White Paper

Bridging the Gap Between Endpoint Security and Network Security with Secure Browsers

Sponsored by: Citrix

Pete Finalle Mike Jude Christopher Rodriguez

August 2025

IDC OPINION

The protection of sprawling IT environments is a consistent challenge for cybersecurity professionals. Efforts often fall into the trap of operating in disparate, specialized practice areas, leading to security gaps. In the case of facilitating access to resources and applications, enterprises operate an array of tools and practices that lack complete coverage and complicate the attack surface. Enterprises rely on endpoint protection, identity and access management, virtual private networks (VPNs), and zero trust network access (ZTNA), along with an array of threat-sensing technologies. As threats evolve and attackers continue probing for weaknesses in defenses, these technologies should function in a more integrated fashion. Ideally, secure application access should initiate at the endpoint and provide full coverage across the modern IT network. However, each area currently operates in a security silo and faces unique technical challenges.

Many approaches to securing the endpoint have been adopted, ranging from antivirus and antimalware to more extensive approaches such as identity management and device management. However, most of these approaches only address specific threat vectors and ignore the fact that many breaches are self-inflicted and come not from deficiencies in endpoint architectures but from the end users themselves or from stolen credentials.

August 2025, IDC #US53733925

There are several approaches to securing how users access apps and resources within the broader enterprise ecosystem in a more comprehensive way. These include virtual desktop infrastructure (VDI), zero trust network architecture, and virtual private networks. Each has advantages, but each also presents challenges:

- VDI provides a complete virtual desktop environment, which is often overkill for simply facilitating access to applications and resources and is often costly and inflexible.
- ZTNA solutions provide continuous authentication and enhanced security, at the expense of support for proprietary applications, which may be essential for adopting organizations.
- VPNs are the simplest technology to deploy and manage, with vast support for applications and resources, but lack security features and capabilities.

Ultimately, all these approaches should coexist with the increasing use of secure service edge (SSE) technologies. Yet, SSE is hard to do, and the challenge is adopting technologies that advance efforts to achieve approaches like SSE and zero trust. However, despite the promising expansion of SSE, buyers face challenges in achieving complete adoption. The effectiveness of SSE is not solely determined by the number of features and capabilities deployed; equally crucial are the percentage of the workforce covered and the percentage of applications supported. These factors play a pivotal role in ensuring comprehensive security and operational efficiency, highlighting the complexity and multifaceted nature of adopting SSE solutions.

With the proliferation of SaaS and web-based applications, most of the work is done by employees, contractors, and vendors using a web browser. However, the web browser is also a top attack vector for security threats and data breaches, particularly on unmanaged devices where traditional defenses, such as EDR, SWG, and network-based security tools, are either not present or ineffective for protecting against browser-based attacks. With the move toward supporting workers to be productive using their own devices, it is important to enforce security controls and achieve governance on unmanaged devices to safeguard data without compromising productivity or user experience. In addition, organizations also need to protect the movement of corporate data accessed via web browser–based applications outside of the corporate environment on unmanaged devices without securing the browser itself.

An ideal approach for many organizations is to deploy an enterprise browser solution that can enable organizations to deliver secure work by leveraging enterprise browsers to access modern web and SaaS applications while leveraging the benefits of VDI technology for legacy applications as well as ZTNA-based technologies for client/service applications as part of unified security architecture.

Enterprise browsers are becoming critical components of security strategies, fundamentally reshaping security through integrated protections. Secure enterprise browsers direct traffic to secure control points in the cloud as needed and can implement web security right on the user device. Advanced capabilities include isolating high-risk activities in secure containers or analyzing traffic for threats without need for decryption.

Yet, enterprise browsers, too, have had issues coexisting with enterprise computing architectures that depend heavily on proprietary applications. While enterprise browsers have gained popularity for their powerful controls, potential buyers find themselves questioning their ability to implement enterprise browsers within their unique IT environments and complex security architecture. What is needed is an approach that marries the virtues of the enterprise browser with the control and management capabilities of a VDI approach and that also provides a path to a zero trust environment and simplifies the admin experience with an integrated management console, consistent policy control, and unified observability across the different application access methods.

