July 2025 | InfoBrief, sponsored by Imprivata

Manufacturing's Digital Transformation Dilemma

Ensuring Secure Access Without Sacrificing Operational Excellence

Reid Paquin
Research Vice President,
Future of Operations, IDC

Simon Ellis
Group Vice President,
Manufacturing and Worldwide Supply Chain, IDC

Table of Contents

CLICK BELOW TO NAVIGATE TO EACH SECTION IN THIS DOCUMENT.

In This InfoBrief

The importance of embracing digital technology has been accepted across all industries, particularly the manufacturing industry. Most companies realize that refusing to adapt to the digital age will result in their peers leaving them behind. While digitization efforts have unquestionably brought numerous benefits to the efficiency/performance of plant floors, it has also resulted in rising levels of cyber vulnerability. Failure to safeguard the industrial network puts a company at risk of expensive and time-consuming downtime, costs, and damages.

Manufacturers must figure out how to achieve their Industry 4.0 goals securely. Security measures tailored specifically for industrial environments are imperative for keeping operations protected, efficient, and profitable.

This InfoBrief, comprised of recent IDC industry sentiment studies, highlights the growing importance for manufacturers to implement a comprehensive security strategy focused on providing frontline workers with seamless and secure access to the resources (e.g., data, devices, and applications) they need.

Digitization Creates New Opportunities

- **Manufacturers continue to face constant disruptions, geopolitical restrictions, and ever-changing workforce challenges.** At the same time, traditional pressures around cost, efficiency, and quality are always present on the manufacturing agenda.
- This is resulting in **factories being relied upon to handle more complex operations and serve a wider range of products with faster throughput and smaller lots/batches** while trying to minimize costs.
- Competing in this dynamic environment has led many manufacturers to rethink fundamental aspects of their operations, and **many have realized that a digital-first strategy is critical to success.**
- **By investing in digital technologies, manufacturers have seen improvements in operational efficiency, resiliency, and customer satisfaction.** In addition, the most mature digital manufacturers are now able to optimize their supply chains and explore new revenue streams.
- This focus on data-driven operations is still top of mind across the industry. In fact, **manufacturers expect their amount of operational data generated to increase by over 21%** over the next 12 months.
- While this new era of connectivity can bring many benefits, **it also results in rising levels of cyber vulnerability** for manufacturers.

Top operational priorities over the next 12 months:

45%
Reducing/ cutting costs

40%
Improving employee productivity

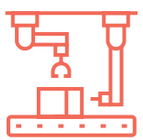
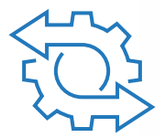
39%
Ensuring product quality

35%
Improving asset productivity/reliability

Source: IDC's *Future of Operations Survey*, August 2024

The Impact of Security Incidents for Manufacturing

The number of security attacks and their impact continue to rise, with industrial segments in particular experiencing attacks at growing rates.

- Over the past 12 months  **57%** of manufacturers experienced a ransomware attack/breach **versus**  **49%** across all industries.
- In addition, roughly 30% of those manufacturing organizations paid a ransom to regain access to their systems/data at an average cost of over **$175,000**.
- The potential impact of a single successful cyberattack goes beyond any ransom paid. Incidents can also include data loss, IP theft, brand tarnishing, and loss of customers.
- For manufacturing, the disruption to operations is the biggest concern. Recent IDC studies have shown the cost of one hour of unplanned downtime to be over **$125,000**.

