WHITEPAPER

THE ROAD AHEAD:

What MSPs need to know about the growing complexity of Enterprise Network Management

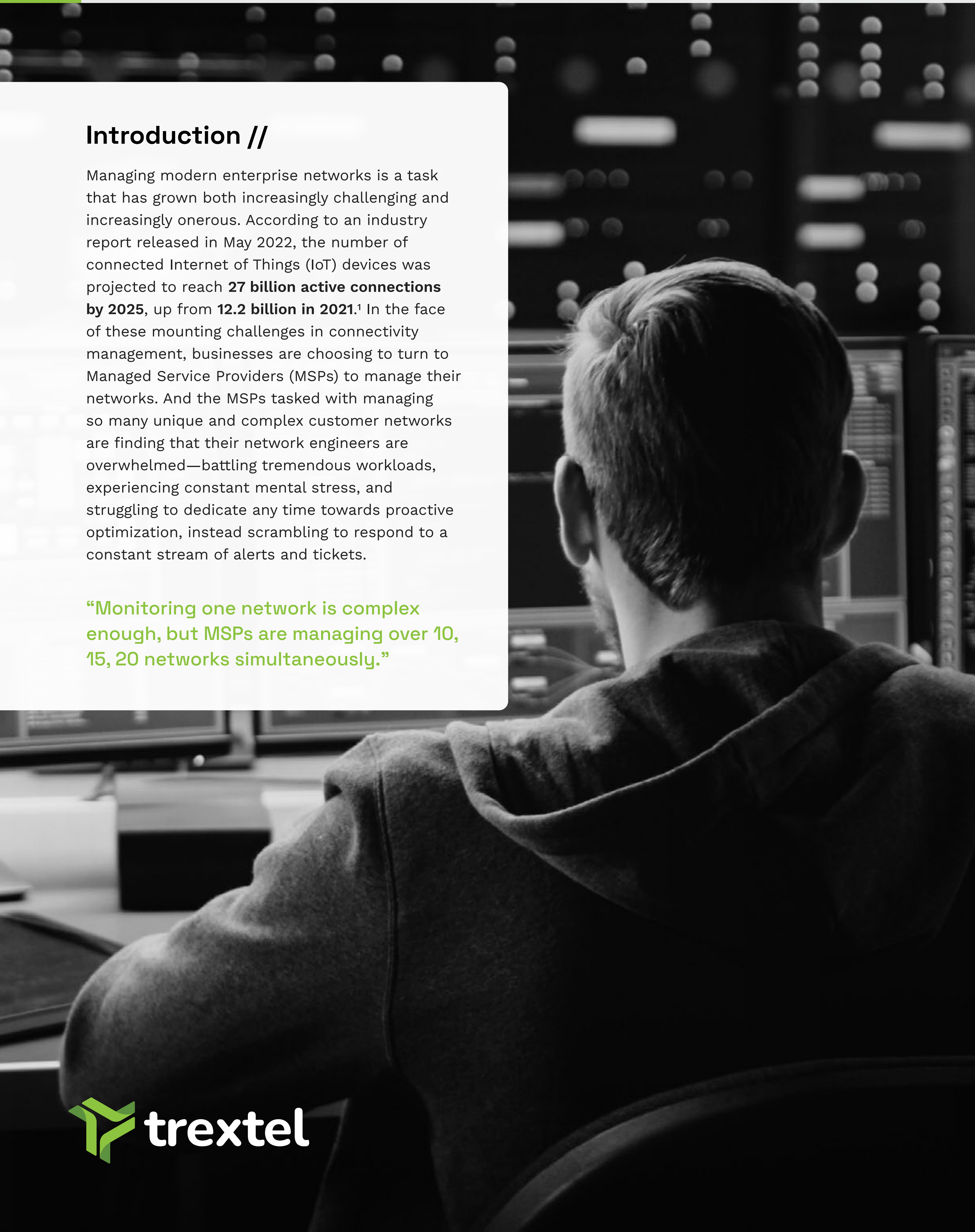
July 2023

trextel

Introduction //

Managing modern enterprise networks is a task that has grown both increasingly challenging and increasingly onerous. According to an industry report released in May 2022, the number of connected Internet of Things (IoT) devices was projected to reach **27 billion active connections by 2025**, up from **12.2 billion in 2021.**[1] In the face of these mounting challenges in connectivity management, businesses are choosing to turn to Managed Service Providers (MSPs) to manage their networks. And the MSPs tasked with managing so many unique and complex customer networks are finding that their network engineers are overwhelmed—battling tremendous workloads, experiencing constant mental stress, and struggling to dedicate any time towards proactive optimization, instead scrambling to respond to a constant stream of alerts and tickets.

> “Monitoring one network is complex enough, but MSPs are managing over 10, 15, 20 networks simultaneously.”



Network Engineers are Facing Overwhelming Workloads and Rising Costs of Mistakes //

Network engineers are a valuable resource—and they are in short supply. Turnover is rampant in the industry. With over **125,000** open positions for network engineers on LinkedIn, it's clear that finding and retaining qualified personnel is a challenge. The average tenure of a network engineer is **only 18 to 24 months**.[2] With so much churn, knowledge loss is common and human error an inevitability.

