Verizon Trusted Connection Boosts Mid-Market Cybersecurity

Making the case for stronger mid-market cybersecurity

In one Northeastern U.S. town, a seemingly routine invoice led to a financial disaster as attackers spoofed a familiar vendor's details and sent the town's municipal accounting team a legitimate-looking yet fraudulent invoice. Without the security systems typically found in larger enterprises, the town's payment system was compromised, resulting in the loss of nearly half a million dollars.

Unfortunately, this type of scenario, is not uncommon. According to Verizon's 2024 Data Breach Investigations Report (DBIR), 68% of breaches involve a human element, such as phishing attacks or user errors. The 2024 DBIR also reported a startling 180% increase in cyberattacks that exploit vulnerabilities. Mid-sized organizations that typically range from 100 to 2,000 employees can face the same cyber threats as larger enterprises – often without the dedicated IT teams and security expertise needed to defend against breaches that can lead to downtime and financial losses.

One U.K. government survey conducted in early 2024 found that 45% of mid-sized businesses experienced a cybercrime in the last year, with phishing being the most common attack type. Despite rising threats, only 55% of mid-sized businesses surveyed had formal incident response plans in place, compared to 73% of large businesses.

Increasingly, the vulnerabilities inherent in many mid-sized organizations lacking the highly skilled specialized cyber defense resources or incident response plans are driving a need for more powerful, comprehensive protection that is both accessible and easy-to-use for mid-sized organizations.

How Trusted Connection empowers mid-market cybersecurity

Trusted Connection is designed to help provide robust, enterprise-grade capabilities tailored specifically for mid-market cybersecurity needs. It's a powerful, integrated platform that simplifies security management and implements comprehensive Zero Trust protection securing access across devices and networks.

Many mid-sized organizations are stretched thin, often with small IT teams who wear multiple hats. They're expected to manage everything from network infrastructure to endpoint security, all while ensuring that daily operations run smoothly.

Trusted Connection is designed to make cybersecurity management as straightforward as possible, integrating advanced features into an intuitive portal that even non-experts can navigate with ease.

Trusted Connection seamlessly integrates with existing LDAP based identity management systems (such as Microsoft Azure Entra ID and OpenLDAP), helping ensure that user access controls are up-to-date without the need for manual synchronization or intervention. Administrators can manage firewall settings, content filtering, and user permissions from a single dashboard. Even the online setup process is guided, helping administrators quickly deploy robust security measures without requiring extensive training or expertise.

Embedded Zero Trust capabilities

Trusted Connection ensures end-to-end security, whether employees are accessing cloud applications, on-premises data centers, or even working remotely from a local coffee shop.

At the core of Trusted Connection is an embedded Zero Trust framework, which sets this product apart. A Zero Trust approach assumes that no user or device can be trusted by default, regardless of whether the user or device is inside or outside the network perimeter. The product's Zero Trust capabilities are fully embedded, which means administrators don't have to complete the complex process of implementing Zero Trust from scratch. Verizon has already done the heavy lifting for them.

Network access is granted only to the applications required by the user to complete daily tasks, and that access is continuously monitored and verified. To illustrate, a construction company's architects only need access to design systems, while billing personnel require accounting system access. Trusted Connection helps ensure that even if an architect's credentials are somehow compromised by a bad actor, the actor can't access financial data, minimizing data breach risks.

verizon business

By embedding Zero Trust into the core of Trusted Connection, organizations can protect against unauthorized access and data breaches, without the complexity typically associated with robust security systems. A higher level of protection is increasingly needed, as highlighted by the 2024 DBIR: 32% of breaches were tied to ransomware and extortion, which often exploit unsecured access to critical systems.

Secure mobile device access virtually anywhere, anytime

In hybrid work environments, employees access organizational resources from various devices and locations. This trend can bring serious security challenges for mid-sized organizations that may not have the infrastructure to support comprehensive mobile security.

That's where Trusted Connection can make a difference by providing robust features that help ensure all endpoints, no matter whether they are company-issued or personal devices, are secured.

According to Verizon's 2024 Mobile Security Index, 53% of organizations surveyed experienced a security incident involving a mobile or IoT device that resulted in data loss or downtime. And mid-sized businesses are not exempted from this trend. Imagine a construction company with teams spread across multiple job sites. Employees rely on mobile devices to access critical project data, such as CAD drawings stored in the cloud. With Trusted Connection, they can securely access and update information in real-time, helping to ensure designs are kept up-to-date, while also helping to avoid exposing the firm to unnecessary risks.

Trusted Connection supports secure access across various devices and networks, including Verizon's Fixed Wireless Access (FWA) and third-party networks, so employees can work from anywhere, confident that their applications and data are secure.

Granular role-based access and content filtering

Trusted Connection also offers advanced content filtering and role-based access controls, particularly in the Trusted Connection "Plus" version. Role-based access controls give IT staff the ability to tailor security policies to the specific needs of different user groups. For instance, marketing teams may need access to social media platforms for their work, while other departments may not. With Trusted Connection, administrators can define exactly who has access to what resources, helping to ensure that each employee only interacts with the applications and data necessary for their role.

Meanwhile, advanced content filtering capabilities can help administrators further customize what users can access and how they interact with different applications. Administrators can block or allow specific websites and services based on company policies, helping to prevent inappropriate or harmful content from entering the network.

Take for example, an engineering firm employee who viewed inappropriate content on their company laptop, then accidentally deleted essential system files when trying to hide their activity. This scenario emphasizes why it's important to block access to harmful or inappropriate content to protect a firm's information, assets and reputation.

For those who opt for Trusted Connection Plus, integration with Cloud Access Security Brokers (CASB) provides even more fine-grained control, allowing administrators to manage specific functions available within SaaS applications.

Incident response expertise

Cybersecurity is an ever-evolving field. Trusted Connection provides strong, easy-to-manage security for mid-market organizations. For additional essential support, incident response capabilities are available with Verizon's Rapid Response Retainer (RRR), which provides access to top-tier security experts during critical incidents.

Why choose Trusted Connection?

Often lacking the extensive resources and dedicated IT security teams of larger enterprises, mid-market organizations need a solution that balances simplicity and robust protection. Trusted Connection addresses this need by providing an integrated platform that streamlines security management while delivering advanced Zero Trust protection. Verizon's comprehensive approach helps ensure secure access across all devices and networks, making it easier for mid-sized businesses to safeguard their operations without the complexity usually associated with enterprise-level security solutions.

Trusted Connection was built with mid-market cybersecurity needs in mind. For IT and security leaders in mid-sized organizations, Trusted Connection represents a significant step forward in defending against cyber threats. With a focus on usability, adaptability and comprehensive protection, Trusted Connection can help safeguard your organization's operations today, and in the future.

We invite you to explore how Trusted Connection can transform your organization's approach to cybersecurity

To learn more about Trusted Connection and how it can help secure your operations, contact your account manager or visit verizon.com/business/products/security/network-cloud-security/trusted-connection/.

verizon business