news & updates September 2026 | Issue 40

In this issue:





CEO's Corner

Dear Colleague,

Radio frequency (RF) technology and cybersecurity are increasingly intertwined as wireless communications—from Wi-Fi, Bluetooth, and cellular networks to satellite feeds and IoT devices—expand the digital attack surface into the available radio spectrum.

Traditional network security focuses on protecting data at the software and protocol layers, but RF cyber threats operate at the physical layer, where rogue transmitters, signal jamming, eavesdropping, and unauthorized wireless bridging can bypass standard firewalls and security controls. Consequently, modern cybersecurity strategies must incorporate physical RF monitoring, wireless intrusion detection, and signals intelligence to identify unauthorized RF transmissions, detect hardware tampering or leakages in secure facilities, and safeguard critical wireless infrastructure against physical-layer exploitation.

Unauthorized transmitters, interference, and RF leakage from shielded spaces all warrant attention in sensitive facilities. Continuous RF monitoring helps teams spot unexpected activity and investigate it promptly. **RadGreen** offers RF monitors for this challenge, including local RadSys500 series units that operate without network, cellular, or Wi-Fi connections and provide visual and audible alerts on site. Their monitoring options span selected frequencies from 100 MHz to 40 GHz, supporting RF awareness in laboratories and secure environments without adding a network connection to the monitor.

Read on to see how RadGreen continuous RF monitoring can support and protect your facility.

Alan Lowne
CEO, Saelig Company Inc.

What's New?

Click here for Update

Contact Information

Voice: 585-385-1750
FAX: 585-385-1768
Sales: sales@saelig.com
Tech Support: support@saelig.com
Quotes: quotes@saelig.com



Promotions

Click here for Promotional Items







PROTECTING THE INVISIBLE ATTACK SURFACE BEFORE ATTACKERS REACH YOUR NETWORK

THE CHALLENGE

Organizations invest heavily in firewalls, EDR and SIEM, yet one critical attack surface often remains unmonitored: the radio frequency (RF) environment. Rogue access points, Evil Twin attacks, unauthorized wireless transmitters and RF anomalies can provide attackers with a path into the enterprise before conventional cyber defenses ever see the attack.

THE THREAT IS REAL

- MITRE ATT&CK identifies Evil Twin / Rogue Access Point attacks (T1557.004) as a recognized adversary technique.
- CISA warns organizations about wireless Man-in-the-Middle attacks and rogue access points.
- Nation-state threat groups have used wireless attack techniques during espionage campaigns.
- 2024: Australian authorities dismantled fake airport Wi-Fi operations used to steal credentials from travelers.
- Growth of Wi-Fi 6/6E/7, private 5G, Bluetooth and IoT is rapidly expanding the enterprise RF attack surface.

BUSINESS IMPACT

- Average global cost of a data breach: approximately US$4.9 million (IBM).
- 83% of organizations experience more than one breach.
- One successful RF intrusion can expose intellectual property, product designs, defense programs, customer data and manufacturing operations.

RADGREEN PLATFORM CAPABILITIES

CONTINUOUS RF MONITORING

24/7 autonomous monitoring across the RF spectrum with no blind spots between inspections.

WIDEBAND COVERAGE

100 MHz – 40 GHz coverage with selectable frequency bands.

WIRELESS THREAT DETECTION

Detects rogue Wi-Fi, Evil Twin attacks, unauthorized RF transmissions and abnormal RF power changes.

AI-POWERED ANALYTICS

Advanced algorithms identify anomalies and suspicious behavior in the RF spectrum with high accuracy and low false positives.

REAL-TIME ALERTING

Instant alerts to SOC, email, SMS or local visual/audio alarms for rapid response.

HISTORICAL INTELLIGENCE

Complete RF event logging and reporting for investigations, compliance and trend analysis.

EASY DEPLOYMENT

Maintenance-free PoE installation with minimal impact on your infrastructure.

SECURE & FLEXIBLE

Suitable for connected or air-gapped defense environments.

THREATS DETECTED

- Rogue Access Points
- Evil Twin Attacks
- Unauthorized Bluetooth Devices
- Unauthorized Cellular Devices
- Hidden Wireless Transmitters
- Unauthorized IoT Devices
- RF Reconnaissance
- Wireless Data Exfiltration
- RF Interference
- Signal Jamming
- GPS/GNSS Spoofing
- Drone Communication Signals
- Suspicious RF Activity

DESIGNED FOR CRITICAL INFRASTRUCTURE & MISSION-CRITICAL ENVIRONMENTS

- Critical Infrastructure: Power & Energy
- Water & Wastewater
- Transportation & Telecommunications
- Defense Vendors
- Aerospace Industry
- Secure Manufacturing



RF MONITORING vs. DIGITAL CYBERSECURITY

CAPABILITY	RF MONITORING	DIGITAL CYBER	WHY IT MATTERS
No access to your IT systems	✓	✗	System access exposes sensitive corporate data
Platform and vendor agnostic	✓	✗	Independent of operating systems and applications
Detects every wireless technology	✓	✗	Cellular, Wi-Fi, Bluetooth and proprietary links
Follows frequency hopping	✓	✗	Evasive transmitters digital tools rarely track
Covers any frequency band	✓	✗	Ultra-wideband, including military and niche bands
Future-proof for new technologies	✓	✗	New bands and protocols added without redesign
Cannot be disabled by the attacker	✓	✗	Keeps alerting even after a successful intrusion
No wireless emissions of its own	✓	✗	Cabled PoE sensors add no new attack surface
No human analysis required	✓	✗	Autonomous detection and alerting, around the clock
Installation effort	Minimal	High	A standard network technician installs the units
Hardware installation	Required	Sometimes	Depends on the digital security solution chosen

WHY CONTINUOUS MONITORING WINS

TRADITIONAL RF SURVEYS		RADGREEN CONTINUOUS MONITORING
Periodic manual inspections	→	24/7 automated protection
Threats often missed	→	Real-time detection
No continuous history	→	Complete RF event history
Reactive	→	Preventive
Limited visibility	→	Persistent situational awareness

EXECUTIVE TAKEAWAY

You continuously monitor your servers.