SITUATION OVERVIEW

The endpoint protection market is being driven by several dynamics, not the least of which are rapidly changing market dynamics, the cybersecurity challenges being faced by enterprises, and business drivers that can include not only revenue generation and cost but also the need to address new regulatory environments. These are briefly discussed in the sections that follow.

Market Dynamics

As a result of the increasing concern over the potential for cyberthreats arising from the user environment, approaches such as enterprise browser implementation are on the rise. Enterprise browser adoption, specifically, is on a significant upward trajectory, with expectations to reach 52% by 2025, a substantial increase from 22% in 2023. This growth reflects the increasing reliance on secure and efficient browsing solutions within corporate environments. Likewise, 79% of organizations are planning to implement secure service edge within the next 24 months, while ZTNA is also experiencing rapid growth, valued at $1.9 billion in 2024 and projected to reach $4.1 billion by 2029, according to the IDC Security Tracker for the second half of 2024.

Current Enterprise Challenges

Despite the promising growth projections, organizations today face significant challenges adopting comprehensive endpoint protection technology due mainly to fragmented security tools and multiple solutions, which often lead to security gaps and

inconsistent user experiences. This fragmentation is exacerbated by the difficulty in managing policies across multicloud environments; in many cases requiring duplication of infrastructure to obtain complete coverage across the entire application ecosystem. The complexity of IT infrastructure management, with its interconnected systems, further complicates the security landscape. As security threats continue to rise, they increasingly exploit the complexity inherent in distributed networks, making it imperative for organizations to streamline their security strategies and tools to ensure comprehensive protection.

Moreover, the deployment of SSE and zero trust solutions is a complex and lengthy process, with buyers struggling to achieve a robust security posture. This struggle includes applying consistent data protection and threat detections universally across all devices and use cases, avoiding performance bottlenecks and technical challenges that hinder user productivity and reducing false positives until complete adoption is realized. Key trade-offs regarding the security of encrypted traffic also pose challenges, as organizations must decide between accepting blind spots or opting for decryption in the cloud. In addition, application support is often inconsistent, further complicating the deployment and management of security solutions. These challenges highlight the need for a cohesive approach to security that addresses the intricacies of modern IT environments and the evolving threat landscape.

Business Drivers

Secure access enables productivity and business outcomes. The growing need for secure remote work solutions has become a critical business driver, as organizations strive to protect their distributed workforce while optimizing costs and resources through the consolidation of security agents. In addition, in today's rapidly evolving digital landscape, businesses are increasingly driven by the need for simplified security management and reduced complexity. According to IDC's March 2025 *SASE Buyer Insights Survey,* 74% of respondents emphasized the importance of having their SSE or secure access service edge (SASE) solutions provided by a single vendor for all components, marking an 11% increase from 2024. This trend underscores the demand for streamlined security solutions that minimize complexity and enhance efficiency.

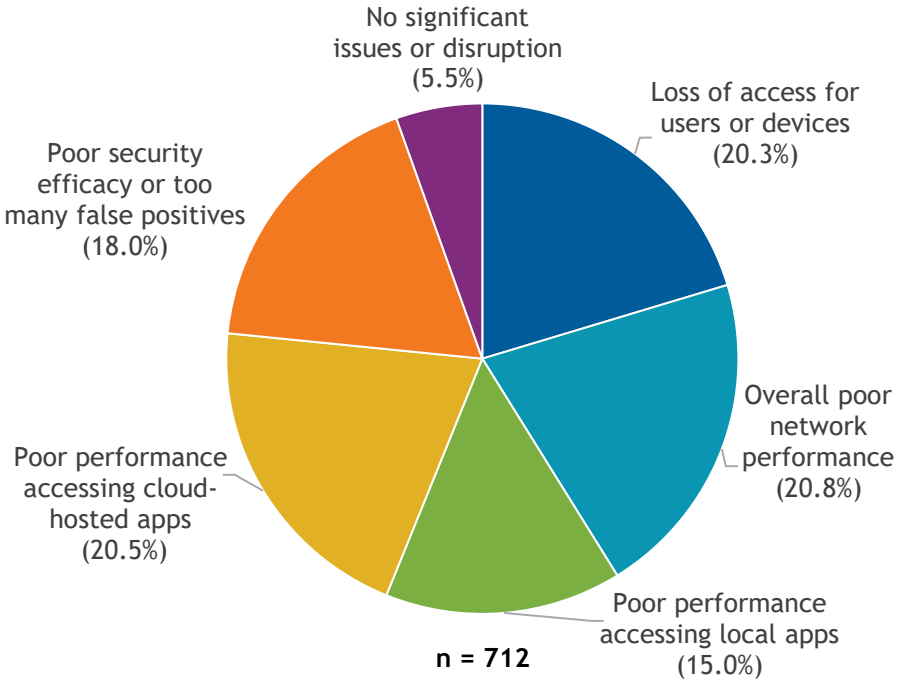
Furthermore, businesses are focused on addressing compliance and data protection requirements, seeking a fast path to adopting essential SSE capabilities that ensure consistent security across the enterprise. The flexibility to quickly respond to zero-day threats and extend security solutions to partner or contractor BYO devices is paramount, especially when an SSE agent-based approach is not feasible. This necessitates a robust and adaptable security framework that can seamlessly integrate with existing systems and provide comprehensive protection. As organizations navigate these challenges, the emphasis on cost optimization, resource efficiency, and the ability

