems (IPS) and anti-spam capabilities to protect against computer viruses, worms and inappropriate Web content**. It also offers complementary products including its FortiManager security management and FortiAnalyzer event analysis systems. To support its widely dispersed global channel and end customer base, it has sales professionals in more than 80 countries around the world. More than 40% of revenue comes from the Americas.

Did you know that?



(1) Source: eMarketer

(2) Source: SonicWall

Source: Cybersecurity Ventures

CAGR*: Compounded annual growth rate