

# Empowering a Global, Distributed Workforce with Zero Trust Secure Access and Device Flexibility



**Industry:**  
Industrial Services

**Location:**  
Stamford, Connecticut

**Organization:**

29,000 employees and over 1,500 locations throughout North America, Europe, Australia and New Zealand

**Solution:**

Cisco Secure Access

United Rentals, Inc. is the largest equipment rental company in the world, serving construction and industrial customers, utilities, municipalities, homeowners, and more across North America, Europe, Australia and New Zealand. The company employs 29,000 workers and offers a vast fleet encompassing roughly 4,800 classes of heavy duty construction rentals, with an original equipment cost (OEC) exceeding \$20 billion.

## Balancing Act: Protecting without Disrupting

United Rentals is the world's largest equipment rental company, trusted by construction firms, industrial sites, and government facilities as a reliable partner dedicated to serving its customers 24/7. Tens of thousands of field employees – including drivers, technicians, sales reps, and logistics teams – depend on mobile devices to work in remote, non-office environments across North America, Europe, Australia, and New Zealand. 24/7 availability means keeping teams securely connected to critical tools and data anytime, anywhere. But a growing remote workforce made it increasingly difficult to deliver strong security without impacting user experience.

## Disconnections disrupted customer experience

Remote users with limited connectivity were often kicked out of OneDrive, SharePoint, or email, disrupting real-time access to files and customer data. Legacy VPN tools made it hard to reach internal systems like pricing and records. This was especially frustrating for sales reps on-site trying to finalize customer quotes – only to be delayed by 5 to 10 minutes while connecting to a VPN. These interruptions didn't just frustrate users; they disrupted customer interactions, reflected poorly on the company, and triggered a spike in help desk tickets.

## Unreliable connectivity impacted productivity

Field service technicians and drivers rely on Samsung handheld devices to manage job assignments, equipment pickups, service schedules, and preventive maintenance. But many job sites have limited or unreliable connectivity and traditional VPNs added overhead, slowed performance and caused frequent disconnections, making it harder for technicians to stay productive in the field.

## Enabling flexible device use was costly and complex

United Rentals wanted to empower remote users with the devices best suited to their roles – from rugged Samsung Galaxy handhelds to Apple tablets and Windows laptops. But providing consistent secure access across a patchwork of devices, OS versions, and environments proved costly. It also complicated policy creation, support, user training, and resulted in gaps in security enforcement.

## Closing cloud security gaps eroded user performance

Despite security controls like multi-factor authentication (MFA), cybercriminals targeted United Rentals' cloud apps with session hijacking and fake MFA requests. In response, the security team restricted access to only trusted sources, which slowed down performance for thousands of remote employees. Meanwhile, the company's Mobile Device Management (MDM) solution used a proxy for email and cloud access, but frequent software updates triggered complex re-enrollments, spiking help desk calls and leading some users to abandon email until returning to the office.

**“Three things really sold us on Secure Access. The first was the native integration with Samsung – something other providers didn't offer. Second, ease of deployment was essential to minimize friction and deliver a seamless user experience. Third, it gave us the flexibility to define continuous posture profiles so we could adapt and enforce security policy updates in real time. Other vendors simply couldn't deliver that same, powerful combination.”**

Aaron O'Hare, Director, IT Security Operations,  
United Rentals

## The Right Combination: Cisco Secure Access with Native Samsung Integration

United Rentals sought a new approach to protection that would give users fast, secure access to applications – from anywhere – without compromising security or user experience. Aaron O'Hare, IT Security Operations Director at United Rentals, led the search for a modern, zero trust solution – evaluating several Security Service Edge (SSE) vendors based on the following criteria:

- Zero trust security for both private and cloud applications to ensure only verified users and trusted devices can access sensitive resources
- Automation that delivers both robust security and a seamless user experience to improve performance, reduce IT overhead, and decrease help desk tickets
- Ease of deployment at scale across Samsung handhelds and other device types and OS versions to support tens of thousands of field and remote workers with minimal disruption

After a thorough search, O'Hare explained why Cisco Secure Access emerged as the clear front-runner. "Three things really sold us on Secure Access. The first was the native integration with Samsung – something other providers didn't offer. Second, ease of deployment was essential to minimize friction and deliver a seamless user experience. Third, it gave us the flexibility to define continuous posture profiles so we could adapt and enforce security policy updates in real time. Other vendors simply couldn't deliver that same, powerful combination."

In addition, O'Hare emphasized the value of Secure Access leveraging MASQUE, a modern protocol designed to tunnel and proxy traffic efficiently. Unlike traditional proxy and tunneling protocols, MASQUE provides a flexible and resilient foundation that secures and accelerates all internet traffic with built-in fast recovery. This ensures United Rentals' field teams get fast, uninterrupted, internet and zero trust access – even in areas with poor cellular coverage.

## **A smooth deployment and transition from Cisco Umbrella**

As an existing Cisco Umbrella user, transitioning to Cisco Secure Access was a natural next step for United Rentals. "For the team that was supporting Umbrella, the shift to Secure Access was seamless," noted O'Hare. Familiarity with Cisco's ecosystem accelerated deployment and onboarding. By combining multiple functions – Secure Web Gateway (SWG), Secure Internet Access (SIA), and Secure Private Access (SPA) – Secure Access also allowed for tool consolidation without losing visibility or control.

