OT REMOTE-ACCESS PLATFORMS

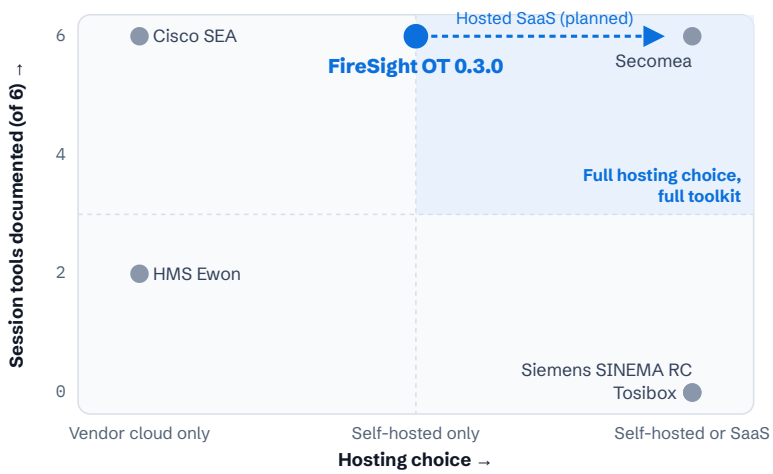
How FireSight OT compares

Twenty-four features, checked against each vendor's public documentation. A dash means no clear statement found, not a missing feature.

Feature	FireSight OT	Secomea	HMS Ewon Talk2M	Tosibox (Tosi)	Siemens SINEMA Remote Connect	Cisco Secure Equipment Access
CONNECTING SITES						
Outbound-only from the site	✓	✓	✓	✓ [1]	✓ [2]	✓ [3]
Sites with the same (overlapping) addresses	✓	✓	– [4]	✓ [5]	✓ [6]	– [7]
Machine VLANs on one site device (trunk port)	✓ 0.4β [8]	✓ [9]	– [10]	✓ [11]	✓ [12]	✓ [13]
The same addresses on every VLAN (identical lines, one box)	✓ 0.4β [14]	–	–	– [15]	✗ [16]	– [17]
Time server (NTP) for the machines	✓ 0.4β [18]	✓ [19]	✓	✓	–	–
Bring your own site hardware (no lock-in)	✓	✓ [20]	– [21]	✓ [22]	–	– [23]
WHO GETS IN						
Access per machine, not the whole network	✓	✓	✓ [24]	✓	✓	✓
Time-limited vendor access (hours and end date)	✓	✓ [25]	– [26]	–	✓ [27]	✓
Multi-factor sign-in	✓	✓ [28]	✓ [29]	✓	✓	✓
Server you can host yourself	✓	✓ [30]	– [31]	✓	✓	✗ [32]
IN THE SESSION						
Web HMI in the browser, no client	✓	✓	✓	–	–	✓
RDP, VNC or SSH in the browser	✓	✓ [33]	✓ [34]	–	–	✓
Serial (RS-232 / RS-485) access	✓ [35]	✓ [36]	–	–	–	✓ [37]
File transfer	✓ [38]	✓ [39]	–	–	–	✓ [40]
Session recording	✓ [41]	✓ [42]	–	–	–	✓ [43]
MONITORING						
Alert when a site device goes offline	✓	✓	✓ [44]	✓ [45]	–	✓ [46]
Alert when a machine behind it stops answering	✓	✓	– [47]	– [48]	–	–
THREAT DETECTION						
Threat detection on the site device	✓ 0.4β [49]	–	–	✓ [50]	– [51]	✓ [52]
Threat linked to the remote session, with one-click response	✓ 0.4β [53]	–	–	– [54]	–	✓ [55]
SIEM AND SECURITY INTEGRATIONS						
REST API	✓ 0.4β [56]	✓ [57]	✓ [58]	✓	✓ [59]	✓
Webhooks for events	✓ 0.4β [60]	– [61]	–	–	–	–
Syslog / SIEM export (CEF, LEEF)	✓ 0.4β [62]	✓ [63]	–	–	✓ [64]	– [65]
Ready-made integrations with OT security platforms	✓ 0.4β [66]	–	–	–	–	– [67]
Audit log	✓	✓	✓	✓ [68]	✓	✓

✓ Yes · ✓ Yes, with a condition (see note) · – No clear statement found · ✗ No · ✓ 0.4β FireSight OT 0.4.0, in beta now

Where FireSight OT sits, and where it's heading



How it's scored. Across: where the server can run, from the documentation (vendor cloud only; self-hosted only, on premises or in your own cloud; self-hosted or vendor SaaS). Up: how many of six in-session tools are documented, counting conditional ones: web HMI in the browser, RDP/VNC in the browser, SSH in the browser, serial access, file transfer and session recording.

