tosi

The fastest way to connect, visualize and control OT networks and critical infrastructure.

Research Report

2026 STATE OF OT SECURITY REPORT

A benchmark study of operational technology security maturity across 77 US enterprises.

RESEARCH CONDUCTED

FEBRUARY 2026

METHODOLOGY

HOW THIS RESEARCH WAS CONDUCTED

This benchmark is built on a structured OT Security Maturity Assessment completed by 77 security and operations professionals at US enterprises. Each respondent answered ten questions across five capability dimensions, scoring their organization on a 1-to-5 scale per question. The maximum total score is 50.

WHO RESPONDED

Security and operations professionals at enterprises with over $1 billion in annual revenue. Research was conducted by an independent firm in February 2026.

INDUSTRIES

Real Estate / Property Management (43%), Retail (17%), Financial Services (16%), Wastewater (11%), Manufacturing (8%), Oil & Gas (5%).

REGION

United States. Results are presented as a standalone benchmark and compared to the European respondents (n=58) throughout.

SCORING

Two questions per dimension, each scored 1-5. Section maximum: 10. Overall maximum: 50. Higher scores reflect greater maturity and operational depth.

Each capability was assessed across two questions: the first measuring breadth or coverage (do you have this in place?), the second measuring depth or enforcement (how well is it operationalized?). This structure allows the research to distinguish between organizations that have adopted a control and those that have truly embedded it.

1 Asset Visibility

Can you identify and inventory your OT assets? How do you track and maintain that information over time?

2 Network Segmentation

How is your OT network separated from IT? How do you manage traffic within your OT environment?

3 Remote Access

How do vendors and employees access OT systems remotely? How quickly can you grant or revoke that access?

4 Threat Detection

How do you monitor for anomalies or threats? How do you identify unusual device behavior or unauthorized connections?

5 Deployment & Multi-Site Management

Can you identify and inventory your OT assets? How do you track and maintain that information over time?

Maturity levels are assigned based on total score:

10-18	19-26	27-34	35-42	43-50
Level 1	**Level 2**	**Level 3**	**Level 4 < US avg**	**Level 5**
Initial significant gaps, high risk	Developing some controls in place	Defined solid foundation, room to grow	**Managed strong posture, improving**	Optimized industry-leading maturity

KEY FINDINGS

WHAT THE DATA SHOWS

The average US enterprise scores 35.9 out of 50, placing the field at Level 4 (Managed). The more interesting story is in the distribution: 18% of organizations have reached Level 5 (Optimized), and the capability profile shows a clear pattern: stronger on Asset Visibility, weaker on managing vendor remote access.

FINDINGS 1

Manufacturing scores lowest of any industry

US Manufacturing scores 31.2/50 on average, more than eight points below Wastewater and nearly four points below Financial Services. Only one in three Manufacturing organizations has reached Level 4.

The gap is concentrated in one area: how vendors and employees access OT systems remotely. That single question averages 1.67 out of 5 across Manufacturing respondents - the lowest score of any individual question in the entire dataset. Five of the six Manufacturing organizations scored a 1 or 2, meaning most have no structured method in place at all.

The ability to remove or revoke vendor access scores only 3.0 out of 5. That means even the organizations that have some form of vendor access in place cannot cleanly control it. Purpose-built OT remote access tools exist to fix this. What is missing is a consistent process for using them.

Manufacturing scores 1.67 out of 5 on how vendors access plant floor systems - the lowest score of any individual question across all 77 organizations in this study. Five of six (83%) Manufacturing respondents scored a 1 or 2, meaning open ports or shared credentials with no individual accountability.

FINDINGS 2

Wastewater scores highest of any industry

US Wastewater enterprises score 39.4/50 on average, the highest of any industry in this study, with 75% at Level 4 or higher. One respondent scored a perfect 50, the highest individual score in the entire dataset. Wastewater sits more than eight points above Manufacturing and four points above the next industry.