United Rentals completed their full Secure Access rollout in only ten weeks, bringing 29,000 global users onto Secure Internet Access (SIA) and securing 20,000 of those users with seamless, zero trust access." "The deployment has been remarkably smooth," noted O'Hare.

To date, over 13,000 Samsung devices, 13,000 iPhones, 3,500 Apple iPads, and a growing Windows fleet are live – with no major support escalations. "In most cases, the only user interaction is the initial sign-in. After that, they don't think about it – Secure Access just runs quietly in the background. That's what we love to hear."

## **Device-agnostic secure access**

With Secure Access's native integration with Samsung and Apple devices, United Rentals' users get fast, frictionless zero trust access to the resources and data they need to do their jobs. On the backend, IT can easily apply and enforce consistent, granular zero trust policies across a broader range of users and devices – no matter where they are. Now, instead of navigating VPN menus and waiting for a connection, Samsung and Apple users just tap the app and they're in.

For example, United Rentals partners closely with Samsung to enable their 13,000–14,000 drivers and field service technicians. With Secure Access, Galaxy handhelds now deliver a fully native zero trust experience. No extra VPN apps, no manual tunnels – technicians just power on their device and are securely connected to mission-critical apps like Microsoft 365, Salesforce and FAST their internal logistics application. Users now have device flexibility, able to leverage Samsung, Apple or other OS platforms as well as device types, from handhelds to laptops.

## **Continuous posture monitoring**

"Unlike some vendors that check device posture only at sign-in, Secure Access runs posture assessments continuously in the background, completely invisible to the user," noted O'Hare. "They don't have to sign in over and over. We just know we can trust that device – all the time." If suspicious activity is detected, connections can be re-authenticated or blocked automatically.

## Staying Secure, Connected, and Productive with Zero Trust Access

Since deploying Cisco Secure Access, United Rentals has seen immediate improvements across IT operations, employee productivity, and the customer experience.

### Transparency delivers a seamless user experience

Secure Access runs quietly in the background, automatically securing access to the apps users need – without forcing them to take additional steps or even notice that security is happening. The result is a smooth, consistent experience across every device and location, whether employees are working from home, visiting a customer site, or operating in the field. “The biggest compliment we can get from an end user is that they don’t know it’s there,” said O’Hare. “My measure of success is that users are no longer calling me to complain that connections are slow or they can’t perform their job. Secure Access just works.”

### Zero Trust keeps Microsoft 365 and Salesforce running smoothly

“Since using Secure Access, those previous connectivity issues have gone away entirely,” said O’Hare. The always-on, zero trust connection keeps users consistently authenticated and securely connected to Microsoft 365 and Salesforce, no matter where they are – reducing the burden on IT support

teams, improving the employee experience, and driving greater operational efficiency.

### Reliable access slashes support tickets and boosts customer visits

Before Secure Access, the average user submitted 3–5 connectivity-related tickets per month – mostly due to VPN, Microsoft 365, or Salesforce issues. “Since rollout, support tickets per user have dropped by roughly 80%. Today, a typical user averages fewer than one ticket per month, and that number typically disappears entirely after the first 30 days post-deployment,” said O’Hare. “Employees no longer call IT for help – that silence is one of the clearest indicators of our success.”

Additionally, outside reps now save 5–10 minutes per job site previously spent trying to connect to VPN. With dozens of customer visits per week, saved minutes means more meetings per day, faster quoting, and better responsiveness. “Gaining 10 minutes back per visit can mean visiting three or four more job sites daily. That’s a significant business impact.” And when reps are face-to-face with customers and every minute matters, that time savings ensures clients experience the efficiency and professionalism they expect – strengthening United Rentals’ reputation as a trusted and reliable partner.

Secure Access achieves these performance gains through faster transport, efficient inspection, and the use of the MASQUE protocol to tunnel and proxy traffic, effectively minimizing latency and connection interruptions when accessing critical resources.

**“Since rollout, support tickets per user have dropped by roughly 80%. Today, a typical user averages fewer than one ticket per month, and that number typically disappears entirely after the first 30 days post-deployment. Employees no longer call IT for help – that silence is one of the clearest indicators of our success.”**

Aaron O’Hare, Director, IT Security Operations, United Rentals

## Staying connected, even in the most challenging environments

Drivers and technicians now have persistent, secure access to Samsung FAST and other internal tools – no manual VPN logins or dropped sessions. “With ZTNA and Secure Access, there are no more complaints from remote workers that things are slow or not working. They now have fast and secure access to see priorities, run diagnostics or apply software updates on-site,” said O’Hare.

## Improved visibility and policy enforcement with DLP and AI Defense

As part of its Cisco Secure Access deployment, United Rentals is leveraging Data Loss Prevention (DLP) and AI Defense features to gain visibility and mitigate emerging risks. “We’re starting to see where and who in our user community are leveraging publicly available AI products and understand what they’re using those tools for,” said O’Hare. “That visibility is helping us secure those products more effectively and enforce granular access policies without disrupting business workflows.”

## Securing the Future Without Slowing Down

United Rentals is focused on finalizing the global rollout of Secure Access and will continue refining posture profiles while leveraging Cisco’s AI and reporting to maintain strong, proactive security across its evolving fleet. The company’s adoption of Cisco Secure Access shows that zero trust doesn’t have to slow business

down. By combining robust protection with native, frictionless integration – especially on Samsung Galaxy devices – United Rentals has strengthened its defenses, reduced support costs, and protected the 24/7 reliability that defines its brand.