MSPs are finding that their network engineers are overwhelmed—battling tremendous workloads, experiencing constant mental stress, and struggling to dedicate any time towards proactive optimization.

For retailers, the impact can be particularly significant, with the average retailer experiencing **over 80 hours** of unplanned downtime every year at a staggering cost of **$5,600 per minute**—not to mention the accompanying reputational losses. In a survey of 500 small businesses, **37%** reported losing customers as a direct consequence of downtime.[4]

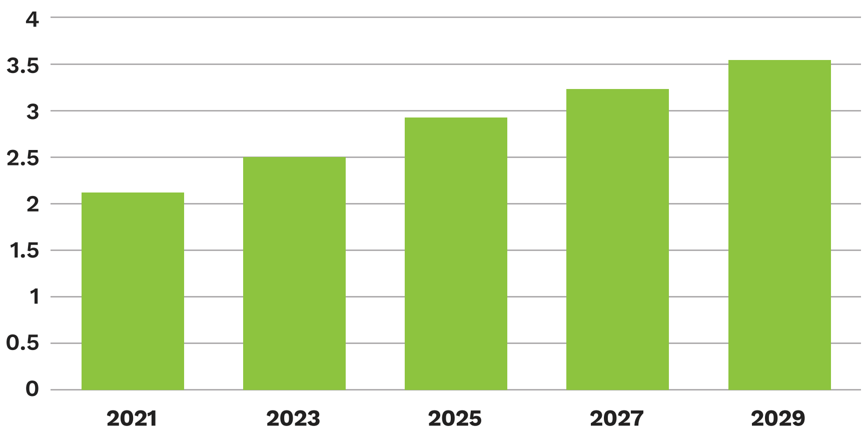
The consequences are significant. **Nearly 40%** of organizations have suffered a major outage caused by human error over the past three years.[3] The cost of these outages is also on the rise: **over 60% of outages** in 2022 cost organizations **more than $100,000**, and **15%** of these surpassed **$1 million**.

To alleviate the burden on their engineers and to minimize the impact of any outages on their customers, MSPs rely on the use of monitoring tools. The global network monitoring market has grown steadily larger in recent years, having been valued at **$2.11 billion in 2021** and projected to grow to **$3.8 billion by 2030**.[5]

In theory, these tools should simplify network management by alleviating the need for direct human intervention via increased automation. However, the reverse has proven to be true: despite the high availability and variety of sophisticated monitoring tools, a recent survey has shown that **52%** of network engineers are reporting increased mean time to resolution (MTTR) for business customers.[6]

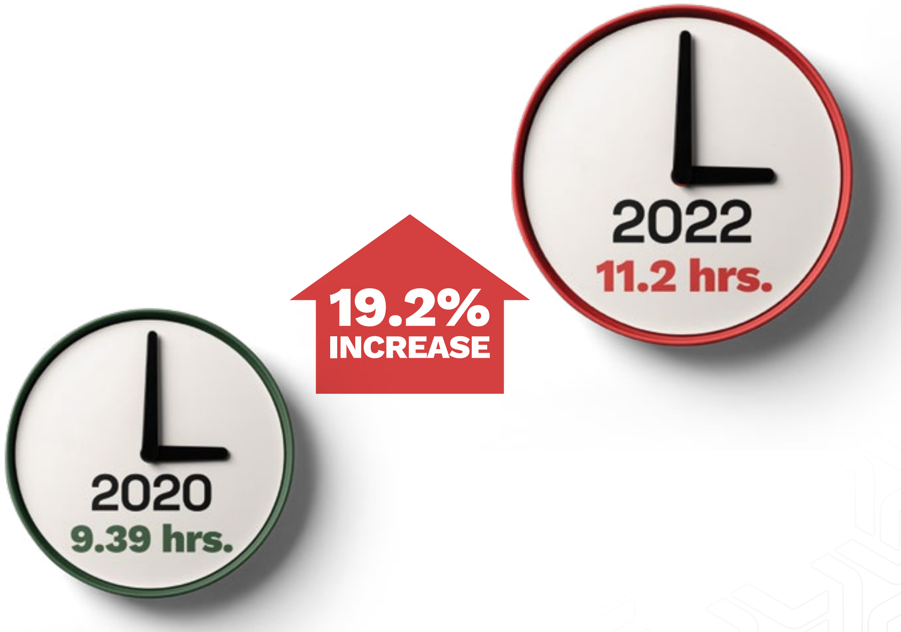
Clearly, the solution cannot be to continue indiscriminately adding more tools: more, in this case, does not mean better. In order for MSPs to effectively overcome the challenges of network management, it is crucial to gain a deeper understanding of the obstacles facing engineers... and to adopt a comprehensive connectivity business intelligence platform that can bring together components across the network to address these challenges.

Network Monitoring Market Size (USD Billion)



The global network monitoring market was valued at **$2.11 billion** in 2021 and is expected to grow at a CAGR of **7%** during the forecast period.