The scores are strongest in Asset Visibility and Threat Detection, both averaging 8.38 out of 10, with Network Segmentation close behind at 8.25. These are the three capabilities where consistent operational discipline shows most clearly. Wastewater's biggest lead over Manufacturing is in Remote Access: 7.25 versus 4.7, a gap of more than two and a half points.

The one area where Wastewater does not stand out is multi-site visibility, averaging 3.12 out of 5 on that question. That pattern is consistent with the rest of the dataset: getting a new site running is faster than getting it fully visible.

The result likely reflects sustained pressure from the EPA and CISA on US water sector operators. That pressure has produced operational discipline applied consistently over time, which is what separates the top of the maturity scale from the middle.

Wastewater leads every capability area except multi-site visibility. Its biggest margin over any other industry is in vendor access management, where it scores 7.25 out of 10 compared to Manufacturing's 4.7.

See Appendix B for full industry breakdown.

FINDINGS 3

Asset visibility scores well overall, but 1 in 5 Real Estate organizations cannot account for what is on their network

Asset Visibility is the highest-scoring capability in the study, averaging 7.50 out of 10. Financial Services is the only industry where every respondent can fully account for what is on their operational network. Every other industry has organizations that cannot.

Real Estate has the most significant gap: 1 in 5 respondents scored critically low on knowing what devices are connected to their network. For an industry that manages large, distributed physical environments with significant OT infrastructure, that is a meaningful exposure.

The risk is not abstract. Every other control in this study depends on the asset inventory being complete. An organization that cannot see all its devices cannot segment them, cannot monitor them, and cannot know whether access to them has been compromised.

1 in 5 Real Estate organizations cannot fully account for what is connected to their network, which means their segmentation, monitoring, and access controls may be protecting against threats they can already see, while leaving unknown devices completely unmanaged.

FINDINGS 4

Vendor access management is the consistent weak point across all five areas

Remote Access is the weakest-scoring capability in the dataset. Specifically, how quickly vendor access can be granted or revoked is the lowest-scoring individual question across all five capability areas. 10 respondents score high on access method but low on managing it: the tools are in place, but the process is not. That gap between having the right tools and managing them is the defining weakness in the dataset.

1 in 3 US organizations takes hours or longer to revoke a vendor's access to plant floor systems. 1 in 8 takes days or weeks. If a vendor's credentials are compromised, that is how long the exposure lasts.

DEEPER ANALYSIS

THREE PATTERNS WORTH NOTING

Looking beyond the headline scores, the question-level data reveals three patterns that are counterintuitive or worth flagging for OT and operations practitioners.

PATTERN 1

The connections within the plant floor are better managed than the boundary between office and plant floor

The survey asked two separate questions about network segmentation:

1. How is your OT network segmented from your IT network?
2. How do you manage east-west traffic within your OT environment?

Respondents scored an average of 3.40 out of 5 on the first question and 4.01 out of 5 on the second. The gap is significant, and the direction matters. Organizations score lower on separating OT from IT networks than on managing traffic within their OT environment - the greater gap lies at the perimeter boundary, not the internal connections.

Nine respondents scored high on one question and low on the other. That means their overall segmentation score looks the same as an organization that has done both well. The score does not tell you which half is missing.

The practical question for any plant manager or facilities director: if a device on your corporate IT network attempted to reach your OT systems, would it be stopped? If the answer is no, or uncertain, that is where the gap is. The data shows organizations manage east-west traffic within their OT environment well - the weaker half is the boundary separating IT from OT.

Nine respondents scored high on one segmentation question and low on the other. A score that looks solid overall can be hiding a gap in one half of the job. Ask your team directly: which half have we verified?

PATTERN 2

Many organizations have strong threat detection, but suffer gaps in OT network monitoring

10 US respondents scored low on broad monitoring deployment but high on identifying unusual device behavior. They have sophisticated detection capability in specific areas but have not extended monitoring across their full OT environment. This is the reverse of the expected pattern, where you would expect broad deployment to come before depth of detection.

This suggests these organizations have invested in advanced detection tools, likely at primary sites or for high-priority assets, without first achieving consistent baseline monitoring across all OT infrastructure. The risk is a false sense of coverage: strong detection where monitoring exists, but significant blind spots where it does not.