You continuously monitor your network.

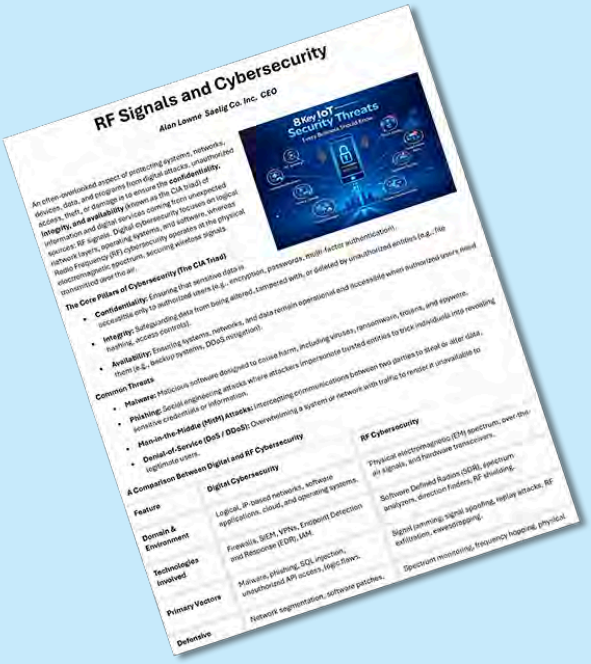
Why leave the RF layer completely unprotected?

RadGreen delivers continuous visibility into the invisible RF environment– helping security teams:

- DETECT THREATS EARLIER
- REDUCE CYBER RISK
- PROTECT VALUABLE IP
- STRENGTHEN OPERATIONAL RESILIENCE

CONTINUOUS VISIBILITY. EARLY DETECTION. STRONGER SECURITY. | THAT'S THE RADGREEN ADVANTAGE.

Click the image Below to download the pdf of "RF Signals and Cybersecurity" >


RF Signals and Cybersecurity

Alan Lowne Saelig Co. Inc. CEO

8 Key IoT Security Threats

An often-overlooked aspect of protecting systems, networks, devices, data, and programs from digital attacks, unauthorized access, theft, or damage is to ensure the CIA triad of **integrity, and availability** (known as the CIA triad) of information and digital services coming from unexpected sources. RF signals, operating systems, and software on logical network layers, digital cybersecurity focuses on logical systems, while RF cybersecurity operates at the physical Radio Frequency (RF) spectrum, securing wireless signals transmitted over the air.

The Core Pillars of Cybersecurity (The CIA Triad)

- **Confidentiality:** Ensuring that sensitive data is accessible only to authorized users (e.g., encryption, passwords, multi-factor authentication).
- **Integrity:** Safeguarding data from being altered, tampered with, or deleted by unauthorized entities (e.g., file hashing, access controls).
- **Availability:** Ensuring systems, networks, and data remain operational and accessible when authorized users need them (e.g., backup systems, DDoS mitigation).

Common Threats

- **Malware:** Malicious software designed to cause harm, including viruses, ransomware, trojans, and spyware.
- **Phishing:** Social engineering attacks where attackers impersonate trusted entities to trick individuals into revealing sensitive credentials or information.
- **Man-in-the-Middle (MitM) Attacks:** Intercepting communications between two parties to steal or alter data.
- **Denial-of-Service (DoS / DDoS):** Overwhelming a system or network with traffic to render it unavailable to legitimate users.

A Comparison Between Digital and RF Cybersecurity

Feature	Digital Cybersecurity	RF Cybersecurity
Domain & Environment	Logical, IP-based networks, software applications, cloud, and operating systems.	Physical electromagnetic (EM) spectrum, over-the-air signals, and hardware transceivers.
Technologies Involved	Firewalls, SIEM, VPNs, Endpoint Detection and Response (EDR), IAM.	Software Defined Radios (SDR), spectrum analyzers, direction finders, RF shielding.
Primary Vectors	Malware, phishing, SQL injection, unauthorized API access, logic flaws.	Signal jamming, signal spoofing, replay attacks, RF intrusion, eavesdropping.
Defensive	Network segmentation, software patches,	Spectrum monitoring, frequency hopping, physical

Check Out Our Website for Other Fine Saelig Product Offerings

For Sales and Promotions, Click Here.

Test Equipment



Automotive Test



EMC/EMI



Cables



Components



Converters



Data Loggers



Displays



Embedded



RF Shielding



RF/Wireless



Ultrasonics



circuit cellar

Inspiring the Evolution of Embedded Design.

Click Me

Click to subscribe to the Magazine and/or Newsletter

Home Magazine NEWSLETTER Research & Design Hub Insights Tech News Resources Advertise

DIGITAL EDITION NUTS AND VOLTS EVERYTHING FOR ELECTRONICS SUBSCRIPTION CLICK ME

Saelig unique electronics

www.saelig.com 1-585-385-1750



The best in world-wide unique electronics