

# Trusted Access

A Study of Remote Connectivity  
in Semiconductor Manufacturing



# Executive Summary

The semiconductor industry faces accelerating innovation, rising technical complexity, and intensifying global competition. As fabs and equipment providers work to improve performance, maximize uptime, and scale expertise across distributed manufacturing networks, **remote connectivity has emerged as a critical differentiator.**

This study, conducted by the Global Semiconductor Alliance (GSA) in partnership with Tracces by Capgemini, examines how the industry leverages remote access, the barriers it faces, and the value it delivers for manufacturing optimization.

Leaders should read this report to understand what's required to **unlock its full potential**, gain a clear view of where the industry stands today, and see what will determine who leads tomorrow.

Despite its importance, remote connectivity remains under-analyzed. Adoption is widespread but constrained by security concerns, trust gaps, and legacy systems. With the right foundations, it can accelerate innovation, empower smarter data-driven decisions, and serve as **a strategic enabler of future semiconductor manufacturing advantage.**

# Key Takeaways

Collaboration across the semiconductor industry has never been more critical

To boost efficiency, accelerate innovation and address workforce challenges



Report Efficiency Gains is the #1 adoption driver of remote connectivity



Report Access to Expertise as key driver of remote connectivity

Currently, security, trust, and scalability are blocking collaboration

Security concerns



Audit & compliance gaps



Performance & scalability issues



Yet, solving these challenges unlocks strategic value

Value derived:

- Reduced on-site support
- Improved equipment uptime
- Increase automation
- Smarter predictive maintenance
- Remote AI/ML-driven optimization

# Why Connectivity?

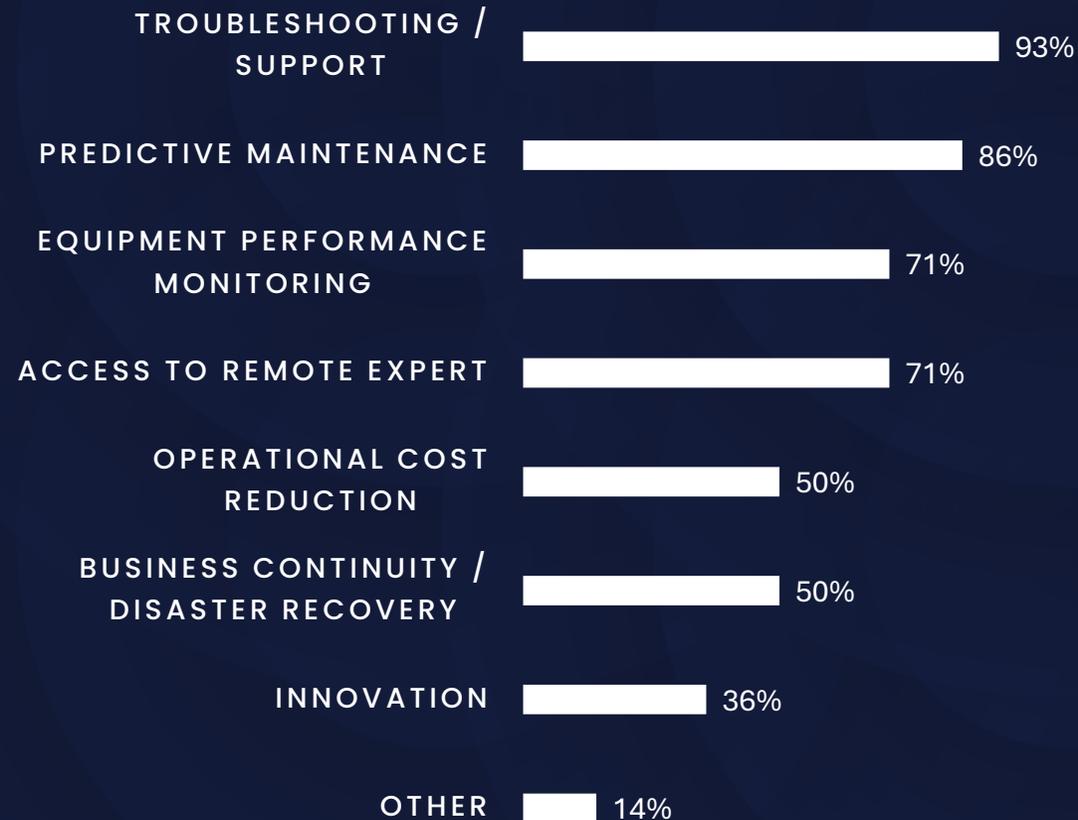
Primary reasons for remote connectivity, capability importance, & key barriers to adoption

