SECURED COMMUNICATIONS

Securing the mission at the tactical edge

REDCOM takes a holistic, multi-layer approach to security that goes beyond typical measures such as encryption and validation. This paper addresses REDCOM's stance on overall mission security, which necessitates a strong focus on encryption, resiliency, interoperability, and ease of use.

REDCOM®

www.redcom.com

INTRODUCTION

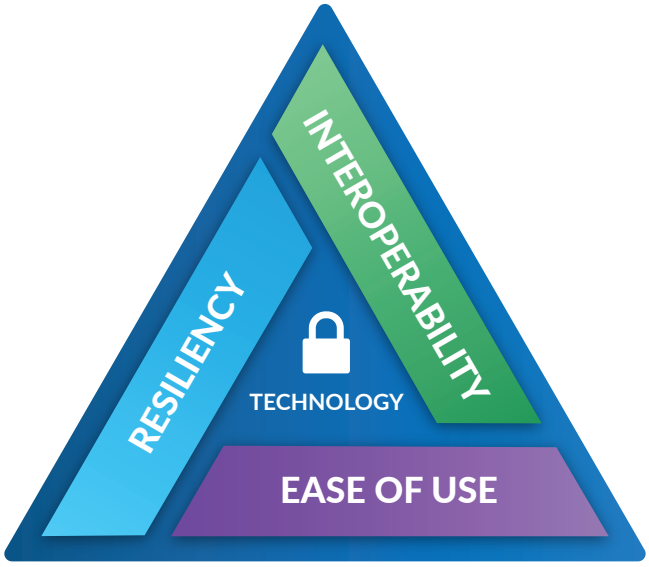
The United States armed forces are facing increased cyber capabilities from our near-peer adversaries such as Russia and China. Our adversaries fully realize how vital communication is to every facet of modern military operations, and so they are becoming more proficient in techniques such as hacking, signal jamming, and disruption.

In today's information-intense domain, security is absolutely critical to the success of the mission. But what exactly does the term "security" mean? Often when users talk about security, they use it as a synonym for technology such as encryption, authentication, and validation. REDCOM has a much broader interpretation of security because we focus on the overall **security of the mission**.

Missions can be compromised by a variety of factors, including:

- **Single points of failure.** Systems limited to a single communication medium, such as IP, become worthless if that medium fails due to a network outage or cyberattack.
- **Slow boot-up/tear-down times.** In chaotic or contested environments where agility is the key to success, systems that boot up slowly or require the user to "save" progress greatly impede the warfighter's ability to "shoot, move, communicate."
- **Interoperability challenges.** Systems that can't talk to each other open the doors for other options that may have insecure talk paths.
- **Complexity.** If a system is unintuitive or too complicated, users will seek out simpler (and possibly less secure) alternatives, or may be unable to complete the mission.

The above scenarios are clearly security concerns, and yet they have nothing to do with encryption or validation. This is why REDCOM takes a holistic, multi-layer approach to security. We take encryption, testing, and compliance seriously, and we happen to excel in this space. But we also know that mission security hinges on three other factors working together with encryption and validation: resiliency, interoperability, and ease of use. This paper addresses REDCOM's stance on the complete security spectrum to ensure mission success at the tactical edge.



TECHNOLOGY

Security often gets a bad rap for adding unwanted complexity to the product development process. It's not uncommon for security measures to be tacked on at the end as an afterthought. What's more, designers aren't typically involved with technical decisions, especially at the operations level.

— Gwendolyn Betts, Security Vs. UX: How To Reconcile One Of The Biggest Challenges In Interface Design

At REDCOM we believe security cannot be achieved through a "bolted on" approach. This is why we build security into all of our products from the start. A strong code base designed with security in mind forms the foundation for all of our military-grade solutions.