Strong detection capability in some areas does not mean comprehensive coverage. For these organizations, the priority is extending baseline monitoring broadly before investing further in detection depth.

PATTERN 3

US enterprises deploy new sites faster than making them visible, which is a risk

Deployment speed consistently outpaces multi-site visibility, with organizations scoring notably higher on how quickly they can stand up secure connectivity at a new site than on how well they maintain visibility and control across all their sites. 13 respondents scored high on deployment speed but low on multi-site control, the highest conflict count of any capability in the US dataset.

Every new site deployed without a corresponding improvement in cross-site visibility adds another blind spot. This is a structural challenge for any enterprise managing a growing multi-site OT estate: deployment processes tend to be optimized for speed, while visibility and monitoring get treated as a follow-on task rather than a go-live requirement.

Deployment speed is not the same as deployment quality. Getting a new site up quickly matters less if you cannot see across all your sites once it is live.

RECOMMENDATIONS

WHAT TO DO NEXT

The patterns above point to a consistent theme: for many organizations, the gap in US OT security is not solely a tools gap; it is also a process and enforcement gap. For those still relying on IT-native tools rather than purpose-built OT solutions, the right technology is also part of the answer. The following recommendations address the four areas where that gap is most consequential.

1 Enforce time-limited, identity-based vendor access with no shared credentials and no exposed endpoints

Remote Access is the weakest-scoring capability in the dataset. 1 in 3 US organizations takes hours or longer to revoke a vendor's access. The tools are in place - the process is not.

1. Open your remote access platform now. Export every active vendor credential. Anything unused in the last 30 days: revoke it before end of day.
2. Check whether each vendor has a unique, individually assigned identity. Shared credentials make attribution impossible - no shared passwords, no backdoors. Separate them.
3. Set every active credential to auto-expire at job completion. Your platform should enforce time-bound access windows by design, not a checklist.
4. Ensure your remote connectivity exposes no static public IP addresses. Encrypted outbound tunnels require no open inbound ports and no visible attack surface. If your architecture depends on exposed endpoints, that is a gap to close now.

2 Put OT security ownership in operations' hands and give them tools purpose-built for OT, not repurposed from IT

US Manufacturing scores 31.2/50 - the lowest of any industry. The single weakest question in the entire dataset is how vendors access plant floor systems, averaging 1.67 out of 5.

1. Walk your OT network physically this week. Identify every device connected to the control network. If something is there that you cannot account for, that is your first priority.
2. Test your segmentation. From an OT device, attempt to reach an IT device by IP address. If it responds, your network is not segmented in practice. Remote access should reach specific assets - not broad segments.
3. List every third-party vendor with access to your control systems. For each one, document: what assets they reach, how they connect, who approves their sessions, and how you revoke access in an emergency.
4. Pick one policy and verify it is followed at every site. Not assumed. Verified. Document where it holds and where it does not.

3 Stop deploying faster than you can see: make visibility a go-live requirement, not a follow-on task

12 respondents scored high on deployment speed but low on multi-site control - the highest conflict count of any capability in the dataset. Getting a site live is faster than getting it visible.

1. List every site you are responsible for. Open your monitoring platform. Confirm each site is visible. Any site not in the dashboard is a blind spot. Write it down and assign a fix date.
2. Add one requirement to your go-live checklist: OT monitoring active and verified before the site is considered operational. No exceptions. Discovery should begin automatically on connection - no added appliances.
3. Set a 30-day inventory deadline per new site. Your platform should identify devices passively, including industrial protocols that IT-native tools cannot read.
4. Configure alerts to be centralized. An anomaly should surface to whoever is on watch - not sit in a local log.

4 Close the gap between documented and enforced: test your controls before an incident does it for you

The organizations at the top of the maturity scale have one thing in common: they have turned deployed tools into enforced controls. The gap between having something in place and running it consistently is what separates Level 3 from Level 5.

