Forcepoint

The Evolution of Network Security

A Brief 35-Year History of Cyber Exploits

Though our perimeters may look different today, compounding threats, increasing attacks, and the complex nature of the interconnected world are all accelerants that demand a more flexible—and trusted—approach to securing assets, people, and data.

1986
First computer virus, **Brain,** emerges on MS-DOS

1987
Vienna Virus neutralized 'in the wild' (ITW)

1987
First self-encrypting file virus, **Cascade,** appears

1988
First computer worm distributed via the internet, the **Morris Worm**

1991
First firewall includes application gateways

1994
Application-layer firewall introduced

1995
WM.Concept first virus to spread throughout Microsoft Word

1997
First web traffic control software developed & released

1998
Snort and open source Intrusion Detection System (IDS) released

2000
First denial-of-service **(DoS)** attack discovered

2006
Evasion concept introduced at **Black Hat**

2008
Conficker infects 9 to 15 million Microsoft systems

2009
Native clustering for high availability and performance introduced

2012
Software enabled security introduced; blade technology becomes obsolete

2012
Evader tool is launched

2013
Yahoo network breach resulted in 3 billion users being compromised

2013
Target servers accessed by hackers and compromised the data of ~70 – 110 million customers

2015
An incorrectly configured database exposes the information of 191 million voters across the US

2016
TrickBot, a computer malware trojan targeting Microsoft Windows, is first reported

2016
First cloud native product integrations released

2016
Forcepoint is born from Websense, Stonesoft, Sidewinder and other Raytheon security solutions

2017
WannaCry worldwide ransomware attack targets Microsoft Windows, affecting 230,000 computers in 1 day

2017
Forcepoint X-Labs encounters an ongoing TrickBot campaign targeting cryptocurrencies

2019
Multiple DDoS attacks forced New Zealand's stock market to shut down temporarily

2018
Forcepoint X-Labs records the evolution of Emotet, a banking trojan turned malware delivery platform

2018
Under Armour discloses cyberattackers successfully penetrated backend database for MyFitnessPal app

2019
LockerGoga ransomware compromises Norwegian aluminum manufacturing company

2020
Forcepoint introduces integrations to meet the demands of modern hybrid infrastructures

2020
Solarwinds software supply chain breach initially discovered

2021
Colonial Pipeline, is breached through one compromised VPN password creating gas shortages on the East Coast

2021
JBS Foods, attacked with ransomware, causing 13 beef plants to close in the US

2020
Robinhood discloses nearly 2,000 accounts were breached

2021
Kaseya supply chain ransomware attack paralyzes as many as 1,500 organizations

2021
Microsoft Exchange Server on-prem data breach compromised thousands of unsuspecting victims

2021
Forcepoint acquires CyberInc, Deep Secure and Bitglass

Secure your assets. Protect your edge.

Read more about Forcepoint Next-Gen Firewall

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

Forcepoint

forcepoint.com