## Key Takeaways

- **Troubleshooting / Support** is the primary reason for remote connectivity
- **Security and Access Control** is the leading capability area
- **Efficiency Gains** is the #1 adoption driver of remote connectivity



# Primary Reasons for Remote Connectivity



Remote connectivity has moved from an emerging practice to a foundational operational capability within semiconductor manufacturing. As industry players manage tighter process windows and equipment spread across global operations, remote access allows them to monitor and improve performance, resolve issues quickly, and avoid costly interruptions.

The study confirms strong integration of remote access into core workflows: 93% of respondents use it for troubleshooting and support, enabling rapid diagnostics without waiting for on-site personnel. Predictive maintenance (86%) further enhances uptime by identifying degradation before failures occur. Another 71% rely on it for performance monitoring to maintain continuous visibility into tool behavior. Additionally, 71% of companies depend on remote access to reach highly specialized experts, underscoring the importance of scaling scarce knowledge across facilities and time zones.

These patterns show that remote connectivity has become essential to maintaining uptime, accelerating service response, and enabling proactive maintenance. As equipment grows more complex and workforce constraints intensify, its strategic importance will continue to expand.

# Capability Importance

## Importance of Remote Connectivity Capability Areas

1 = Low, 5 = High

**4.8** Security & Access Control

**4.2** Support & Service

**4.1** Audit & Compliance

Fab	4.4
Equipment	3.6

**4.1** Performance & Scalability

Fab	4.4
Equipment	3.6

**4.1** Integration & Compatibility

**4.0** Usability

As companies broaden their remote connectivity programs, security and access control remain the most critical capabilities, with an average rating of 4.8. Given the sensitivity of operational data and IP, robust security is the foundation upon which all other remote activities depend.

Beyond this shared priority, fabs and equipment providers diverge in their needs. Fabs place greater emphasis on integration and compatibility (4.4 vs. 3.6) because they must manage multi-vendor environments and ensure interoperability across the production line. They also rate performance and scalability higher (4.4 vs. 3.6), reflecting the demands of supporting remote access across global fabs without compromising responsiveness.

These differences illustrate the operational realities each group faces: fabs must orchestrate complex system landscapes, while equipment providers focus more on the tools they deliver than on cross-platform integration. Aligning these priorities will require shared standards, scalable architectures, and consistent security and data governance frameworks.

# Key Drivers of Adoption

93%

Report **Efficiency Gains** is the #1 adoption driver of remote connectivity.

73%

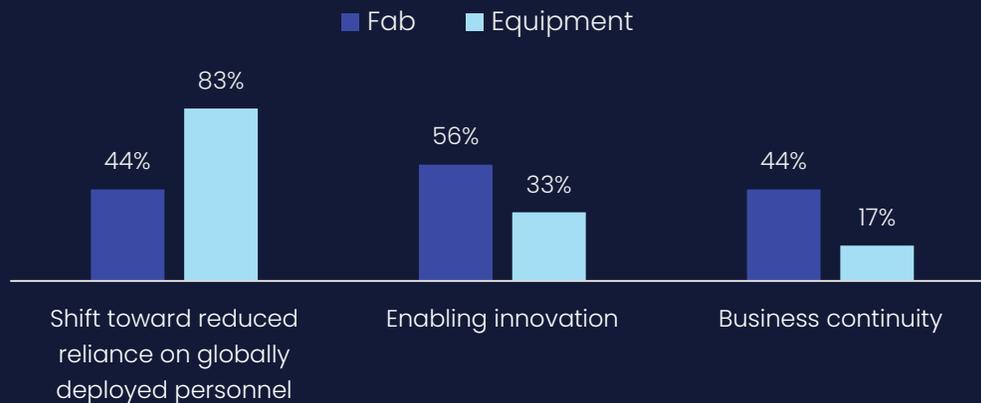
Report **Access to Expertise** as a key driver of remote connectivity.

