

Cisco Company Complicity Profile



Cisco's complicity in Israel's apartheid and genocide is well documented through its illegal operations in the Occupied Palestinian Territory, discriminatory policies, partnership with the Israeli military, and acquisitions of Israeli companies complicit in human rights violations. Cisco knowingly provides Israel with technology that is deployed to facilitate grave human rights violations, war crimes, and crimes against humanity. An senior Israeli Air Force officer has publicly [admitted to](#) using Cisco-powered infrastructure in Israel's genocide against Palestinians in Gaza to support operations for communications and managing high volumes of operational data—including the use of networking tools by drone operators and ground forces to store and analyze videos and share coordinates for strikes.

Cisco Has Illegal Operations in the Occupied Palestinian Territory including Settlements

Cisco and Israel partnered to build 100 Tech Hubs by the end of 2019, seven of which are in illegal settlements – which are [war crimes](#) under international law – 5 in the occupied West Bank, 2 in the occupied Syrian Golan Heights. Cisco also has [provided services](#), including cybersecurity tools and access to network management and monitoring platforms, to institutions involved in the illegal occupation, including the Israel Electric Company, Mekorot (the National Water Company of Israel), the municipality of Jerusalem, the Israeli Ministry of Justice, as well as major Israeli banks operating in the West Bank such as Bank Leumi, Israel Discount Bank, and Bank Hapoalim.

- Mekorot was cited in the International Court of Justice's [July 19 2024 Advisory Opinion](#) under "Exploitation of natural resources" which reported that [Israel prioritizes the water supply of illegal settlements](#) which causes Palestinians to suffer from lengthy and frequent water outages.

Cisco is a Long-Standing Partner of the Israeli Occupation Forces

Military Partnerships

- In October 2023, [Cisco increased sales and services to Israel](#), driven overwhelmingly by the needs of the Israeli military perpetrating the genocide. A leaked slide deck comparing revenue results between 2023 and 2025 shows that the total Cisco revenue from its Israeli business in the first half of each year rose from \$109 million to \$150 million between 2023 and 2024. It highlighted the importance of "capturing defense opportunities" in Israel, with one slide headlined with a quote: *"Never let a good crisis go to waste."*
- Since at least 2023 Cisco has been providing numerous [recurring services sold to institutions](#) that make up key nodes of the Israeli government and military, including the Israeli Air Force, Israeli Navy, the Israeli Defense Forces Computing and Information Systems unit (MAMRAM), the office of the Prime Minister, which includes the Mossad and Shin Bet, the Israel Prison Service (SHABAS), the Ministry of Defense computing unit (MALAM), and numerous defense companies owned by or closely tied to the government, [including](#) Israeli weapons manufacturers Elbit Systems, Rafael Advanced Defense Systems, and Israel Aerospace Industries.
- In November 2023, Cisco sold Webex, a communications solution, to the Israeli military in partnership with [Bynet](#), an Israeli tech company that assists in automating genocide and provides services to Israeli prisons and illegal settlements. During this period, Cisco also introduced [Security Service Edge](#), cloud-based security platform, following a [request](#) from Israel as "One of the asks for Israel War relief/support".
- In 2023, Dell was [selected](#) to replace Cisco as the main provider of servers for the Israeli military.

However, the military continues to buy Cisco servers, as was revealed by an [Israel Ministry of Defense \(IMoD\) procurement database](#). It shows that in just three months, between November 2023 and January 2024, in the middle of Israel's Gaza genocide, IMoD purchased Cisco servers worth a total of almost \$2 million over eight different contracts. This is likely an underestimate, as this database only discloses *unclassified* contracts that were awarded without a tender process.

- Israel's initial genocidal attacks on the Gaza Strip required unprecedented computing power. The Israeli military [took several steps](#) to address the need for increased computing capacity and it is likely that the urgent procurement of Cisco servers was a part of this process. This potentially implicates Cisco in the mass killing of tens of thousands of Palestinians. Cisco technologies possibly form the hardware infrastructure that hosts at least some of the databases and AI systems ([The Gospel](#), [Lavender](#), and [Where's Daddy?](#)) that the Israeli military developed to generate mass targets at unprecedented scale with minimal human intervention.
- [According to Cisco's former VP of Technology, Haim Pinto](#), "The connection between the technology units in the Israeli military and the high-tech companies in Israel is a significant anchor in the accuracy and advanced development of technologies that serve the security of the state and the bodies responsible for it... The sight of officers in uniforms sitting next to our engineers and developing technological solutions together is very natural to us, but still exciting."
- In October 2023, as Israel began its genocide in Gaza, Cisco's CEO Chuck Robbins stated that Cisco was "[working day and night to ship our technology to Israel](#)" including unique cybersecurity capacities. He had previously [stated](#), "We are proud to partner with Israel. The incredible amount of innovation that comes out of Israel is something that we look forward to continue driving in the future."
- In April 2021, an [internal report entitled "Cisco Israel Ministry of Defense Win"](#) boasts that the company was already making \$40-50 million a year from computer contracts with the Israeli MoD, highlighting an agreement to provide a new list of itemized services, including enterprise and data center networking, cybersecurity, and classified network support. For the MoD, the report notes, the services in the Cisco agreement "are as important ... as the focus on aircrafts, tanks and any other essential military tools."
- In March 2020, Cisco Systems began laying tens of [Unified Communication systems for the Israeli military](#), expected to reach hundreds of systems. The unified network centralizes the transfer of video, voice, and data between different Israeli military units.
- Cisco Systems' computing and communication systems, as well as cyber security and load balancing systems, were [integrated](#) into the Israeli military's largest ICT underground data center in the Naqab called David's Citadel, completed in 2020.
- In 2017, Cisco was [selected](#) by the IMoD to replace [Hewlett Packard Enterprise](#) as the sole provider of servers for the Israeli military and other security forces. Cisco Israel's CEO [stated](#) at the time that this contract "is integral to [the company's] commitment to the State of Israel." The contract was initially valued at a minimum of \$250 million, paid for by the U.S. government through its [Foreign Military Sales program](#).
- In 2013, Cisco [partnered with the Israeli military](#) to supply \$150M in communications equipment over 5 years with an option to extend 2 years.