1. Take one control you have documented and test it. Not reviewed on paper. Actually tested. Does the segmentation hold? Does the alert fire? Does anyone get notified?
2. Ask your team: if an unauthorized device appeared on the OT network right now, what would happen? Monitoring purpose-built for OT should flag it automatically - new devices, abnormal traffic, unexpected external connections. If uncertain, that is your gap.
3. Check whether your detection tools are deployed at every site, not just the primary one. Fleet-wide visibility should require no exposed public endpoints. List any site without active monitoring and treat it as your highest priority.
4. Fix the weakest control before adding anything new.

CONCLUSION

THE BOTTOM LINE

The average US enterprise sits at Level 4 (Managed), and 18% have reached Level 5 (Optimized). The organizations at the top have one thing in common: they have turned deployed tools into enforced controls. That distinction, between having something in place and running it consistently, is what separates the top of the maturity scale from the middle.

The two areas that need attention are vendor remote access management and Manufacturing maturity. Both represent a gap between having the right tools and using them well. Where purpose-built OT tools are in place, consistent operational discipline at the site and team level is what's needed - the kind that facilities managers, automation engineers, and plant leads are positioned to drive directly. For organizations still relying on IT-native tools, moving to purpose-built OT solutions is also part of closing the gap.

The US OT security story is one of strong highs and avoidable lows. The organizations at the top have gotten there through consistent enforcement, not by purchasing more tools. The organizations that are falling behind, particularly in Manufacturing and Remote Access, may be relying on IT-native tools rather than purpose-built OT solutions. And where the right tools are in place, what's missing is the day-to-day operational ownership that turns a deployed control into an enforced one.

Average maturity: Level 4 (Managed) | n = 77 | $1B+ revenue | February 2026

APPENDIX

REFERENCE DATA

APPENDIX A: US VS EUROPE CAPABILITY SCORES

■ US stronger ■ Roughly on par ■ US weaker

CAPABILITY	US /10	EUROPE /10	OBSERVATION
Threat Detection	**7.76**	7.55	Strongest capability; US leads Europe modestly
Asset Visibility	**7.50**	6.83	US significantly ahead; 18% still score critically low
Network Segmentation	**7.39**	7.26	Strong on both sides; US holds a small edge
Deployment	**6.80**	6.83	Roughly on par; multi-site control a weakness for both
Remote Access	**6.47**	6.62	Only capability where US trails Europe; active management is the weak point

APPENDIX B: SCORES BY INDUSTRY

INDUSTRY	N	AVG SCORE	AT L4-5	PRIMARY GAP
Wastewater	8	39.4/50	75%	Deployment
Oil & Gas	5	37.2/50	80%	Remote Access
Real Estate / Prop. Mgmt	33	36.8/50	67%	Deployment
Retail	13	35.2/50	46%	Remote Access
Financial Services	12	34.2/50	50%	Remote Access
Manufacturing	6	31.2/50	33%	Remote Access