Remote connectivity is driven by both operational efficiency and strategic necessity. The #1 adoption driver is efficiency gains (93%) followed by access to expertise (73%), cost savings (67%) and speed of support (67%).

Equipment providers are especially motivated by the ability to reduce reliance on globally deployed personnel—83% identify this as a key driver. Supporting a widely dispersed customer base intensifies pressure to deliver expertise without constant on-site presence. Fabs, by contrast, view remote connectivity as an engine for innovation (56%), enabling faster experimentation, collaboration, and optimization. They also see it as a means of strengthening business continuity (44%), ensuring stable operations despite staffing shortages or regional disruptions.

In practice, remote connectivity is already producing measurable gains: faster troubleshooting prevents production delays, predictive maintenance safeguards yield and equipment effectiveness, and instant access to experts eliminates geographic bottlenecks. Together, these advantages improve availability, reduce costs, and support more resilient, scalable operations.

Differences: Key Drivers of Adoption



# What's Holding the Industry Back?

Adoption barriers and overall challenges

## Key Takeaways

- **Data / IP Protection** is the primary barrier to adoption
- **Security Concerns** ranked as the leading challenge
- **Resistance or delays due to internal policies or compliance requirements** emerged as the top security and access control challenge



# Primary Barriers to Adoption

80%

Data & IP Protection

67%

Cybersecurity Concerns

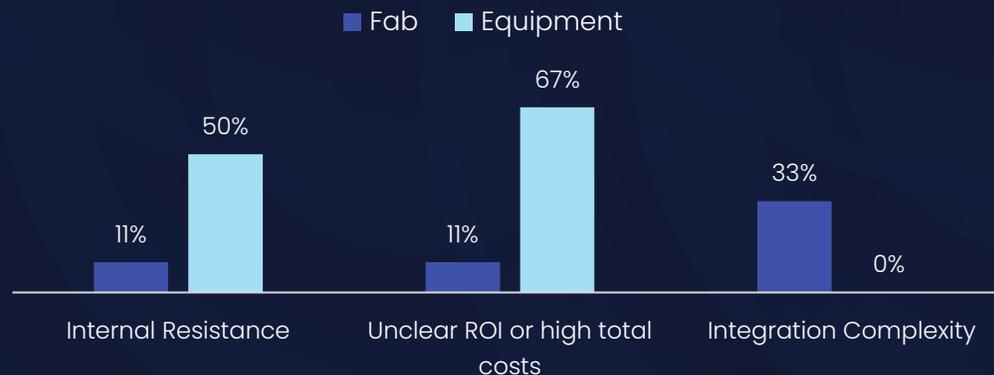
Despite strong demand, remote connectivity adoption faces significant technical and organizational obstacles. Data / IP protection and cybersecurity remain foremost concerns, cited by 80% and 67% of respondents, respectively. In a sector where IP defines competitive advantage, any perceived vulnerability carries serious risk and slows broader adoption.

Beyond these shared concerns, barriers differ by stakeholder group. Fabs report integration challenges (33%) because they operate multi-vendor environments where interoperability is essential. Equipment providers, however, report virtually no integration issues, as they focus on individual tools rather than large-scale system orchestration.

Equipment providers face their own internal hurdles: 50% cite internal resistance and 67% cite unclear ROI or high costs. These concerns reflect the need to justify investments in remote capabilities across diverse teams and customer environments, often before financial benefits are fully realized.

Collectively, these findings demonstrate that challenges are not purely technical—they are closely tied to organizational culture, governance, and strategic alignment. Moving forward will require addressing both security fundamentals and the social, financial, and operational structures that influence adoption.

Differences: Primary Barriers to Adoption



# Overall Challenges

## Security Concerns

**71%**

50% Inadequate access controls or user management  
50% Insufficient encryption or secure communication