Continue reading

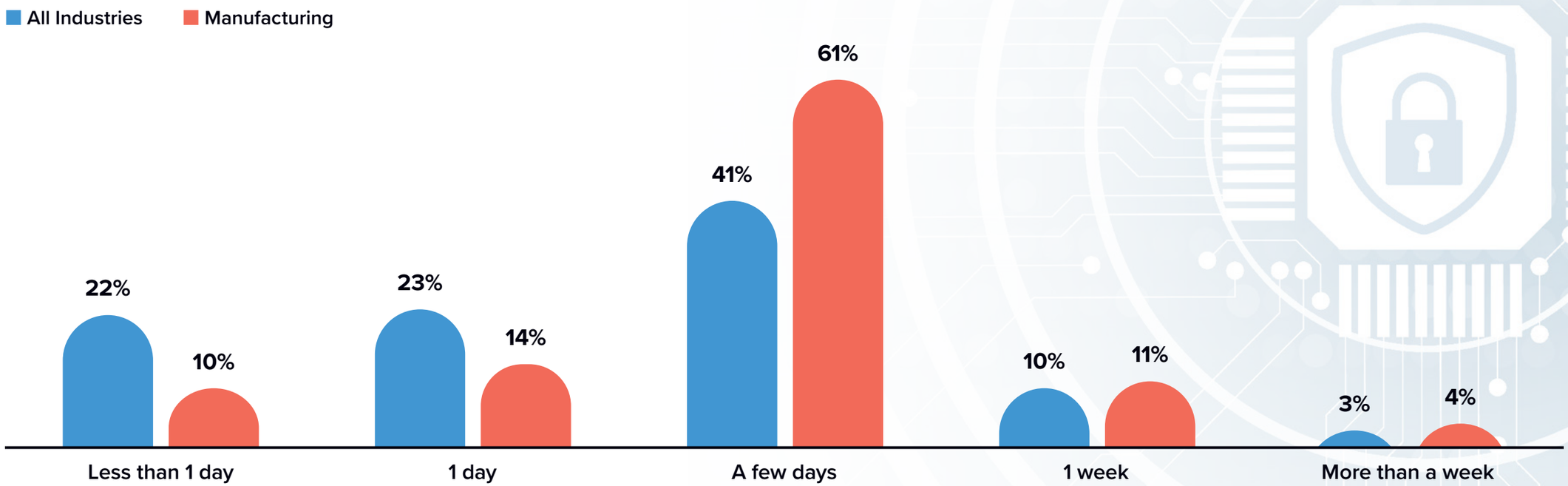
n = 720 (All Industries), n = 127 (Manufacturing); Source: IDC's *Future Enterprise Resiliency and Spending Study,* October 2024

The Impact of Security Incidents for Manufacturing (continued)

Manufacturing experiences longer business disruption than the industry average.

For your most recent security incident, how long was business disrupted?

(Percentage of respondents)



n = 720 (All Industries), n = 127 (Manufacturing); Source: IDC's *Future Enterprise Resiliency and Spending Study,* October 2024 | For an accessible version of the data on this page, see Supplemental Data in the Appendix.

IT/OT Convergence Is Where It Comes to a Head

Top Barriers for IT/OT Convergence in Manufacturing

Concerns about the security of integrating IT and OT systems

Lack of staffing capacity or expertise on how to accomplish integration

Technology issues/lack of compatibility with legacy applications

Lack of industry standards or adoption of standards

Not enough familiarity with the concept of IT/OT integration across the organization

- **The goal of IT/OT convergence is to integrate the tools a manufacturer uses to collect data with the tools it uses to control operations,** allowing operations to use more sources of real-time data to make better decisions.
- Historically, **manufacturers have viewed security as more of an afterthought,** especially in the OT environment.
- Enterprise Access Management solutions can bridge this divide by **securing access across legacy OT and modern IT systems.**
- **Connecting these legacy assets to the internet** or other public networks **exposes industrial automation systems and field-level devices to vulnerabilities** and/or threats.
- Ultimately, manufacturers find themselves in a dilemma — **digitization is essential to compete but also opens more avenues for cybercriminals** to attack.

n = 1,051; Source: IDC's *IT/OT Convergence Study,* August 2024

Legacy Systems and the Shift to Hybrid Environments

- Many manufacturers tend to rely on a mix of plants, assets, and technology systems that are aging and limited in functionality.

  Roughly 50%
  of manufacturers stated the average age of their OT assets is 15 years or more.