Today, with 0.3.0, FireSight OT has the full in-session toolkit: browser remote desktop and terminal, serial consoles, file drop and terminal transcripts. It runs on your own servers or in a cloud VM, with strengths in identical lines and vendor access hours (see page 1).

Site hardware, your choice. Cloud Connectors are based on Raspberry Pi: buy ours, or build your own from parts at any local store.

Coming soon: RDP/VNC video recording, SMS alerts and a mobile app. A hosted SaaS option would move it across to full hosting choice.

A simple, transparent count, not a market ranking or an analyst rating. It doesn't weigh price, scale, support or maturity.

INTRODUCING IN FIRESIGHT OT 0.4.0 (IN BETA)

Remote access that knows when it's being abused

Threat detection, the remote session on the attacked machine, and the off switch, in one box.

Detect, at the point of access

A Cloud Connector with 8 GB listens to the switch's mirror port, built on Suricata with FireSight's signed OT rules for Modbus, DNP3, EtherNet/IP and S7. The listening port has no address and sends nothing. A licensed add-on, one licence per Cloud Hub.

The session, and the off switch

Each incident lists who had remote access through that site at the time, and flags a session on the attacked machine. One click ends the session, suspends the vendor or locks down the site.

Machine VLANs: identical lines on one box

Up to 20 machine VLANs on one Cloud Connector's trunk port, all with the same addresses, on top of 1:1 mapping between sites. Other gateways support VLANs, but we found none that documents identical addresses across them on one device.

Works with your SOC

REST API, signed webhooks and CEF, LEEF or JSON syslog. One-click setup for Dragos, Claroty, Nozomi Networks, Armis, Tenable and Forescout.

Lab-tested on simulated plant traffic, not yet at a customer site. Integrations: works with these platforms; no partnership or certification is implied.

Notes

1. Lock and Lock for Container need no open ports; a Virtual Central Lock needs a reachable address.
2. The device starts the tunnel; docs don't say outright that nothing inbound is needed.
3. Connects out to Cisco's broker; docs don't say outright that nothing inbound is needed.
4. 1:1 NAT exists; identical sites not described.
5. 1:1 NAT on hardware Locks in Layer 3 mode; not on Lock for Container.
6. With SCALANCE devices that support SINEMA RC NAT (e.g. SC-600, M-800, S615).
7. Works “regardless of IP address or NAT strategy”; overlap not described.
8. Up to 20 machine VLANs on one Cloud Connector's machine port.
9. Up to 4 isolated LAN ports on SiteManager 1439/3439; VLANs not described.
10. Designed for one machine LAN by default; more LANs through routers on distinct subnets.
11. 802.1Q access and trunk ports on the Tosibox 610 (up to 127 VLANs).
12. VLAN subnets per device (16 on S615 and M-800, 257 on SC-600).
13. Up to 10 VLANs on IE switches; not on IR routers.
14. Each VLAN is kept apart, so all 20 can use the same addresses, e.g. ten identical lines all on 192.168.1.x.
15. 1:1 NAT handles identical subnets across different Locks; on one Lock it's not described.
16. SCALANCE NAT document: identical subnets can't be connected to one S615 (V06.02 firmware).
17. Overlapping addresses across its VLANs not described.
18. Kept in step with the Hub through the tunnel; sites can refuse it.
19. Relays NTP requests to an upstream server through GateManager.
20. SiteManager Embedded, including Docker.
21. Hardware gateway.
22. Lock for Container on Docker, without Layer 2 or 1:1 NAT.
23. IOx app on Cisco IE/IR switches and routers.
24. Per Ewon gateway, with Talk2M Pro pools.
25. Account expiry only; no working hours described.
26. Temporary users only.
27. Expiry for temporary users per role; no working hours described.
28. SMS or single sign-on.
29. Talk2M Pro, by SMS.
30. “GateManager Own” option.
31. Only the Talk2M cloud is described.
32. SaaS; the broker runs in Cisco's cloud.
33. Secomea Prime, GateManager 11.9 and later.
34. RDP and VNC through M2Web; SSH not described.
35. RS-232 through USB console cables or USB-to-RS232 adapters on the Cloud Connector; RS-485 not covered.
36. SiteManager hardware with RS-232.
37. Reverse Telnet to a router's serial line (older developer docs).
38. Site file drop: files uploaded to the Cloud Connector over SFTP or FTP (kept 1–10 days), copied to the Hub and collected by backup software over SFTP or S3.
39. FTP and Shared Folder agents.
40. SEA Plus agent, up to 1 GB.
41. Text transcripts of browser terminal sessions (SSH, Telnet, serial), kept 90 days. RDP and VNC video recording is planned.
42. Professional and Premium tiers, in-browser protocols only.
43. Advantage tier, to your own AWS S3.
44. Talk2M pool offline notification by email, after 1 hour to 1 week; pools aren't in Talk2M Light.
45. Email alerts per node from the Tosibox HUB, with your own SMTP server.
46. IoT Operations Dashboard alert rules for gateway devices; SEA's own alerts cover sign-ins.
47. Only the Ewon itself going offline is described.
48. Disconnection alerts only; devices behind a node not described.
49. Detect add-on (one licence per Cloud Hub) on 8 GB Cloud Connectors, built on Suricata, with FireSight's signed OT rules.
50. Tosi Insight on existing Locks; Professional and Enterprise tiers.
51. Separate product: SINEC Security Monitor (no SINEMA RC link described).
52. Built in: identity threat alerts (ITDR). Network threat detection is the separate Cisco Cyber Vision sensor, which can run on the same IE switches.
53. Each incident lists the remote sessions at the time, flags one on the attacked machine; end session, suspend user or lock down the site.
54. Insight shows who connects; a one-click response tied to a detection is not described.
55. Blocking a user ends their sessions (ITDR); linking Cyber Vision detections to sessions is not described.
56. Scoped tokens per company and source address; OpenAPI file.
57. CRM API on customer-owned GateManagers.
58. Talk2M APIs, with a Talk2M Developer ID.
59. With a separate API licence.
60. Signed with HMAC-SHA256, with retries: access, Cloud Connector offline, machine down, threats, sign-ins, changes.
61. KB lists “Sending alerts over HTTP and TCP”; webhooks not described.
62. CEF, LEEF or JSON over TLS, TCP or UDP, plus signed webhooks and one-click OT platform setup.
63. GateManager logging to a syslog server; CEF/LEEF not described.
64. Syslog to a central server over UDP, TCP or TLS; CEF/LEEF not described.
65. Session logs export as CSV.
66. One-click setup for Dragos, Claroty, Nozomi Networks, Armis, Tenable and Forescout: syslog events out, a read-only API token in, optional session ending. Works with; no partnership implied.
67. Integrations (e.g. Splunk) are documented for Cisco Cyber Vision, a separate product.
68. Audit events on the Virtual Central Lock.