to swiftly adapt to emerging threats remains central to their strategic objectives. In addition, SSE/SASE adoption is a complicated journey for buyers deploying a traditional solution from their firewall, cloud security, or SD-WAN vendor of choice. This can result in growing pains in the form of issues and disruptions that can impact access for users and devices, network performance, security efficacy, and others, which can negatively impact productivity. With only 5% of buyers experiencing no significant issues and disruptions, the SSE/SASE market would greatly benefit from increased simplicity, integration, and built in support out of the box. By reducing complexity of functionality, management, and deployment, SSE/SASE solutions will enable buyers to achieve desired security outcomes quicker, and with fewer disruptions to business operations along the way (see Figure 1).

FIGURE 1

Complexity Disrupts Functionality

Q. What issues/disruption of services has your organization encountered since deploying an SSE/SASE?



Note: 47% of SSE/SASE buyers indicated that complexities with security policies created issues or disruptions with their vendor's solution.

Source: IDC's *SSE/SASE Buyer Adoption Survey,* March 2025

Citrix Secure Private Access Integrated with Google Chrome Enterprise Premium

Holistic secure access requires a breadth of network security controls working in tandem with endpoint protections — starting with device/user environments. One approach to reducing the complexity associated with securing the user environment is to employ a secure browser that integrates the operating environment with the browser itself. Such an approach addresses the difficulty that often exists with VDI solutions that need to accommodate proprietary enterprise applications. An example of this approach is Citrix's integration of its Secure Private Access, a ZTNA solution, with Google's Chrome Enterprise browser, which delivers many of the SSE capabilities organizations need.

The integration of Citrix Secure Private Access with Google Chrome Enterprise Premium offers significant security enhancements that cater to modern enterprise needs. Citrix Secure Private Access provides granular contextual access, allowing organizations to secure access to internal web and SaaS applications based on zero trust principles, ensuring that interactions are limited to only authorized users that have been verified with strong authentication methods and constrained to only the resources required. This is done without the need for traditional VPNs, thereby addressing issues like agent sprawl, fragmented access control, and performance bottlenecks while streamlining connectivity and reducing potential vulnerabilities. Leveraging additional Citrix security solutions provides further options for enhancing security (such as RBI or WAF) or addressing specialized use cases (e.g., legacy applications).

Google's data loss prevention and web security capabilities latent in Google Chrome Enterprise Premium offers an additional layer of protection. Advanced security features such as anti-keylogging, anti-screen scraping protection, and multifactor authentication support ensure comprehensive safeguarding against potential threats. The combination of Google Chrome Enterprise Premium and Citrix Secure Private Access enables holistic data protection, allowing organizations to detect threats and sensitive data on the device, thereby preventing the need for decryption.

Operational efficiency is improved through the seamless integration with Citrix Workspace, which enhances overall user experience and productivity. Automatic Citrix Cloud redirection upon log in, combined with contextual routing through hybrid data routing to the optimal resource location, ensures users are directed to the appropriate resources without manual intervention while Google's acceleration capabilities boost performance. While utilizing Google's network infrastructure, unified management is achieved through the Citrix admin console to provide centralized control. By

consolidating security tools into a unified system, complexity is reduced, enabling streamlined operations and management.

