**Companies**

1. Avigilon
2. Hikvision
3. Agent Vi
4. Verkada
5. BriefCam
6. Cylance
7. DarkTrace
8. Vectra
9. Fortinet
10. Palo Alto Networks
11. Check Point Software Technologies
12. Symantec
13. Cisco Systems
14. Trend Micro
15. Axis Communications
16. Avigilon - Founded in 2004, Avigilon is headquartered in Canada and provides security solutions that incorporate CV technology, video analytics, and artificial intelligence (AI). Avigilon provides end-to-end security solutions that include video analytics, facial recognition, and license plate recognition .

Revenue: $354 million

1. Hikvision - Established in 2001, Hikvision is based in China and is one of the largest providers of video surveillance products and solutions in the world. Its product line includes cameras, video management software, and access control systems, which all rely on CV technology.

Revenue: approximately $9.7 billion

1. Agent Vi - Founded in 2003, Agent Vi is an Israeli company that specializes in video analytics and CV-based security solutions. Agent Vi is a provider of video analytics software that uses computer vision to detect and classify objects, people, and events in real-time, enhancing security and situational awareness.

Revenue: $17 million

1. Verkada - Founded in 2016, Verkada is a California-based company that develops cloud-based video surveillance systems that use CV technology. Its products are used by organizations in various industries, including healthcare, education, and manufacturing.

Revenue: $190 million

1. BriefCam -Founded in 2007, BriefCam is based in Israel and offers video analytics solutions for security and business intelligence. BriefCam's customers include law enforcement agencies, government organizations, and private enterprise.

Revenue: $1.8 billion

1. Cylance - Cylance is a cybersecurity company that uses machine learning to provide endpoint protection against advanced threats and malware.

Revenue: $1.4 billion

1. Darktrace - Darktrace offers AI-based cybersecurity solutions that use machine learning to detect and respond to threats in real-time, without relying on rules or signatures.

Revenue: $199.1 million

1. Vectra - Vectra uses machine learning to detect and respond to cyberattacks in real-time, with a focus on detecting threats that bypass traditional security measures.

Revenue: $28.4 million

1. Fortinet - Fortinet provides a range of security solutions that use machine learning to protect against advanced threats and malware, including their FortiAI system.

Revenue: $4.4 billion

1. Palo Alto Networks - Palo Alto Networks offers a range of security solutions that use machine learning to identify and prevent cyber threats, including their Cortex XDR system.

Revenue: $4.2 billion

1. Check Point Software Technologies - Check Point offers a range of security solutions that use machine learning to detect and prevent cyber attacks, including their SandBlast Mobile system which uses ML to identify and block mobile threats.

Revenue: $2.04 billion

1. Symantec - Symantec provides a range of security solutions that use machine learning, including their Endpoint Protection system which uses ML to protect against advanced threats and malware.

Revenue: $4.73 billion

1. Cisco Systems - Cisco offers several security solutions that use machine learning, including their Cisco Stealthwatch system which uses ML to detect and respond to threats across an organization's entire IT environment.

Revenue: of $49.3 billion

1. Trend Micro - Trend Micro provides a range of security solutions that use machine learning, including their Deep Discovery Inspector system which uses ML to detect and respond to advanced threats.

Revenue: approximately $436 million

1. Axis Communications: Founded in 1984, Axis Communications is based in Sweden and specializes in network cameras, video encoders, and video management software that incorporate CV technology. The company's products are used in a variety of applications, including surveillance, remote monitoring, and access control.

Revenue: approximately $1.1 billion

**Advantages**

1. Accuracy:
2. Real-time monitoring
3. Cost-effective
4. Scalability
5. Versatility

**Disadvantages**

1. Limited view
2. Dependence on lighting.
3. Vulnerability to hacking.
4. Complexity
5. Privacy concerns

**Avigilon Models**

1. Avigilon Control Center (ACC): a comprehensive video management software that includes advanced video analytics powered by computer vision.
2. Avigilon Appearance Search: a video analytics technology that uses deep learning algorithms to help locate a specific person or vehicle across multiple cameras and video footage.
3. Avigilon Unusual Motion Detection (UMD): an advanced artificial intelligence technology that uses deep learning algorithms to continuously learn what typical activity looks like within a scene and detects any unusual motion.

**Hickvision Models**

1.DeepinMind: A deep learning-based AI technology used for video analytics, face recognition, vehicle recognition, and behavior analysis.

2.DarkFighterX: A low-light surveillance camera technology that uses sensors and image processing algorithms to capture clear video in low-light conditions.

3.ColorVu: A camera technology that captures full-color video in low-light conditions using high-performance lenses and advanced sensors.

**Briefcam Models**

1. Object detection and tracking: Used for detecting and tracking objects of interest in video footage.
2. Face recognition: Used for identifying individuals in video footage based on facial features.
3. License plate recognition: Used for reading and identifying license plates in video footage.

**Fortinet Models**

1. FortiGuard: Fortinet's threat intelligence service, which uses machine learning algorithms to analyze massive amounts of threat data and provide real-time protection against emerging threats.
2. FortiSandbox: A virtual environment used to analyze suspicious files and detect advanced threats using behavior-based analysis.
3. FortiWeb: A web application firewall that uses machine learning to detect and block malicious traffic and protect against application layer attacks.

**Vectra Models**

1. Cognito: This model is designed to detect advanced cyberattacks by analyzing network traffic in real-time using machine learning algorithms.
2. Account Lockdown: This model helps prevent cyberattacks by automatically detecting and responding to suspicious activity in user accounts.
3. Threat Certainty Index (TCI): This model provides a risk score that quantifies the level of threat posed by a given network device or user based on their behavior patterns.

**palo alto network Models**

1. Next-Generation Firewall: Palo Alto Networks uses a next-generation firewall (NGFW) that leverages machine learning and AI to provide visibility and control over network traffic.
2. Cortex XDR: Cortex XDR is a security operations platform that combines endpoint detection and response, network detection and response, and cloud workload protection to detect and respond to threats.
3. Prisma Cloud: Prisma Cloud is a cloud security platform that uses machine learning and AI to provide security and compliance for cloud workloads and applications.

**symantec Models**

1. Norton AntiVirus Plus: Uses machine learning and artificial intelligence algorithms to detect and remove malware.
2. Norton 360: Offers multi-layered security using signature-based detection, heuristics, and behavioral analysis.
3. Norton Mobile Security: Uses machine learning and artificial intelligence to detect and remove malware, and also includes anti-theft and privacy protection features.

**cisco system Models**

1. Cisco Identity Services Engine (ISE): This model provides advanced access control and security policy enforcement for wired, wireless, and VPN networks.
2. Cisco Advanced Malware Protection (AMP): This model provides endpoint security through malware detection, blocking, and remediation.
3. Cisco Umbrella: This model provides cloud-delivered security for web browsing and internet access across all devices on a network.

**Trend microModels**

1. Trend Micro Deep Discovery Inspector - This solution uses machine learning to detect and analyze threats in network traffic. It uses a combination of supervised and unsupervised learning to identify suspicious activity and malware in real-time.
2. Trend Micro XDR - This is a cloud-based detection and response platform that uses machine learning to identify and respond to advanced threats across endpoints, email, and networks. It includes advanced analytics and machine learning models to detect and prevent threats.
3. Trend Micro Cloud App Security - This solution is designed to protect cloud applications like Microsoft Office 365 and Google G Suite. It uses machine learning to detect and block threats like malware, phishing, and ransomware.