APPENDIX C: CAPABILITY SCORES BY INDUSTRY

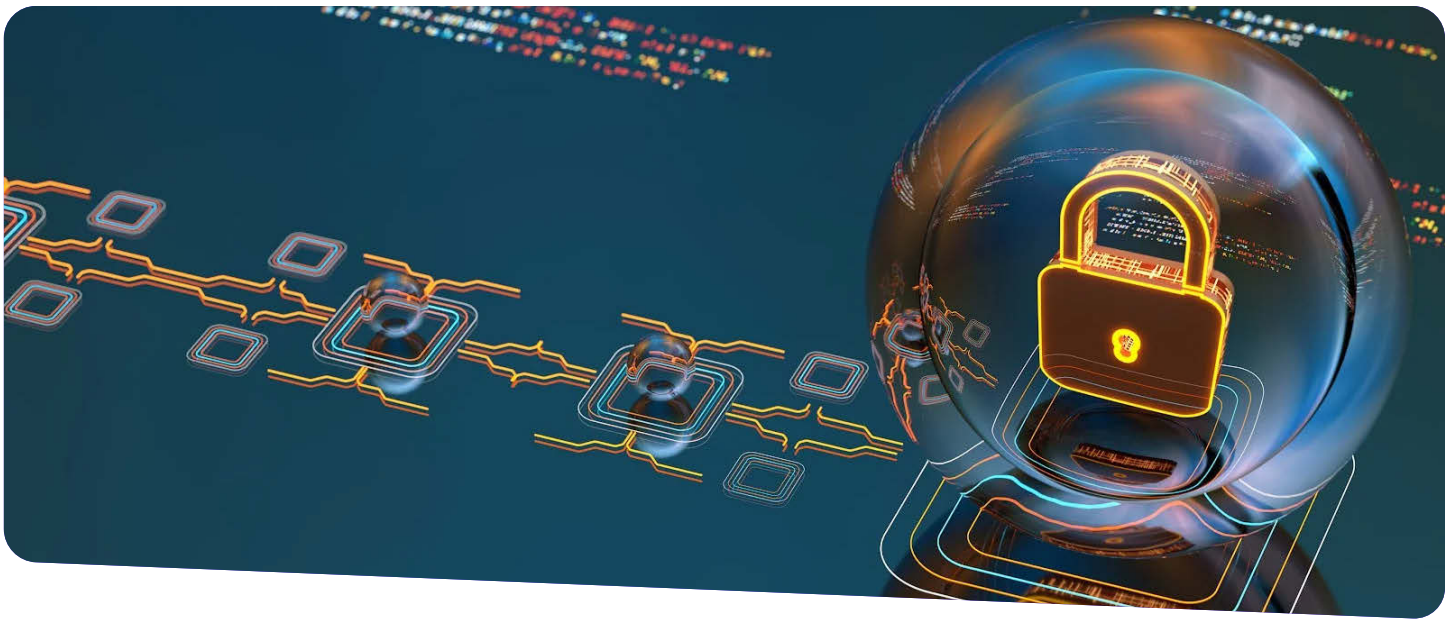
Average scores per capability area, out of 10. Overall score out of 50. Industries ranked by overall score. US Overall row reflects 77 respondents.

INDUSTRY	N	OVERALL /50	ASSET VISIBILITY	NETWORK SEG.	REMOTE ACCESS	THREAT DETECTION	MULTI-SITE DEPLOYMENT
Wastewater	8	39.4	8.4	8.2	7.2	8.4	7.1
Oil & Gas	5	37.2	7.2	7.8	6.6	8.2	7.4
Real estate	33	36.8	7.5	7.5	7.1	7.8	6.9
Financial services	12	34.2	7.2	7.0	6.0	7.5	6.5
Retail	13	35.2	7.9	7.2	5.7	7.8	6.5
Manufacturing	6	31.2	6.8	6.8	4.7	6.7	6.2
US Overall	**77**	**36.0**	**7.5**	**7.4**	**6.5**	**7.8**	**6.8**

Score ranges: 1.0-4.0 = developing capability 4.1-6.0 = defined capability 6.1-8.0 = managed capability 8.1-10.0 = optimized capability

---

Primary research conducted February 2026 with 77 security and operations professionals at US enterprises with annual revenues exceeding $1 billion. The full global study includes 135 respondents across the US, UK/Ireland, Germany, Benelux, and Finland. All scores calculated using a standardized 50-point rubric across five OT security capability domains.



NEXT STEPS

FIND OUT WHERE YOUR ORGANIZATION STANDS

The organizations that have reached the top of the maturity scale did one thing differently: they knew exactly where they were before they decided what to fix. Both options below start with that.

OPTION 1

Take the assessment yourself

The same ten-question assessment used in this study. Takes 5 minutes. You will receive a scored report showing where you stand across all five capability areas.

START THE ASSESSMENT

OPTION 2

Talk to an OT security specialist

A 30-minute conversation with a specialist who works with facilities, operations, and plant teams. No sales pitch. A direct conversation about what the data shows and what it means for your sites.

BOOK A CONVERSATION

US HQ
1212 Corporate Drive
Suite 170
Irving, Texas 75038

GLOBAL HQ
Elektroniikkatie 2a
7th floor
90590 Oulu, Finland

CONTACT US

tosi