Mean Time To Respond (MTTR) is Increasing



52% of the network engineers surveyed reported seeing an increase in MTTR with their business customers.

trextel

The Network Engineer's Challenge: More Monitoring Systems, More Problems //

Why, in a technology landscape teeming with sophisticated monitoring systems, are network engineers actually taking longer to resolve network issues?

The crux of the problem is that efficiency is not hindered by a lack of technology, but rather by human resourcing challenges. A traditional service model for a Network Operations Center might allocate a certain number of nodes to each technician or engineer to monitor. But as the number of nodes—and associated monitoring tools—has grown, so too has the number of alerts, making this model less viable and resulting in overwhelm for NOC techs and network engineers.

Consider the astonishing scale and scope of the modern enterprise network: at the edge, this might include any number of systems, from SD-WAN appliances to point-of-sale systems to network security systems, spanning multiple points of presence (PoP) and multiple connection types, each with its own unique configuration and challenges, each monitored individually. The sheer volume of notifications produced by these monitoring systems—many of which might turn out to be false, unactionable, or even irrelevant—makes it difficult to identify a network issue, let alone resolve it within a reasonable timeframe.

Environmental sensors, which represent a growing market within the IoT industry, provide an illustrative example. In a scenario where a single PoP might have 50 or so floor sensors distributed in 1m^2 segments across a warehouse floor, having one or two sensors in each segment malfunction is not a significant event in isolation. However, each sensor might be configured by default to send out its own alert—a torrent of information that technicians and engineers must then sift through to determine the appropriate course of action, consuming valuable time and increasing MTTR across the board.

> "Any system that is not correctly configured and administered will absolutely drown you in alerts. And most people don't understand the data that they're getting from these devices and what it means, so a lot of what you're getting is quite honestly useless."

trextel

The Elusive Quest for Provider Accountability During Network Outages //

When an outage occurs, the most urgently needed information isn't necessarily why the outage has occurred, but rather where in the circuit it's happening and who is responsible for its resolution.

It's not unusual for a single circuit to cross a half-dozen or more providers. When an outage occurs, often the first step that a network engineer or NOC tech will take is to reach out to each of these providers to determine the point of failure. The typical response is, "We've looked into the issue, and the problem is outside of our area." Without comprehensive network-wide visibility, it's difficult for a network engineer to challenge such claims with concrete evidence. The engineer is left to navigate a labyrinth of finger-pointing and delays while every provider continues to pass the metaphorical buck and the mean time identify (MTTI) continues to rise.

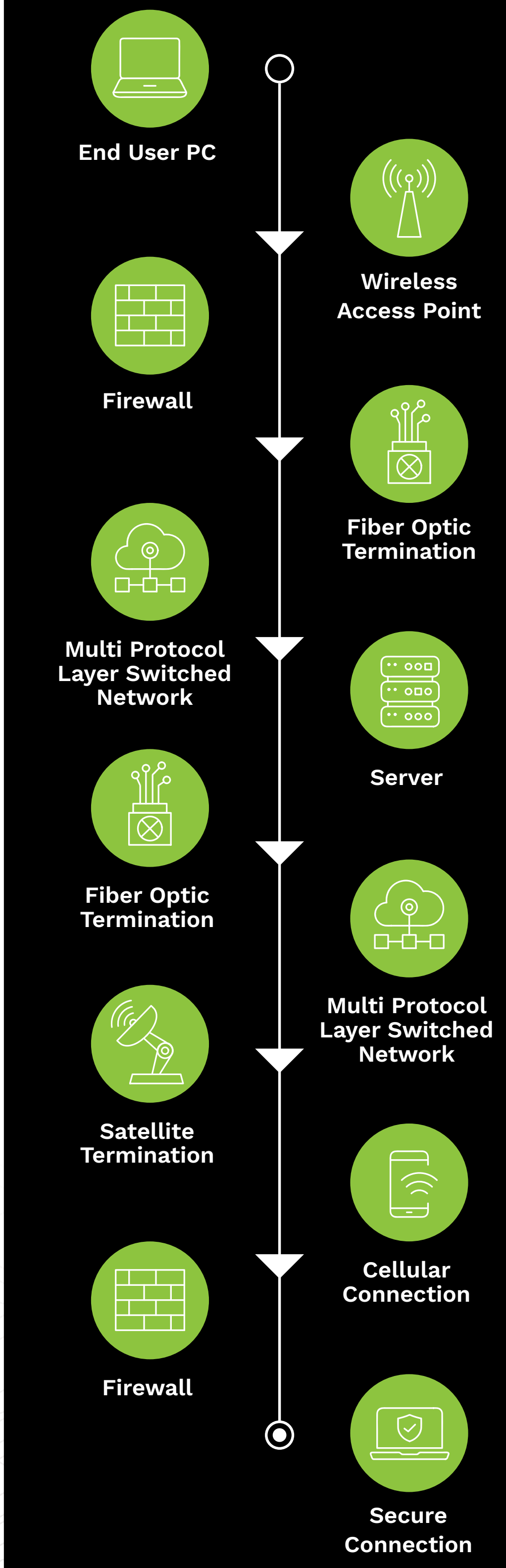
Providers, of course, have their own interests at stake when disclaiming responsibility during an outage—chief among which is avoiding any penalties associated with failing to uphold service-level agreements (SLAs) regarding network uptime. Shifting the blame also buys providers time to conduct their own internal investigations and quietly repair any issues, neatly transferring the risk of financial loss and reputational damage onto the MSP.