- This situation results in information being difficult to access/analyze, hindering the ability to make the most effective decisions in the necessary time frame.

  Only 30%
  of manufacturers reported the ability to provide front-line employees with real-time operational data.

- The industry's continued shift away from legacy, on-premises systems to the cloud has become a clear goal for modernization efforts. However, it is not realistic for manufacturers to rip and replace all these systems; they must be factored in when planning a security strategy.

  The majority of manufacturers have a policy of moving significant amounts of operational data to the cloud. → **51%**

- The adoption and scale of the cloud usage have become key indicators for how effectively an organization can leverage operational data to drive decision-making.

  Leaders in manufacturing are roughly three times more likely to do this than followers.

- The expanded use of cloud has helped with data accessibility/sharing initiatives but also makes securing this hybrid environment more complex for manufacturers.

  Seamless integration/authentication for legacy on-premises and cloud-based applications is required.

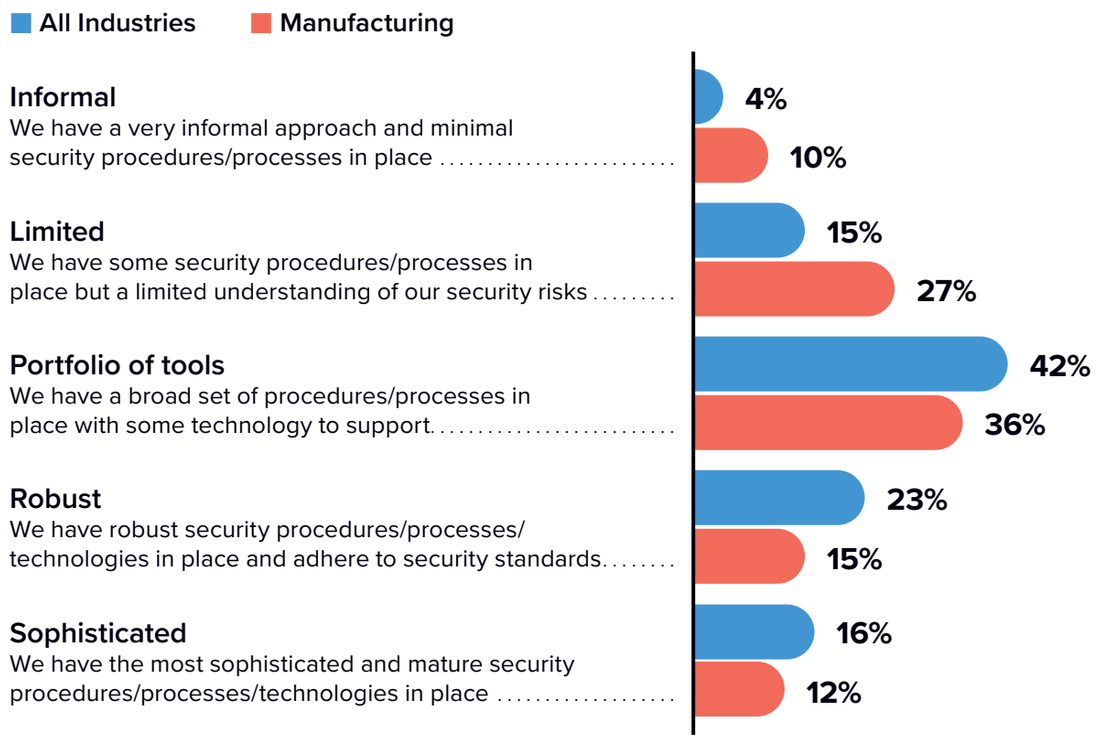
n = 1,051; Source: IDC's *IT/OT Convergence Study,* August 2024. n = 864; Source: IDC's *Future of Operations Survey,* July 2024

Security Maturity, Expertise, and Conflicting Priorities

- A large factor behind the industry's security woes is the maturity (or lack thereof) of cybersecurity programs.
- These problems are heightened by the growing manufacturing skills gap, and most companies lack security expertise.
- There have also been conflicting priorities between the IT and Ops teams themselves.
- IT's top focus is to ensure the confidentiality and integrity of data, making cybersecurity paramount.
- Frontline workers, on the other hand, are tasked with achieving operational excellence goals.