Reduced costs are a key advantage of this integration, as it eliminates the need for multiple vendor contracts, thereby streamlining procurement processes. Organizations can balance cost and risk by reducing duplicate security infrastructure, leading to more efficient resource allocation. Expenses related to VDI are lowered, and resource utilization is improved through a unified agent approach. The simplification of IT infrastructure contributes to cost efficiency, while the Citrix platform license offers a comprehensive solution portfolio, including enterprise browser, ZTNA, and VDI-based access, without incurring additional infrastructure costs. An additional cost-saving advantage of the Citrix platform license is the included service and support.

Deployment flexibility is another significant benefit as Chrome Enterprise Premium, integrated with Citrix Secure Private Access, allows organizations to consume the solution as a cloud-based service or opt for a hybrid deployment. This flexibility gives buyers control over user traffic routing via NetScaler and optimizes efficiency and application latency by avoiding cloud hairpinning. The unified user experience, integrated with the Citrix Workspace solution, provides a seamless portal for end users to launch all enterprise applications with a single log in, enhancing convenience and productivity.

Operational simplicity is achieved by allowing Citrix customers to administer and manage zero trust access policies via a single unified administrative console through the Citrix Secure Private Access console that is part of Citrix Web Studio. This is complemented by a single observability platform for troubleshooting, monitoring, and session management using Citrix Monitor.

How Google Chrome Enterprise Premium with Citrix Secure Private Access Addresses Secure Browser Adoption

Citrix has recognized both the increasing need for a user computing environmental solution that not only improves security but also improves the business experience. Consequently, it has shifted its focus from its zero trust (Citrix Secure Private Access) solution to a value proposition that includes Google's Chrome Enterprise Premium. The sections that follow illustrate notable benefits in this approach.

Technical Implementation

Google Chrome Enterprise Premium and Citrix Secure Private Access have multiple integration points, including steering Chrome Enterprise traffic through Secure Private Access infrastructure for ZTNA to internal applications, application configuration and access policies established in the Secure Private Access console with DLP policies, and

finally, monitoring Chrome Enterprise Premium web and SaaS application access via Citrix Monitor's unified help desk troubleshooting workflows. This setup allows organizations to swiftly respond to zero-day threats, ensuring robust security measures are in place to protect sensitive data and operations. The browser's architecture supports identity and context-aware access controls, adapting access permissions based on user identity and contextual information such as device security posture, thereby enhancing security protocols. In addition, remote browser isolation capabilities are available as optional features, providing further security for browsing activities by isolating potentially harmful web content from the user's device.

Seamless integration with existing IT infrastructure is a hallmark of this technical implementation, ensuring that organizations can incorporate these advanced security features without disrupting their current systems. This integration includes compatibility with existing security service edge technologies, allowing for a cohesive security strategy that aligns with modern enterprise requirements. By integrating Chrome Enterprise Premium with Citrix Secure Private Access, businesses can maintain a streamlined and efficient IT environment, reducing complexity and enhancing overall operational efficiency.

In addition, balancing cost and risk is a difficult task facing many SSE/SASE buyers, and supporting all users and applications can result in costly duplication of security products and capabilities. Citrix solves this by providing a comprehensive desktop environment based on the SSE principles, which emphasizes support for the most frequent app published to VDI — Google Chrome Browser. This can result in significant cost savings, without sacrificing security or tightening endpoint controls to the point of reducing functionality.

Security Framework

The security framework of Citrix Secure Private Access with Chrome Enterprise Premium is grounded in a zero trust security model, which mandates continuous verification of users and devices to ensure secure access. This approach minimizes the risk of unauthorized access by implementing stringent security checks at every stage of user interaction. Granular access control mechanisms further bolster this framework, offering detailed permissions that protect against unauthorized access and potential security breaches.

Protection against browser-based attacks is a critical component of this security framework, providing robust defenses against threats targeting the browser. By leveraging advanced security features and continuous monitoring, organizations can safeguard their digital assets from malicious activities. Google Chrome Enterprise Premium also receives automatic security updates and patches directly from Google, making the product ideal for providing protections against zero-day malware/attacks.