The repercussions go beyond business productivity. Network outages create fertile ground for cybercriminals to exploit network vulnerabilities. Extended downtime can disrupt security monitoring protocols, leaving MSPs and their customers more susceptible to cybersecurity risks. Additionally, as MSPs rush to implement failover mechanisms in a bid to maintain customer operations, new vulnerabilities appear and attack surface increases, since such temporary solutions may lack the same level of security controls as the primary infrastructure. The longer the outage, the more opportunity for malicious actors to strike.

A talented network engineer might be able to quickly make an educated guess that reduces MTTI and expedites resolution. But talented engineers are more and more thin on the ground, progressively costly to hire, and increasingly difficult to retain.

The average tenure of a network engineer is only 18 to 24 months.

Network Connectivity Path



End User PC

Wireless Access Point

Firewall

Fiber Optic Termination

Multi Protocol Layer Switched Network

Server

Fiber Optic Termination

Multi Protocol Layer Switched Network

Satellite Termination

Cellular Connection

Firewall

Secure Connection

Trading Simplicity Now for Complexity Later: Why Abstracted Equipment Spells Trouble for MSPs //

Insight into the networks at the edge can be limited, often requiring engineers to physically visit sites to resolve issues. In fact, **91%** of organizations say they occasionally send network engineers or technicians out to sites to resolve issues, with **42%** saying that they do this for the majority of outages and downtime.[7] Not only does this result in wasted resources, increased downtime, increased mean time to repair (MTTR) and reduced network performance, it also creates dissatisfaction for the high-level engineering resources forced to travel out to remote sites.

This is in part because business models within the hardware industry have shifted, with manufacturers looking to increase the share of revenue coming from recurring subscription, software and service fees. Manufacturers of network equipment may deliberately limit what commands and information can be accessed remotely as a way of enforcing the use of manufacturer-specific tools or management services, demanding that technicians and network engineers manage multiple platforms in tandem to achieve a comprehensive view of the network and simultaneously making it challenging for them to address equipment issues without physically going on-site.

Equipment abstraction and simplification will only become more prevalent in the future, continuing a trend that gained momentum during the COVID-19 pandemic, when engineers were restricted from physically accessing sites and organizations were forced to seek out streamlined plug-and-play solutions that were remotely configurable. This shifting landscape has moved the focus away from intricately designed hardware configuration and towards simpler, abstracted devices.

For small and medium businesses with more limited resources—or enterprise organizations ruthlessly focused on enhancing the scalability and agility of their IT operations—this trend is a boon. However, for the NOC technicians and network engineers responsible for network management, the growing prevalence of abstraction portends increased impediments to resolution, and an even greater number of field deployments as a consequence.

Unlocking More Network Management Efficiencies Through Integrations and Diagnostics //

One way to manage the challenges associated with abstracted devices and proprietary protocols is by having a network management platform that comes strapped with comprehensive integrations. There are three areas where integration can help streamline workflows, each with its own distinct advantages:

1. Manufacturers.

2. Incident management and ticketing.

3. Circuit providers.

In the case of manufacturer integrations, traditional protocols have required MSPs to have network-level access to equipment for setup, configuration and troubleshooting—a time-consuming and laborious process that requires the participation of the customers, besides. For a larger MSP managing multiple customers, each of which might have equipment from multiple manufacturers, this adds considerable bloat to engineers' and technicians' workloads. With manufacturer integrations, however, MSPs can gain immediate visibility into equipment across all their customers with a simple password or API key. Leveraging manufacturer APIs allows network engineers to take a more standardized approach towards device management, irrespective of equipment provenance, by ensuring compatibility, facilitating integration and simplifying device onboarding for clients looking to rapidly scale their network infrastructure.

Traditional protocols have required MSPs to have network-level access to equipment for setup, configuration and troubleshooting—a time-consuming and laborious process that requires the participation of the customers, besides.