## Audit & Compliance Gaps

**50%**

71% Resistance or delays due to internal policies or compliance requirements

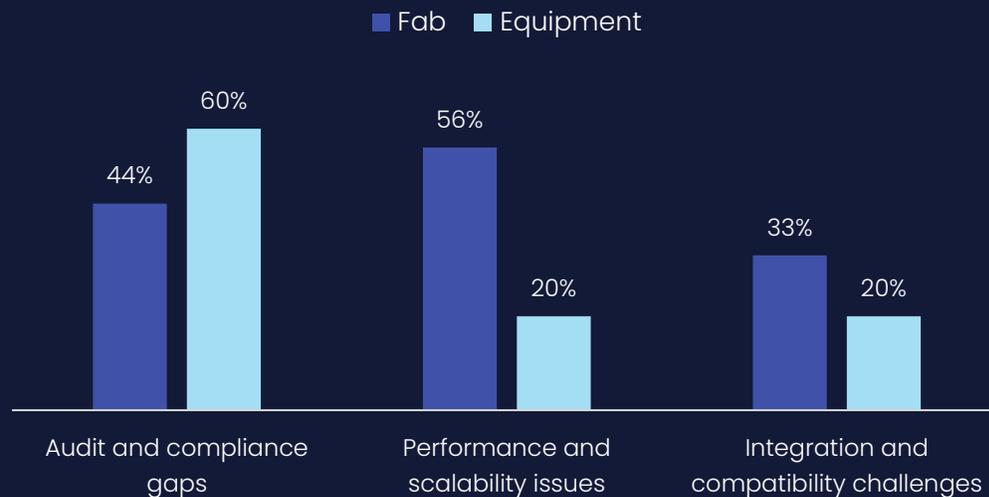
## Performance & Scale

**43%**

57% Latency & performance Issues

# Overall Challenges

Differences: Remote Connectivity Challenges



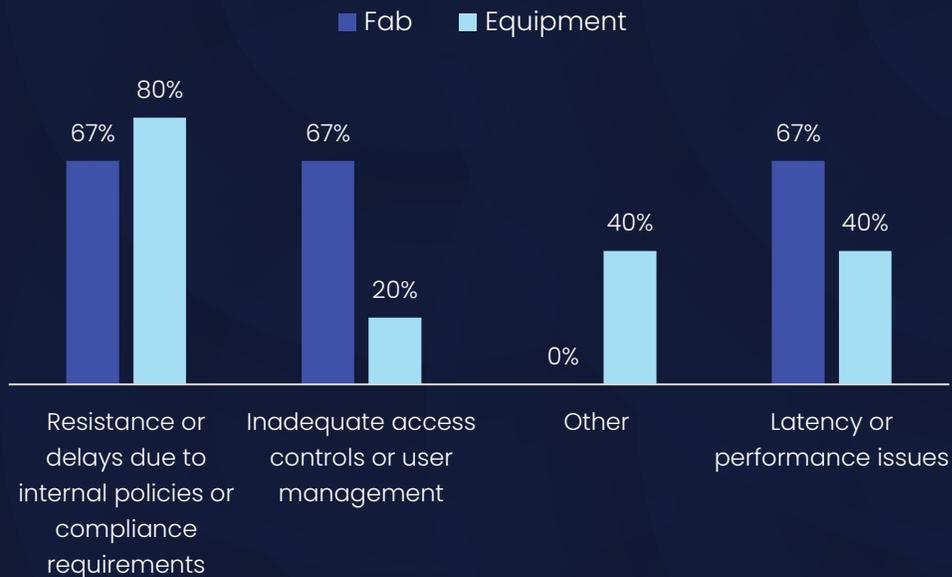
The broader challenges surrounding remote connectivity reflect differing roles and responsibilities across the ecosystem. Security remains the dominant concern (71%) followed by audit and compliance gaps (50%) and performance and scalability issues (43%).

Audit and compliance gaps pose a greater challenge for equipment providers (60%) than for fabs (44%), likely due to providers' need to meet diverse regulatory requirements across multiple customer environments. Also, 56% of fabs report performance and scalability issues while only 20% of equipment providers report the same. Integration and compatibility difficulties further highlight a divide, with 33% of fabs reporting challenges.

These distinct concerns underscore the need for aligned standards and governance. Without shared approaches to security, compliance, performance, and integration, the industry cannot fully realize the gains remote connectivity promises.

# Security, Access Control, & Performance Challenges

Differences: Security, Access Control,  
& Performance Challenges



Persistent security and performance issues continue to shape how companies implement remote connectivity. Overall, 71% cite resistance or delays due to internal policies or compliance requirements, 50% identify inadequate access controls or user management, and 50% note insufficient encryption or secure communication.