Which of these statements best describes your organization's approach to cybersecurity?

(Percentage of respondents)



n = 720 (All Industries), n = 127 (Manufacturing); Source: IDC's *Future Enterprise Resiliency and Spending Study,* October 2024 | For an accessible version of the data on this page, see Supplemental Data in the Appendix.

Building a Culture and Foundation for Security

Successful manufacturers are more likely than their peers to do the following:

- Establish cross-functional teams responsible for developing an Industry 4.0 road map that balances security, operational performance, and corporate goals.
- Establish and enforce standardized security policies and network access.
- Utilize a formal escalation process for critical network performance or security issues.
- Establish a center of excellence responsible for capturing and promoting best practices for operational security across the enterprise.
- Put a formal process in place for updating systems/patch management (traditionally a big gap on the shop floor).
- Regularly review and evaluate the security policies in place. Security is a dynamic process that must be adapted as necessary.

It is important to realize that operational security is complicated. There is no silver bullet to ensuring the security of all the elements in a manufacturing facility.

Enabling Productivity While Maintaining Security

- Balancing **security and productivity can be a challenge** for most manufacturers.
- **If operational groups view corporate IT guidelines as unnecessary roadblocks to getting their jobs done,** they will be resistant to implementation or try to find ways around policies altogether.
- **Mobile devices allow for data access** no matter the location and faster decision-making, **but they also represent new touch points for security threats** to manage.
- **Frontline workers typically utilize shared workstations.** Ensuring secure and seamless connections to all devices is essential.
  - Leading manufacturers are **58% more likely than their peers to utilize user and device authentication solutions.**
- In addition, IDC's *2024 Manufacturing Talent Study* highlighted **digital literacy as one of the top skill sets most lacking among frontline workers.** The ease of use for security solutions cannot be overlooked.
- The industry expertise of technology partners is also important to consider. **Being able to access offline systems and understand operational workflows is necessary to achieve security** without disrupting frontline workers.
- Having **solutions designed specifically for manufacturing** results in a system requiring less configuration/customization to implement and a more effective system overall.

Top objectives for IT/OT security investments:

37%
Improving operational reliability

30%
Maximizing employee productivity/safety

25%
Mitigating risk

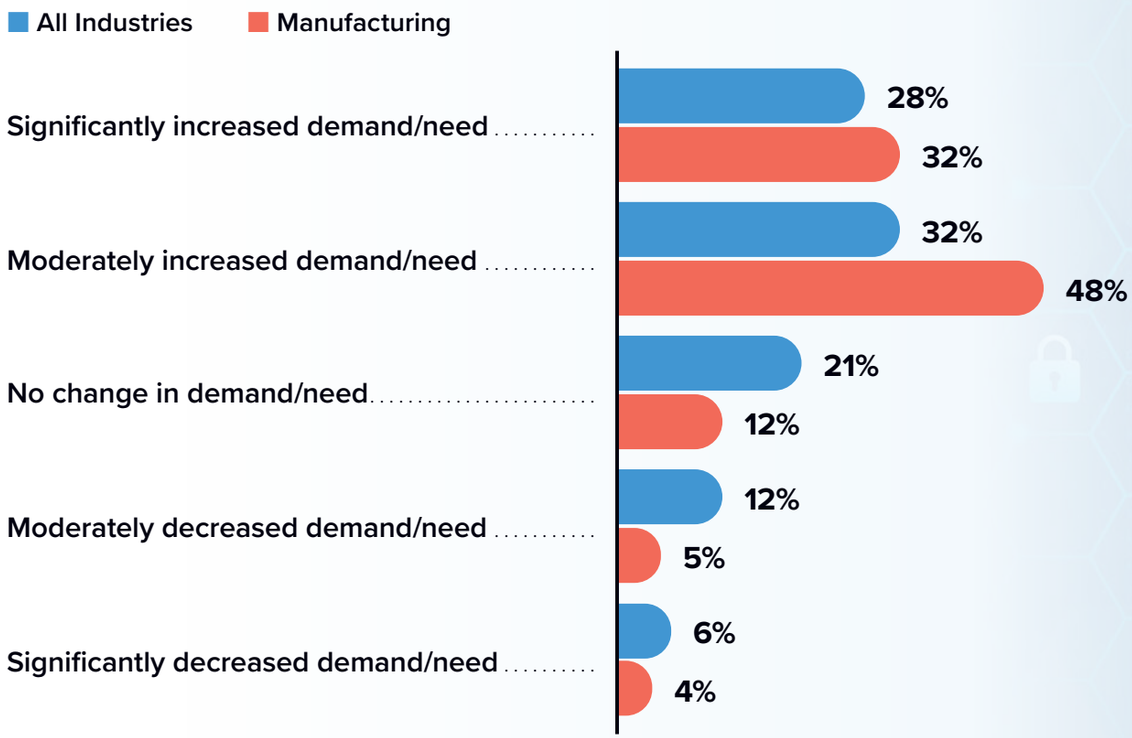
17%
Ensuring compliance with regulations/standards