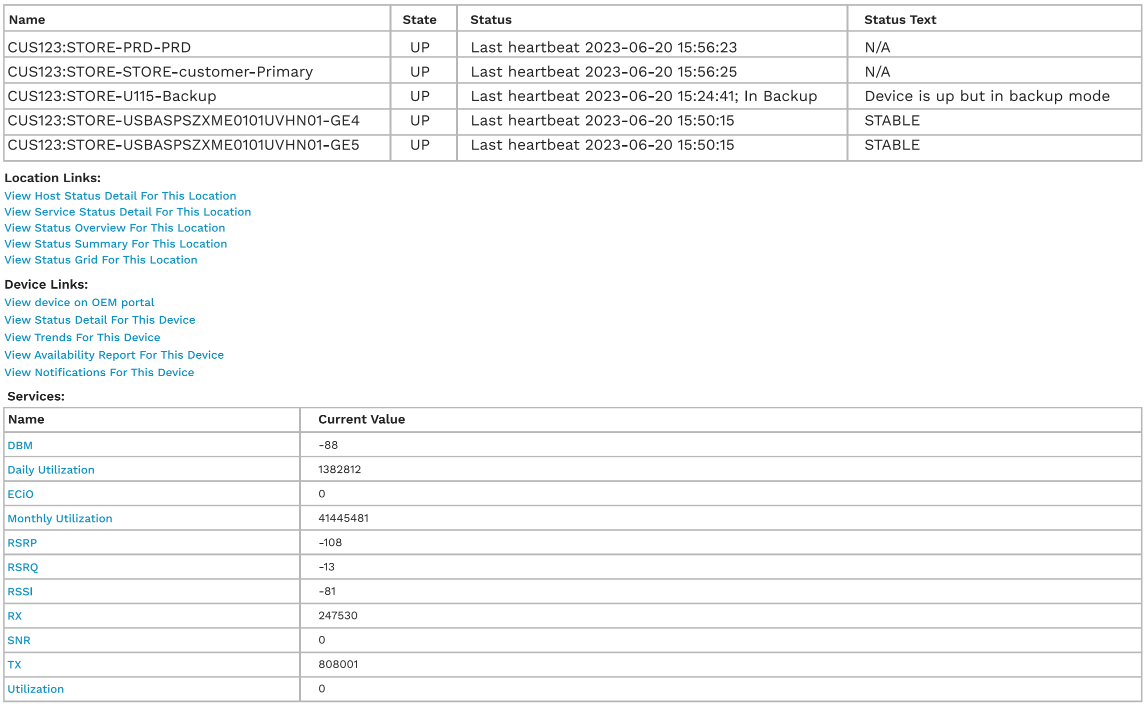
Integrations with incident management and ticketing systems help streamline workflows and reduce administrative burden for NOCs. Every technician is familiar with the tedium of manually entering incident details into one or more ticketing systems, but with an integrated solution, tickets can be automatically created and populated inside of the management system without the need for manual entry.

Such integrations can also streamline monitoring and incident routing. With the right integrations, a network management platform can automatically generate a ticket with enough detailed information to provide the context necessary for rapid resolution. The flow of data becomes bidirectional: capturing more accurate information around network events in the ticketing system allows teams to track the entire incident lifecycle more easily and providing improved upstream and downstream visibility, all behind a single pane of glass.

Solving practical problems with integrations //

Consider a scenario where a connectivity problem is detected in a specific location with two devices, a primary and a backup. A stock ticketing system might send a notification with a basic description of the problem, the location and some contact details. However, this information might not be sufficient for a tech to assess the severity of the problem, requiring them to manually gather additional information.

But with integration into a management platform, the ticket generated can be made to include additional relevant details, like the devices involved and their last known status before failure. With this context, the engineer can quickly conclude that the site is still able to continue operations, though with potential limitations. On the other hand, in a scenario where direct resolution is required, troubleshooting can be initiated promptly, or in some cases, the issue can be resolved remotely without even needing direct access into the affected system.



Name	State	Status	Status Text
CUS123:STORE-PRD-PRD	UP	Last heartbeat 2023-06-20 15:56:23	N/A
CUS123:STORE-STORE-customer-Primary	UP	Last heartbeat 2023-06-20 15:56:25	N/A
CUS123:STORE-U115-Backup	UP	Last heartbeat 2023-06-20 15:24:41; In Backup	Device is up but in backup mode
CUS123:STORE-USBASPSZXME0101UVHN01-GE4	UP	Last heartbeat 2023-06-20 15:50:15	STABLE
CUS123:STORE-USBASPSZXME0101UVHN01-GE5	UP	Last heartbeat 2023-06-20 15:50:15	STABLE

Location Links:
View Host Status Detail For This Location
View Service Status Detail For This Location
View Status Overview For This Location
View Status Summary For This Location
View Status Grid For This Location

Device Links:
View device on OEM portal
View Status Detail For This Device
View Trends For This Device
View Availability Report For This Device
View Notifications For This Device

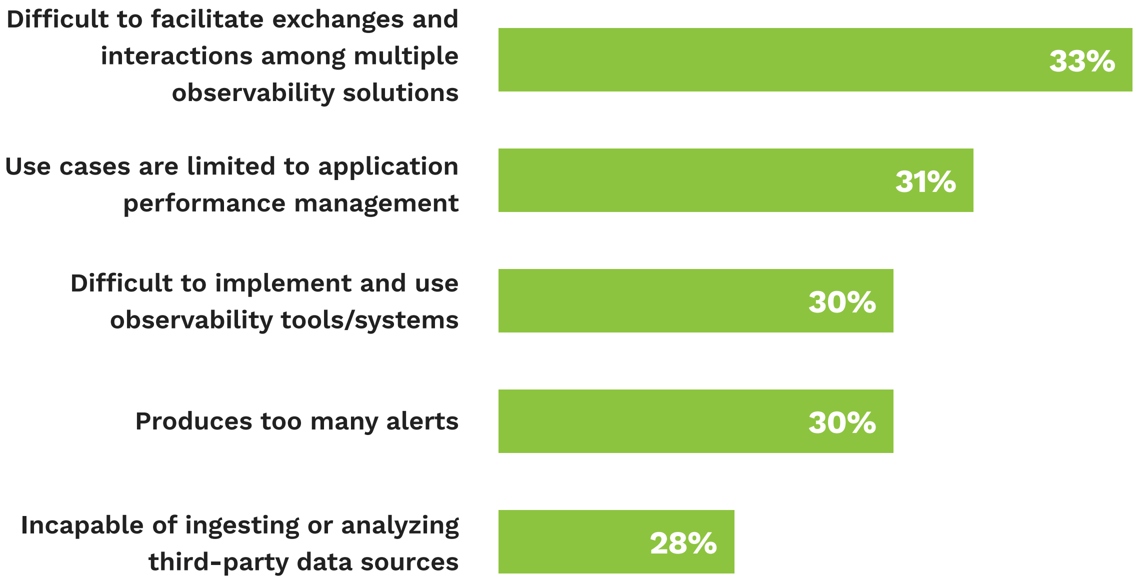
Services:

Name	Current Value
DBM	-88
Daily Utilization	1382812
ECIO	0
Monthly Utilization	41445481
RSRP	-108
RSRQ	-13
RSSI	-81
RX	247530
SNR	0
TX	808001
Utilization	0

Integrations with circuit providers unlock similar benefits—in the case of an issue with the circuit, an integrated platform eliminates the need for manual intervention by automatically generating a ticket and notifying the circuit provider.

These reductions in administrative overhead are especially helpful for frontline staff like service desk personnel and tier one support, who handle a high volume of tickets and aim for quick resolutions. Not only is service delivery (and, consequently, customer satisfaction) improved as a result, tier two and tier three engineers are empowered to focus on the NOC's core objective: proactively optimizing network performance and identifying potential issues before they can impact the business.

Monitoring Tool Customers Express Problem Areas with Existing Monitoring Tools



83%

IT respondents are either actively seeking new monitoring services or have plans to expand or improve their approaches to monitoring.

11%

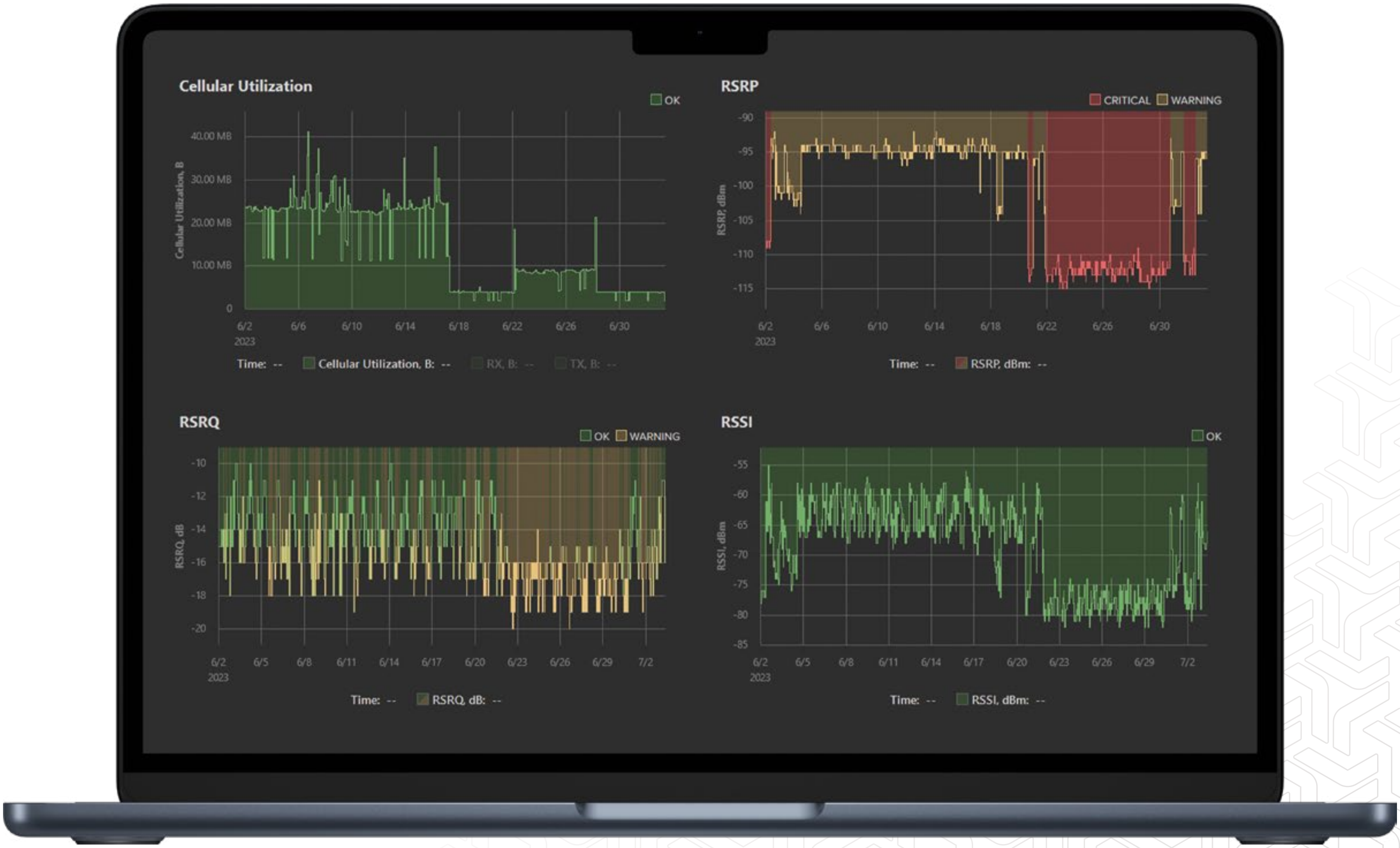
With only 11% saying they're satisfied, users are demanding new functionality from vendors.