REDCOM solutions are:

- **Standards-based.** REDCOM builds our products to industry standards, which ensures interoperability with a variety of transmission paths, gateways, and endpoints. Users are never locked into proprietary end instruments.
- **Encrypted.** We invest in the latest forms of encryption, including Suite B, TLS/SRTP, and IPsec. We also allocate significant R&D efforts towards the development of next-generation encryption and authentication technologies.
- **Compliant.** REDCOM maintains compliance with numerous DISA and NIAP requirements.
- **Tested & Certified.** REDCOM meets stringent session controller functionality and interoperability requirements as defined in the Unified Capabilities Requirements (UCR). We rigorously test our products with the Joint Interoperability Test Command (JITC) to ensure our solutions are certified on the DoDIN Approved Products List. REDCOM Sigma® and the REDCOM Secure Client for Android have passed FIPS 140-2 validation testing, meaning that we can provide standardized, secure solutions for government agencies by appropriately handling SBU data.

RESILIENCY

> *Frankly, my concern is these systems may or may not work in the conditions of combat that I envision in the future with the changing character of warfare because of issues with line of sight, electromagnetic spectrum, the inability to operate on the move, the inability to operate in large, dense complex urban areas or complex terrain.*
>
> *— General Milley, Army Chief of Staff*

Resiliency refers to the ability of a system to continue operations under adverse conditions. Resiliency has always been an attractive feature of a network, but it has quickly become an essential element of mission security for warfighters at the tactical edge.

REDCOM's integrated approach delivers mission-critical command and control functionality that offsets cybersecurity concerns while enhancing network resiliency.

REDCOM solutions are:

- **Built for survivability in the field.** If the IP-based network is compromised, REDCOM technology allows the sustainment of command and control functions by merely falling back to legacy networks. This level of redundancy allows for the continuity of operations in the limited, intermittent, or denied communication environments.
- **Resilient to hard shut-downs.** REDCOM systems do not require the operator to "save" the work before shutting down, which makes our systems resilient to hard or unexpected power-off.
- **Quick to boot up.** REDCOM platforms feature extremely rapid boot times. These factors make REDCOM technology ideally suited for tactical deployments and are directly aligned with the DoD's strategy to become more agile.
- **Hardened.** REDCOM solutions can employ "hardened" components that meet the rigors of harsh tactical environments.

INTEROPERABILITY

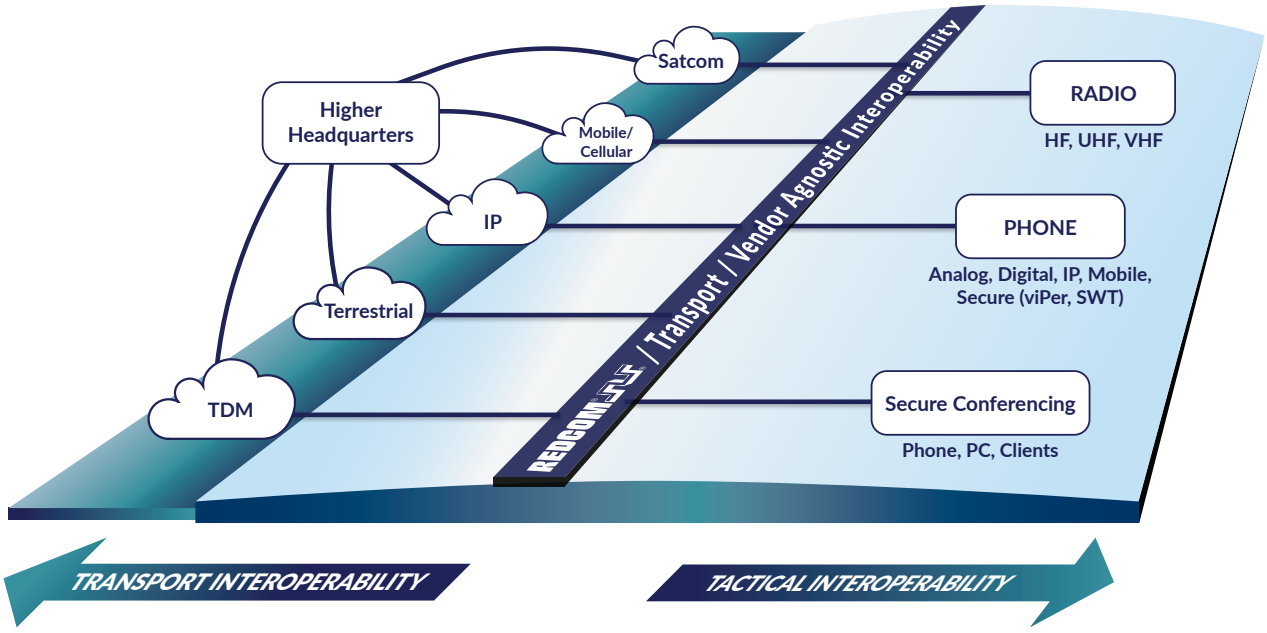
Interoperability does not necessarily require common military equipment. What is important is that this equipment can share common facilities and is able to communicate with other equipment.