Source: IDC's *IT/OT Convergence Study,* August 2024

The Use of Technology to Ensure Security

Change in Demand for Identity and Access Management Solutions

(Percentage of respondents)



- Identity and access management systems help identify, authenticate, and control access for anyone who will be utilizing manufacturing devices/applications.
- Ensuring that the right users have the appropriate access to manufacturing systems is an identified need across manufacturing.
- Investment in technology to help manufacturers manage security will only rise over time.

n = 889 (All Industries), n = 143 (Manufacturing), Source: IDC's *Future Enterprise Resiliency and Spending Study (Wave 11)*, December 2024 | For an accessible version of the data on this page, see Supplemental Data in the Appendix.

Enterprise Access Management in Manufacturing

- **Enterprise access management is a system/solution that controls and monitors how users access enterprise resources and data.**
- Given the shared environment of manufacturing operations and increased reliance on shared mobile devices, **providing frontline workers access to shared resources with a single set of credentials (unique to the individual) improves the user experience and saves time, all while maintaining security.**
- **Increased usage of remote access** across manufacturing makes solutions that can **provide multifactor authentication** important.
- These access management tools typically **allow for better assignment/management of permissions,** ensuring users have the appropriate access level.

- In addition, the use of role-based access control will allow manufacturers to be **more targeted in the access they grant, as they will be able to base it on a user's role/responsibilities.**
- For manufacturers facing regulatory requirements (e.g., CMCC certification) related to security, **having a solution to control and monitor access to sensitive information is needed to maintain compliance.**
- It is also important to think outside the "four walls" when it comes to the enterprise. **Most manufacturers work with a network of suppliers, contractors, or partners that can all benefit from accessing systems.**

32%
of manufacturers cited **"managing contractors and third parties with access to our facilities and assets"** as a growing security challenge.

n = 1,051; Source: IDC's *IT/OT Convergence Study,* August 2024

Essential Guidance

Security can no longer be an afterthought; the potential impact of a single incident is too great.

Accept that industrial security is complicated and that complex problems require comprehensive solutions.

Enabling frontline worker productivity while maintaining security will be key for manufacturers to achieve their long-term goals.

Manufacturers need to address the user experience, shared workstation/mobile access, and the integration of legacy and modern apps.

Think outside the four walls. Third parties, including partners, contractors, and external vendors, must be factored in as potential users requiring access.

Enterprise access management can provide manufacturing workers with seamless and secure access to shared devices/workstations and data on legacy and modern applications.

Security solutions tailored specifically for industrial environments are imperative for keeping operations protected and profitable.