trextel

Human Experience + Business Intelligence = Proactive Network Optimization //

Proactive optimization is especially crucial in the context of cellular networks. As 5G technology improves and the cost of data decreases, a growing number of enterprises are moving away from traditional hardline connections and adopting wireless communications as their primary connectivity solution. Cellular networks are taking up a greater share of the WAN provider market; a 2022 industry report found that the use of 4G and 5G cellular links is expected to grow the fastest, with a projected increase of **68%**.[8] This choice, however, comes with a greater need for remediation when compared to less complex hardline connections—and a greater need for the advanced capabilities that come with a sophisticated connectivity business intelligence platform.

Network performance management solutions with advanced network capabilities, like the ability to algorithmically analyze historical performance data and generate trendline insights, provide incredible value for NOCs tasked with managing cellular networks.



trextel

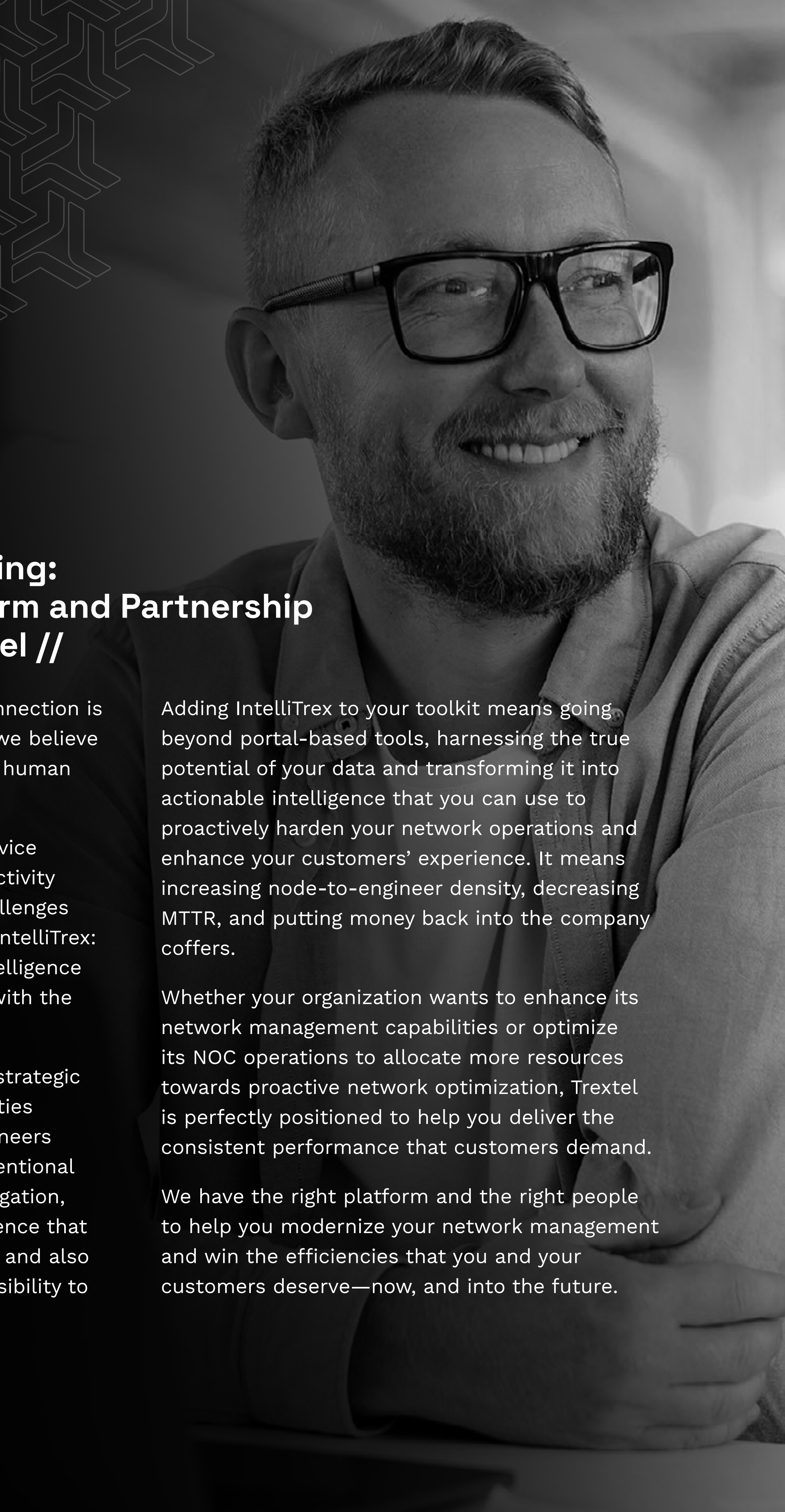
Storytime: Where Technology and Expertise Meet //