— NATO document on Interoperability for Joint Operations

Military and public safety operations are typically joint, requiring the command and control systems of multiple services to work together effectively. System interoperability is a force multiplier for command and control systems. In these situations, commanders constantly consider how technology might affect the unit's ability to communicate within their jurisdiction, with neighboring agencies, and with federal partners.

REDCOM solutions align with the ongoing modernization efforts of global military and defense forces that demand interoperability with both legacy and emerging technologies. REDCOM solutions are:

- **Interoperable with coalition forces.** The lack of a single coalition network or standard has been a longtime challenge. Each environment often has different requirements, baselines, and standards to suit each partner nation's various demands, missions, and capabilities. REDCOM technology can integrate with any of these environments to deliver true interoperability between joint and coalition forces.
- **Standards-based.** REDCOM products are designed to open standards, which enables our customers to reuse existing endpoints without being forced to rip and replace. Interoperability testing — both in-house and at JITC — ensures our products maintain compatibility with both legacy and emerging technologies.
- **Technology-agnostic.** REDCOM can connect to a wide range of interfaces, protocols, and endpoints, from legacy systems (such as magneto lines) to today's over-the-top voice solutions (such as LTE and 5G). As leaders in SIP development, REDCOM can seamlessly connect various SIP networks that have different interpretations of the spec.



EASE OF USE

> *Unfortunately, our current network is too complex, fragile, not sufficiently mobile nor expeditionary, and one that will not survive against current and future peer threats, or in contested environments. We find ourselves in a position now, within a new environment and facing new challenges, where our network is not user-friendly, intuitive, or flexible enough to support our mission in the most effective manner and demands a heavy reliance on industry field service representatives to operate and sustain these systems.*
>
> *— The United States Army Network Modernization Strategy, September 2017*

At REDCOM, we understand that the less users have to think about technology, the more time they have to accomplish their mission. Warfighters do not have the luxury of time to contact tech support or wait for field service reps to solve IT issues.

REDCOM recognizes the importance of a simple and intuitive user interface that enables the warfighter to "shoot, move, communicate." The key to a superior user interface is 'Human-Centered Design' which puts the user and their specific needs at the center of every interface. Using this design philosophy, every choice we make as we develop our software requires us to investigate and open up the lines of communication between our team of designers, engineers, and testers. REDCOM actually conducts one-on-one interviews with our end users to seek their input about ways to improve our interfaces and make their lives easier.

REDCOM solutions are:

- **Extremely easy to learn.** Specialized certifications are not required to get up and running with REDCOM products. Users can learn to configure and operate our hardware and software with very little training.
- **Built for the warfighter.** Our software's web-based interface is easy to navigate, highly customizable, and quick to set up. This eliminates the armed forces' requirement for industry field service representatives.

CONCLUSION

At REDCOM, we are intensely focused on meeting the communications needs of the modern warfighter. We do this through a "brilliance in the basics" approach — we build simplicity and reliability into every product we develop, which directly translates into effectiveness at the tactical edge. We enable mission security for our government and military customers with solutions that are validated, resilient, interoperable, and easy to use.

Contact a REDCOM solution advisor today to learn more about our military-grade products, or for a demonstration of our communications technology in action.

One REDCOM Center, Victor, NY 14564 585-924-6500 sales@redcom.com www.redcom.com