This comprehensive security strategy ensures that all aspects of user interaction are protected, maintaining the integrity and confidentiality of enterprise data.

User Experience

The user experience offered by Google Chrome Enterprise Premium with Citrix Secure Private Access is designed to be intuitive and familiar, utilizing a widely adopted browser interface that enhances user comfort and familiarity.

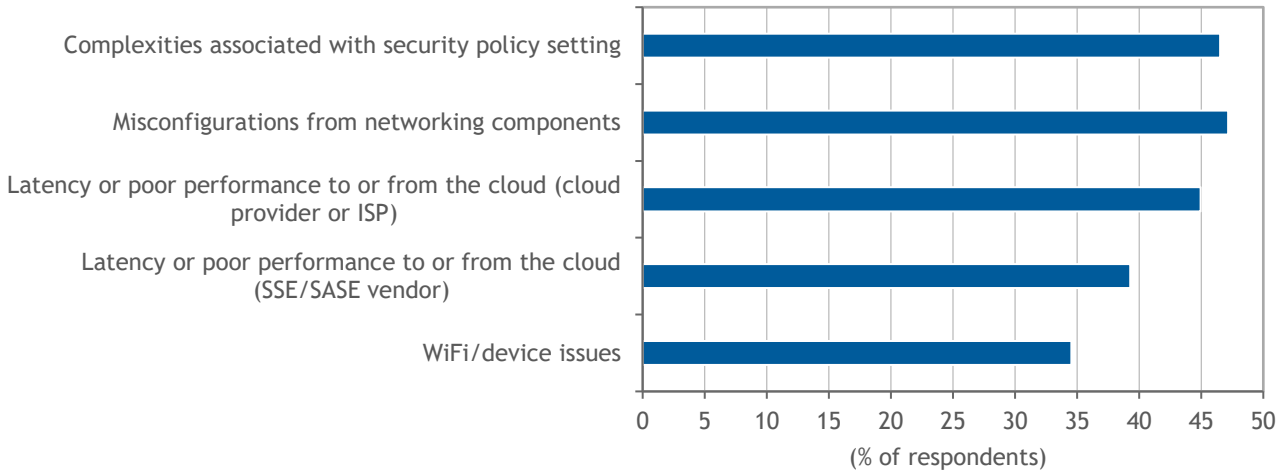
The Citrix solution is integrated with Chrome Enterprise Premium so that by logging into Chrome, traffic is then redirected to Citrix control points. This approach ensures that users can navigate the system with ease, minimizing the learning curve and promoting productivity. Support for progressive web applications is also included, ensuring compatibility with modern web technologies and applications that are essential for business operations.

Seamless application access is a key feature of this user experience, facilitating smooth transitions between applications and maintaining productivity across the enterprise. Users benefit from consistent cross-device experience, allowing them to access their applications and data from various devices without compromising functionality or security. Integration with NetScaler appliances further enhances this experience by protecting local user traffic, ensuring secure and efficient operations across the network (see Figure 2).

FIGURE 2

Enterprise Browser Demand: SSE/SASE Buyers Increasingly Turning to Enterprise Browser as an SSE Addition

Q. Please gauge your organization's interest in the integration of enterprise browser into your SSE/SASE solution.



n = 634

Source: IDC's *SSE/SASE Buyer Adoption Survey,* March 2025

CHALLENGES

Industry Challenges

There are industry challenges that apply to the adoption of any new or additional security technologies. However, in the context of cybersecurity solutions, the challenges that should be considered are discussed in this section.

Complex policy configuration requirements demand meticulous attention to detail, as organizations must ensure that security policies are correctly configured to protect sensitive data and maintain compliance with industry standards. Managing distributed teams adds another layer of complexity to the technical implementation of these solutions. With employees working remotely or across different geographical locations, maintaining consistent security protocols and ensuring seamless access to enterprise resources becomes challenging. The management overhead associated with coordinating these distributed teams can strain IT resources, requiring robust management tools and strategies to ensure effective communication and collaboration. These technical challenges necessitate a comprehensive approach to implementation,

focusing on optimizing performance, ensuring compatibility, and streamlining policy configuration to support distributed teams effectively.