Fabs report significant challenges with access controls and user management (67%), reflecting the need for granular governance over who accesses sensitive systems. Equipment providers, meanwhile, struggle with internal policy delays (80%) and other roadblocks (40%), indicating that security issues extend beyond technology and into internal processes.

Performance limitations also affect implementation. Concerns about latency and responsiveness are reported by 67% of fabs and 40% of equipment providers. For fabs, performance issues can directly impact uptime. As innovation in equipment drives continuous data generation, platform performance for data handling must keep pace with rising volumes and complexity.

These challenges demonstrate that remote connectivity requires both technical excellence and organizational alignment. Secure governance, clear processes, and consistent performance standards are essential for trust and scalability.

# Looking Ahead

Future capabilities, emerging use cases, expected value, & future impact

## Key Takeaways

- **Reduced On-Site Support, Improved Equipment Uptime, and Increased Automation** tied as the expected value of future use cases
- **Security and Risk Management** is the leading anticipated future impact of remote connectivity
- **Increased Automation and AI-based Predictive Analytics** tied as needed future capabilities
- **AI-driven Root-Cause Analysis** is the leading emerging use case



# Future Capabilities

80%

Increased Automation

80%

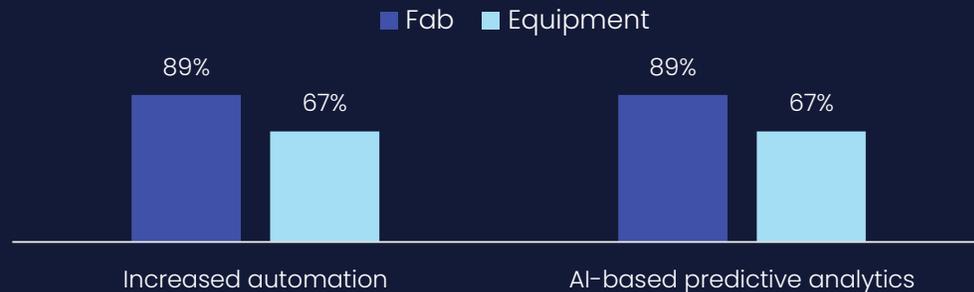
AI-based Predictive Analytics

As semiconductor manufacturing becomes more data-driven and interconnected, remote connectivity is transitioning into a platform for intelligent, self-optimizing operations. Companies increasingly view future remote capabilities as essential for enabling automation, AI-driven insights, and more proactive maintenance strategies.

Increased automation is a top expectation, cited by 89% of fab respondents and 67% of equipment providers. Automated detection, corrective action, and workflow optimization reduce the burden on scarce technical personnel and accelerate response times. AI-based predictive analytics are equally anticipated, with the same levels of interest, enabling better forecasting, planning, and continuous improvement across distributed sites.

Together, these capabilities signal a shift toward real-time, predictive, and autonomous manufacturing environments that minimize human error and maximize operational agility.

Differences:  
Needed Future Capabilities



# Emerging Use Cases

The next wave of remote connectivity applications is moving beyond traditional support and into areas that fundamentally reshape collaboration and decision-making.

AI-driven root-cause analysis, cited by 87% of respondents, is emerging as a powerful tool for identifying underlying process or equipment issues. By combining real-time data with historical patterns, it accelerates resolution and reduces disruption.

Real-time multi-vendor collaboration is especially important for fabs (56%), which must coordinate across heterogeneous toolsets. This capability enables seamless yet controlled sharing of diagnostics and insights between equipment providers and fabs, strengthening alignment and improving cross-system optimization.

These emerging applications illustrate a broader transformation toward intelligent, collaborative, and predictive operations across the semiconductor supply chain.