A retailer had been facing connectivity issues, specifically during the hours of 3 p.m. to 7 p.m. By pulling the information around signal levels of the customers' devices, the transit times of data, and mapping these against the PoPs in question, the network engineers were able to interpret these trends and determine a root cause. "Looking at the data, we saw first off that all of these affected locations were next to major highways," noted Garrett. "The times where connectivity dropped matched up with rush hour—we were able to figure out that the cause was all the bored commuters stuck in gridlock, scrolling their phones, checking social media and chewing up most of the available bandwidth in the area. We were able to make the recommendation to the customer to swap cell towers and adjust antenna placements to help address the issue."

In another scenario, a different organization found that the performance of its cellular network decreased during spring, but only in certain locations. The network engineers examined historical data around signal strength, correlated it to geographic and topographic elements, and determined the issue: that increased transpiration from trees in warmer weather was creating increased humidity, and the additional water vapor in the air was disrupting cellular signals. "We were able to recommend that the customer either remove the existing tree cover or relocate their network antennas to maintain service uptime throughout the summer, which would otherwise be a pretty miserable time," Garrett said.

In both these cases, the availability of a platform with metric graphing and location-based monitoring provided experienced engineers with the information they needed to make smart deductions and mitigate their customers' problems before they had significant business impact.

When armed with comprehensive insights, engineers can more quickly and easily identify recurring issues, predict potential bottlenecks, and proactively allocate resources to optimize cellular network performance without impacting day-to-day work.



More Than Mere Monitoring: Say Yes to People, Platform and Partnership You Can Trust, with Trextel //

At Trextel, we envision a world where connection is possible for everyone, everywhere—and we believe that success lies in the synergy between human expertise and powerful technology.

As a leading Managed Software-as-a-Service (MSaaS) provider and a pioneer of connectivity solutions, we understand the unique challenges MSPs face today. That's why we created IntelliTrex: our proprietary connectivity business intelligence platform purposefully designed to align with the growing demands of the industry.

IntelliTrex is deliberately crafted to be a strategic enabler for MSPs, enhancing the capabilities and reach of NOCs and empowering engineers and technicians to do more. Where conventional monitoring solutions focus on data aggregation, we built IntelliTrex with business intelligence that combines and streamlines network data, and also provides valuable insights by providing visibility to performance trends.

Adding IntelliTrex to your toolkit means going beyond portal-based tools, harnessing the true potential of your data and transforming it into actionable intelligence that you can use to proactively harden your network operations and enhance your customers' experience. It means increasing node-to-engineer density, decreasing MTTR, and putting money back into the company coffers.

Whether your organization wants to enhance its network management capabilities or optimize its NOC operations to allocate more resources towards proactive network optimization, Trextel is perfectly positioned to help you deliver the consistent performance that customers demand.

We have the right platform and the right people to help you modernize your network management and win the efficiencies that you and your customers deserve—now, and into the future.

trextel

Sources Cited //

1. https://iot-analytics.com/number-connected-iot-devices/ and Cisco VNI Complete Forecast

2. Uptime Institute. (2022). 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening. https://uptimeinstitute.com

3. Opengear. (2022). The Costs of Downtime. https://opengear.com/white-papers/white-paper-the-costs-of-downtime/

4. Digi International. Retail: The Cost of Business Downtime. https://www.digi.com/resources/library/solution-briefs/digi-infographic-retail-costs-of-business-downtime

5. Polaris Market Research. (2021). Network Monitoring Market Size, Share, Trends, Analysis Report. Retrieved from https://www.polarismarketresearch.com/industry-analysis/network-monitoring-market

6. Opengear. (2022). The Costs of Downtime. https://opengear.com/white-papers/white-paper-the-costs-of-downtime/

7. Opengear. (2022). The Costs of Downtime. https://opengear.com/white-papers/white-paper-the-costs-of-downtime/

8. Cradlepoint (2022). The State pf Wireless WAN 2022. https://newcomglobal.com/wp-content/uploads/2023/01/State-Of-Wireless-Wan-2022-Report.pdf

trextel

From the Edge to the Engineer.

Trextel is a leading managed Software-as-a-Service (mSaaS) provider. And we're all about connections. For over 25 years, we've worked hard to equip businesses with reliable connectivity and innovative technology. We're passionate about innovation—and about our customers. Our priority is always in delivering seamless connectivity, optimizing performance, and resolving any issues that arise along the way. More than a provider, we strive to be a trusted partner for businesses to enhance their network capabilities and reach new heights.

Ready to take the next step? Let's connect.

General Inquiries	**Sale Inquiries**
info@trextel.com	sales@trextel.com