Government Partnerships

- In October 2023, Cisco Israel [developed](#) "Israel Rises" for the Israeli military (Home Front Command), which is a Cisco-powered national platform that facilitates cross-sector joint action to materially support

Israel's genocidal assault on Gaza in violation of three legally-binding orders by the International Court of Justice (ICJ).

- In 2017, Cisco [sold](#) servers and support services to upgrade the Israeli military's and Israeli Ministry of Defense's networks through Bynet, Israel's leading provider of end-to-end integration solutions and services. Bynet [provides](#) Israeli border patrol, police, and other law enforcement agencies with [invasive surveillance tools](#). Bynet is also widely recognized for [providing services to Israeli prisons](#), including a [phone tapping service](#) using voice biometric data of Palestinian prisoners, many of whom are [held hostage without charge or trial](#) in inhumane conditions described as "[human chicken coops](#)" by the leading Israeli human rights organization.
- In 2017, Cisco [partnered](#) with the Israeli municipality of Jerusalem to develop, on a pro bono basis, "Smart City" technology specially designed to surveil Palestinians in occupied East Jerusalem. In the same year, [Cisco installed communication equipment and CCTVs](#) for the municipality. Deployment of Cisco's surveillance technology violates, *inter alia*, the [Universal Declaration of Human Rights articles 12 and 17](#), which state that no person should be subjected to arbitrary interference with their privacy.

Police Partnerships

- Between 2020 and 2021, Cisco [sold](#) equipment and software worth over \$1M to the Israeli police, [notorious for its human rights violations](#). Additionally, Cisco sold additional software to the [Israeli police](#) in August 2022.

Cisco Has Acquired at Least 20 complicit Israeli Companies (below is a non-exhaustive list)

- May 2026: Astrix Security (US\$400M) - Cybersecurity company founded by Alon Jackson and Idan Gour, both from Israel's infamous Unit 8200
- September 2024: Robust Intelligence (US\$400M) - AI security platform founded by Yaron Singer, an Israeli senior executive at Cisco (former IOF special operations unit combat officer), who recently [said](#), "Personally, I'm eager to invest in Israeli companies and recruit talent from Israel."
- August 2023: Oort - cybersecurity company co-founded by Israeli Didi Dotan, a Senior Director at Cisco who [espouses extremist racist views](#) against Palestinians.
- October 2021: [Epsagon](#) (US\$500M) - application monitoring and observability company co-founded by Israelis, Nitzan Shapira and Ran Ribenzaft, who are now Directors at Cisco.
- May 2021: [Sedona Systems](#) (US\$100M) - communications company co-founded by Israeli, Ori Gerstel, who is a Senior Director at Cisco.
- October 2020: [Portshift](#) (US\$100M) - cybersecurity company co-founded by Israeli, Zohar Kaufman, who is a Director in Cisco's Tel Aviv office.
- March 2016: [Leaba Semiconductor](#) (US\$350-400M) - co-Founder Eyal Dagan is currently on Cisco's Executive Leadership Team reporting directly to the CEO.
- February 2013: [Intucell](#) (US\$475M) - co-Founder Rani Wellington was a VP and General Manager and co-founder Ido Susan was the Head of Mobility Solutions at Cisco.

Cisco has also invested heavily in Israeli technology companies. By 2018, Cisco had [invested more than \\$2](#)

[billion](#) and has since [continued investing](#) further.

Cisco Engages in Discriminatory Practices and Anti-Palestinian Racism

- **Internal Censorship:** In 2025, [Cisco announced a restriction of internal discussions and debates on the “Middle East”](#)—and specifically on Palestine, fired a pro-Palestinian employee and shut down its employee led collective “Bridge to Humanity” chat room and educational website for holding the company accountable to its own policies & the law with regards to their employment conditions.
- **Hostile Environment:** In 2024, Cisco leadership failed to properly address several instances of [anti-Palestinian racism from their internal chats](#).
- Cisco operates a donation matching program that matches employee contributions up to \$10,000 per employee to organizations including **Friends of the Israeli Defense Forces**, which raises funds for the Israeli military and supports Israeli settlements.
- **Company Policy of Institutionalized Economic Discrimination:** In 2008, [Cisco pioneered a model of racial discrimination and exploitation](#) that Intel, Microsoft, and Mellanox soon followed. Whereas an Israeli hi-tech worker would have been paid ~\$4,000, Cisco Israel began outsourcing work to skilled Palestinian hi-tech workers at a far lower rate, ~\$2,500, benefiting from Israel’s system of apartheid.