## Emerging Use Cases for Remote Connectivity Identified

**87%**

AI Driven Root Cause Analysis

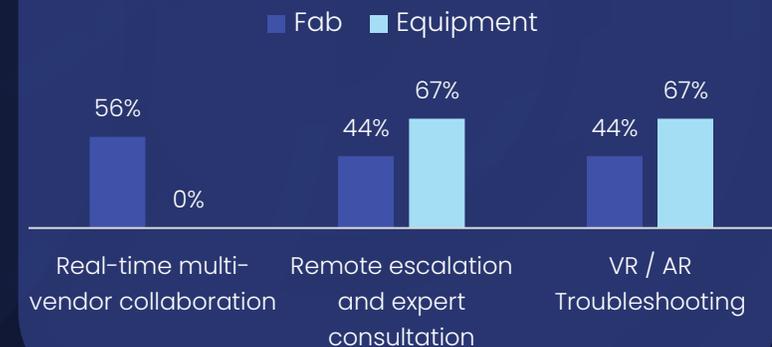
**60%**

Remote Process Calibration & Tuning

**53%**

VR / AR Troubleshooting

## Differences: Emerging Use Cases



# Expected Value

**87%**

Reduced on-site support,  
Improved equipment uptime,  
and Increased automation

**80%**

Smarter Predictive  
Maintenance

**60%**

Remote AI / ML-Driven  
Optimization

The advanced applications of remote connectivity deliver clear operational and strategic benefits. Companies expect significant reductions in on-site support (87% of respondents), as technologies like VR and AR enable remote troubleshooting and optimization, reducing travel expenses and deploying expertise more efficiently.

Improved equipment uptime (87%) is another major expected outcome, supported by predictive analytics and AI-enabled diagnostics that identify issues before they disrupt production. Increased automation, anticipated by 87% respondents, enhances consistency, decreases manual errors, and frees teams to focus on higher-value work.

Together, these benefits translate into lower operational costs, higher productivity, and more resilient manufacturing networks. As companies integrate automation, AI, and advanced remote capabilities, remote connectivity will continue evolving from a support tool into a strategic driver of next-generation operational performance.

## Anticipated Future Impact of Remote Connectivity

(1 = Low, 5 = High)

- 4.3 Operational efficiency
- 4.3 Security / risk management
- 3.8 Equipment lifecycle management
- 3.8 Collaboration between OEM and fab
- 3.7 Innovation and R&D

Respondents expect remote connectivity to reshape core business priorities across the semiconductor ecosystem, expanding its influence well beyond traditional operational support. Companies anticipate meaningful improvements in operational efficiency, stronger security and risk management frameworks, improved equipment lifecycle management, new avenues for innovation and R&D, and enhanced collaboration between fabs and equipment providers.

Security and risk management stands out as the highly anticipated future impact of remote connectivity (4.3), reflecting the sensitivity of data management and the operational consequences of any breach.

Operational efficiency remains one of the clearest areas of impact, with an overall rating of 4.3. Remote access drives faster problem resolution, more effective predictive maintenance, and improved equipment utilization, strengthening both operational efficiency and equipment lifecycle management.

Innovation and R&D are additional areas where remote connectivity is poised to play a larger role as industry players recognize that AI-enabled analytics, automated monitoring, and enhanced visibility into tool behavior can accelerate experimentation, process development, and yield improvement.

Collaboration also emerges as an important dimension of future impact. Remote connectivity between equipment providers and fabs is a way to deepen communication, share diagnostics in real time, and resolve issues leading to more efficient collaboration.

# Industry Preferences

Future deployment, standardized approach, & vendor considerations

## Key Takeaways

- **Hybrid** is the preferred future deployment model and a strong preference of an **independent third-party** industry standardized approach
- **Proven experience and security certifications** are the top vendor considerations while **failure to meet security and compliance expectations** is the top reason to switch vendors



# Future Deployment & Standardized Approach

**67%**

Hybrid is preferred future deployment model of remote connectivity

**53%**

Strong preference for third-party independent industry standards

Looking forward, the industry shows a clear preference for hybrid deployment models that combine remote access with on-site support. A majority of respondents (67%) favor this balanced approach, which maintains operational control and allows for hands-on intervention when necessary while still leveraging the speed, efficiency, and scalability of remote connectivity.

The strong shift toward hybrid deployment reflects a growing recognition that remote connectivity enhances rather than replaces on-site operations.

On standardization, the industry also shows a clear direction with 53% of respondents strongly preferring third-party independent industry standardized approaches, underscoring the need for consistent security protocols, access controls, data-sharing rules, and integration frameworks across the ecosystem.

Ultimately, harmonizing deployment models and standardization practices will be essential to unlocking the full value of remote connectivity across the semiconductor industry.