Sources (public vendor documentation, read 24-28 October 2026)

Secomea: secomea.com product pages; SiteManager 15xx/35xx datasheet; kb.secomea.com articles on in-browser connections, account expiry, GateManager Own, SiteManager Embedded and alerts. **HMS Ewon / Talk2M:** hms-networks.com Talk2M security whitepaper and firewall requirements; help.ewon.biz (M2Web, Talk2M Pro, pool offline notifications). **Tosibox (Tosi):** helpdesk.tosibox.com (Lock, Lock for Container, Virtual Central Lock, Access Groups); Tosibox HUB user manual; blog.tosi.net. **Siemens:** SINEMA Remote Connect operating manuals V3.2 SP3/SP4 and NAT / Dedicated Device Access notes, cache.industry.siemens.com. **Cisco:** Secure Equipment Access datasheet, cisco.com; IoT Operations Dashboard docs (incl. alerts and notifications), developer.cisco.com/docs/iotod.

Detection, VLANs, API, webhooks, syslog, integrations and NTP rows: Secomea SiteManager 1439/3439 datasheet, Security FAQ whitepaper, kb.secomea.com (NTP server relay, release 11.5); HMS: developer.ewon.biz (M2Web and DMWeb APIs), hms-networks.com KB (NTP server, multiple machine LANs); Tosi: tosi.net (Tosi Insight, network monitoring and analytics, TosiControl datasheet), Tosibox 610 datasheet, helpdesk.tosibox.com (NTP, 1:1 NAT, overlapping addresses); Siemens: SINEMA RC Server operating instructions (API licence, syslog), SCALANCE NAT application document 109744660, SINEC Security Monitor product page; Cisco: developer.cisco.com/docs/iotod (ITDR insights, SEA multi-VLAN, SEA APIs), Cisco Cyber Vision 5.6 release notes (SEA renamed Cyber Vision Secure Remote Access).

Features, editions and names change; check with each vendor before deciding. Some features depend on edition or licence tier. Secomea, Ewon, Talk2M, Tosibox, Tosi, SINEMA, SCALANCE, Siemens, Cisco and Raspberry Pi are trademarks of their respective owners; no endorsement is implied. Spotted something out of date? Tell us at hello@firesightsystems.com and we'll correct it.