Appendix: Supplemental Data

The table in this appendix provides an accessible version of the data for the complex figures in this document. Click "Return to original figure" below the tables to get back to the original data figures.

SUPPLEMENTAL DATA FROM PAGE 6

For your most recent security incident, how long was business disrupted?

	Less than 1 day	1 day	A few days	1 week	More than a week
All Industries	22%	23%	41%	10%	3%
Manufacturing	10%	14%	61%	11%	4%

n = 720 (All Industries), n= 127 (Manufacturing); Source: IDC's *Future Enterprise Resiliency and Spending Study,* October 2024

Return to original figure

Appendix: Supplemental Data (continued)

SUPPLEMENTAL DATA FROM PAGE 9

Which of these statements best describes your organization's approach to cybersecurity?

	Informal: We have a very informal approach and minimal security procedures/processes in place.	**Limited:** We have some security procedures/ processes in place but a limited understanding of our security risks.	**Portfolio of tools:** We have a broad set of procedures/processes in place with some technology to support.	**Robust:** We have robust security procedures/ processes/technologies in place and adhere to security standards.	**Sophisticated:** We have the most sophisticated and mature security procedures/ processes/technologies in place.
All Industries	4%	15%	42%	23%	16%
Manufacturing	10%	27%	36%	15%	12%

n = 720 (All Industries), n = 127 (Manufacturing); Source: IDC's *Future Enterprise Resiliency and Spending Study,* October 2024

Return to original figure

SUPPLEMENTAL DATA FROM PAGE 12

Change in Demand for Identity and Access Management Solutions

	Significantly increased demand/need	Moderately increased demand/need	No change in demand/need	Moderately decreased demand/need	Significantly decreased demand/need
All Industries	28%	32%	21%	12%	6%
Manufacturing	32%	48%	12%	5%	4%

n = 889 (All Industries), n = 143 (Manufacturing), Source: IDC's *Future Enterprise Resiliency and Spending Study (Wave 11),* December 2024

Return to original figure

About the IDC Analysts

Reid Paquin
Research Vice President,
Future of Operations, IDC

Reid Paquin is responsible for IDC's Future of Operations program. The program focuses on how operations will need to continually evolve to respond to rapid change and disruption. Traditional pressures (e.g., costs and efficiency) will always be present, but additional factors (e.g., increased customization and resiliency) are causing many to rethink operations. The goal of the program is to deliver thought leadership, strategic guidance, and best practices to organizations impacted by the growth of data-driven operations and how to become future enterprises able to meet the needs of the digital economy.

More about Reid Paquin

Simon Ellis
Group Vice President,
Manufacturing and Worldwide Supply Chain, IDC

As Group Vice President, Simon Ellis currently leads the U.S. Manufacturing Insights, U.S. Energy Insights, and Global Supply Chain Strategies practices at IDC, specializing in advising clients on manufacturing/energy strategies, supply chain digital transformation, sustainability, cloud migration, network, and ecosystem design. Ellis works with end-user companies, supply chain organizations, and technology providers to develop best practices and strategies leveraging IDC quantitative and qualitative data sets. Within the supply chain practices, Ellis contributes extensively to the Supply Chain Planning and Multi-Enterprise Networks Strategies practice while also overseeing the Supply Chain Execution practices.

More about Simon Ellis

Message from the Sponsor

Imprivata solutions provide all users with simple and secure access to the devices, applications, and other resources they need to do their jobs efficiently and effectively.

The company's portfolio of solutions includes single sign-on, multifactor authentication, shared mobile device access management, analytics, and privileged access management for IT admins, vendors, and other third parties requiring network access. Imprivata solves access, security, and auditing challenges associated with shared workstations and mobile devices while providing real-time analytics to drive actionable insights. Together, these capabilities provide both the security organizations need and the task-based efficiency users require to drive productivity and ensure that every second of critical work is both frictionless and secure.

For more information, visit the Imprivata Website or Contact Us

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com @idc @idc