# Remote Connectivity Vendors: Considerations & Reasons to Switch

**73%**

Proven experience and security certification

**60%**

Significantly better support and service

**60%**

Current vendor fails to meet security and compliance expectations

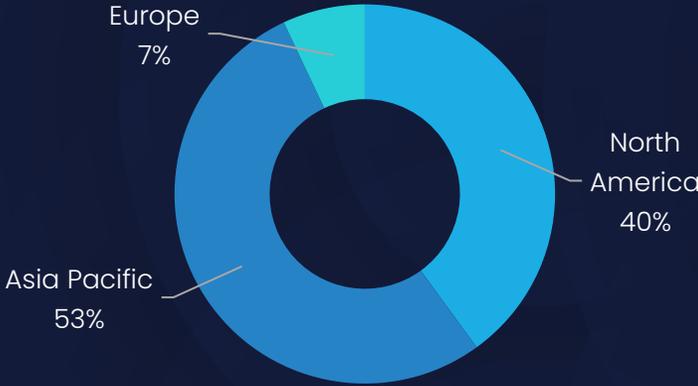
As remote connectivity becomes central to semiconductor manufacturing, vendor selection has evolved into a strategic decision. Companies are evaluating not just technical functionality but also the trustworthiness, security posture, and support capabilities of remote connectivity providers. Because downtime is costly and IP protection is paramount, the stakes of choosing the right partner are high. Increasingly, companies also consider whether vendors offer connectivity via hyperscaler platforms and the capabilities such platforms provide to support secure and reliable operations.

Respondents identify proven experience (73%) and security certifications (73%) as the most critical factors when selecting a vendor. Both indicate that a provider can implement reliable solutions and navigate complex fab environments.

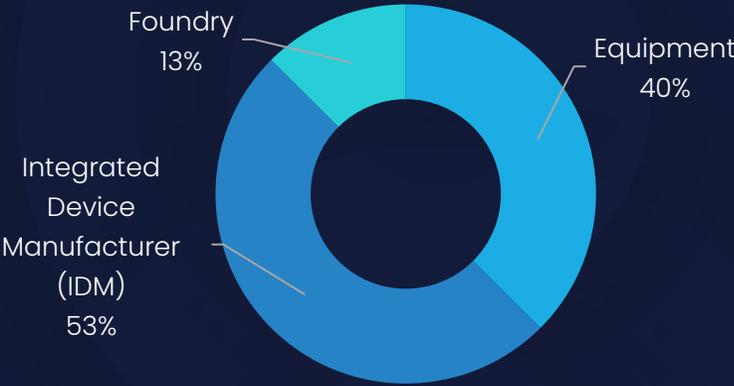
Similar themes appear in the reasons companies would switch providers. 60% would move to a vendor offering better support and service, highlighting that rapid, knowledgeable assistance is essential for minimizing downtime and maintaining stable operations. Another 60% would switch if their current vendor fails to meet security or compliance expectations - underscoring that vulnerabilities or weak governance are unacceptable in a sector where IP risk is existential.