Citrix Secure Private Access with Chrome Enterprise Premium is a good approach for organizations looking for a well-articulated approach to securing access holistically, including within the end-user computing environment. However, this solution does present some challenges to organizations wishing to adopt it. These include implementation barriers and operational considerations.

Implementation Considerations

The implementation of Citrix Secure Private Access with Chrome Enterprise Premium faces several barriers that are common to most cybersecurity solutions, including difficulty in demonstrating return on investment (ROI). Organizations often struggle to quantify the financial benefits of these security solutions, as the costs associated with implementation and maintenance can be substantial. Citrix and Google's approach to SSE inherently favors integrations with the Citrix platform over existing security architecture that buyers likely have already in place, but this may result in policy and configuration complexities, duplicate functionality, and limitations in telemetry and threat sharing with existing firewalls and SASE/SSE platforms. However, for existing Citrix customers, tight integration with VDI is likely to be a more pressing concern and will undoubtedly yield its own set of productivity-based ROI gains.

Some training will likely be necessary so that employees understand the "why" and the "when" to use the enterprise browser versus consumer browsers. Traditional network security platforms function almost entirely in the background for employees/users, and many agentless architectures are completely invisible. With an enterprise browser-based approach, Citrix and Google are at the forefront of users' devices and thus are directly interfaced with by the users. It is noteworthy that while Chrome is widely used, it is not the (only) choice for all users, with some still more familiar with alternatives. This requires a strategic approach to change management, focusing on educating employees about the benefits of the new system and addressing any concerns or resistance to change. Though minor, these implementation considerations highlight the need for a clear strategy that addresses ROI, balances security with user experience, and facilitates training and adoption to ensure successful deployment.

Operational Considerations

Policy management complexity is a critical operational consideration that organizations must navigate with any security product or platform, which introduces new configurations and security policies across the enterprise. For existing Citrix customers, migration will be seamless, however, new customers should consider the increased complexity of adding a new set of security products into their ecosystem. For new

customers, the introduction of new interfaces, management plane, and policy engine could result in the need for increased operational overhead.

CONCLUSION

The market impact of enterprise browsers, specifically when integrated with solutions like Citrix Secure Private Access, is profound. As enterprise browser adoption is expected to reach 52% by 2025, these tools are becoming essential components of modern security architecture. This growth trajectory is mirrored in the adoption of ZTNA and SSE solutions, which are experiencing rapid expansion. The increasing focus on holistic security solutions reflects the urgency and importance of robust, integrated secure access measures in the evolving digital landscape. By addressing the complexities of IT infrastructure management and the challenges of multicloud environments, this integration positions Citrix as a key player in the cybersecurity market, offering comprehensive protection and operational efficiency.

For Citrix Secure Private Access with Chrome Enterprise Premium in particular, the outlook is promising, as organizations continue to adapt to emerging threats and evolving security requirements. The continued evolution of security features, such as advanced threat analysis and zero trust communication principles, will enhance the solution's capabilities, providing robust defenses against sophisticated attacks. Enhanced integration capabilities will further streamline the deployment process, ensuring seamless compatibility with existing systems and reducing implementation barriers. As organizations prioritize performance optimization and resource efficiency, this integration will play a critical role in supporting their strategic objectives, enabling them to maintain a competitive edge in the digital marketplace while safeguarding their operations against future threats.

MESSAGE FROM THE SPONSOR

Citrix, a business unit of Cloud Software Group, was founded on a key principle, to Secure the Work, by pioneering secure remote access for the workplace. Built on zero-trust principles, the Citrix Platform enables enterprises to optimize application access to meet the needs of each critical use case, ensuring productivity, while reducing cost and complexity. In a world of continuous disruptive change, Citrix continues to innovate to support the entire application value chain—from changing methods of secure application development to application delivery—and an evolving workforce that depends on artificial intelligence (AI) agents and co-pilots to accelerate productivity. Citrix has long-standing relationships from serving a diverse global customer base, including major enterprises in healthcare, financial services and government agencies. We empower organizations to enable flexible work, supporting a broad spectrum of end-user needs while giving IT confidence in the safety of their data and devices. Learn more at www.citrix.com.

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com