# Appendix: Respondent Profile

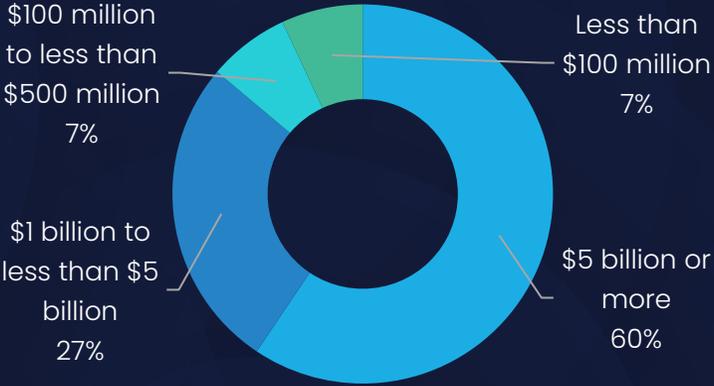
Headquarters Region



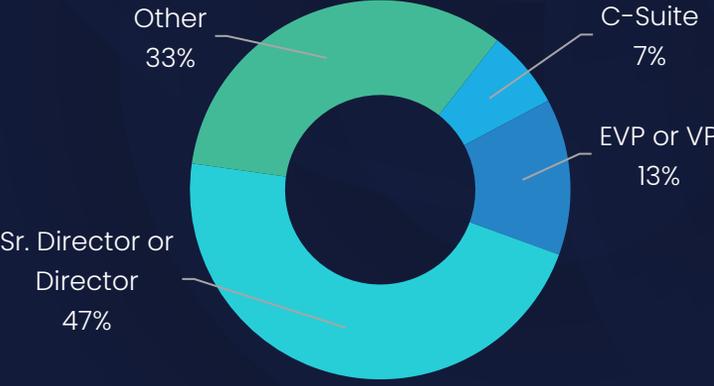
Role in Semiconductor Ecosystem



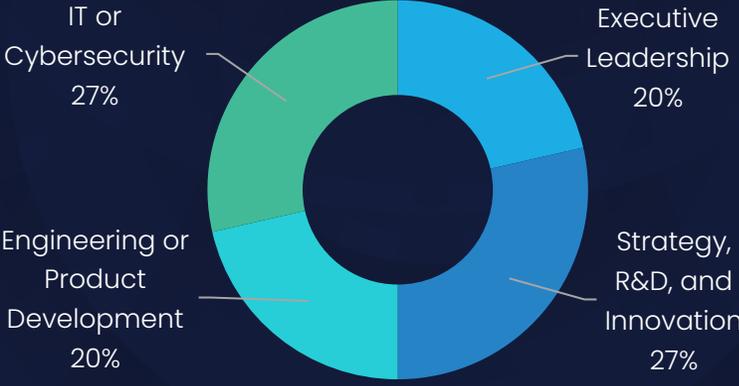
Organization's Annual Revenue Range USD



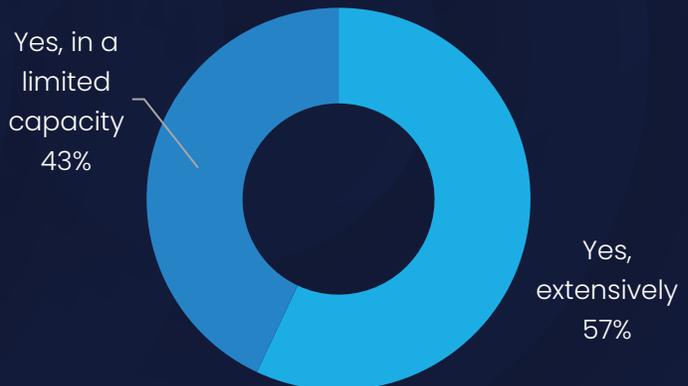
Current Job Title



Current Department / Function



Current Use of Remote Connectivity



# Contact Us

For more information, please  
contact report contributors:

**Traces by Capgemini**  
[traces.nl@capgemini.com](mailto:traces.nl@capgemini.com)

**Theo van Roekel**  
Managing Director  
[theo.van.roekel@capgemini.com](mailto:theo.van.roekel@capgemini.com)

**GSA Resources**  
[resources@gsaglobal.org](mailto:resources@gsaglobal.org)

**Jessica Mueller**  
Vice President, Products & Services  
[jmueller@gsaglobal.org](mailto:jmueller@gsaglobal.org)



### **About Capgemini**

Capgemini is an AI-powered global business and technology transformation partner, delivering tangible business value. We imagine the future of organizations and make it real with AI, technology and people. With our strong heritage of nearly 60 years, we are a responsible and diverse group of 420,000 team members in more than 50 countries. We deliver end-to-end services and solutions with our deep industry expertise and strong partner ecosystem, leveraging our capabilities across strategy, technology, design, engineering and business operations. The Group reported 2024 global revenues of €22.1 billion.

Make it real.

[Traces Semiconductors - Capgemini](#)

### **About GSA**

GSA is *Where Leaders Meet* to establish an efficient, profitable, and sustainable high technology global ecosystem encompassing semiconductors, software, solutions, systems, and services. A leading industry organization that represents 300 corporate members, including 122 public companies, GSA provides a unique, neutral platform for collaboration, where global executives interface and innovate with peers, partners, and customers to accelerate industry growth and maximize return on invested and intellectual capital. Members of the GSA represent 84% of the \$662 billion semiconductor industry and continue to grow.

For more information, visit [www.gsaglobal.org](http://www.gsaglobal.org). Follow GSA on [LinkedIn](#), [Facebook](#), [Instagram](#), [Twitter](#), [YouTube](#) and [WeChat](#).

