WHITE PAPER

Achieving CMMC Compliance

How Keysight helps defense contractors secure cybersecurity compliance

KEYSIGHT

Table of Contents

The Cyber Threat

Cybersecurity is essential to the basic functioning of the US economy, data privacy, the operation of critical infrastructure, and the preservation of democratic institutions.

Several high-profile attacks, such as SolarWinds, Colonial Pipeline, and Apache Log4j, have focused attention on vulnerabilities in government and contractor information systems. The exfiltration of data from defense contractors threatens economic and national security and is a critical issue for the US Department of Defense (DOD).

The US Defense Industrial Base (DIB) provides research and development for weapons systems, subsystems, and components. It includes hundreds of thousands of companies and their subcontractors. Because of its close connections to the military and national security, the DIB faces frequent and complex cyberattacks. Malicious actors target defense contractors, including large prime contractors and smaller subcontractors.

To safeguard sensitive national security information, the DOD launched the Cybersecurity Maturity Model Certification (CMMC) program. Although DOD contracts have included cybersecurity requirements for years, the department created CMMC as a mechanism to verify that defense companies are implementing these requirements.

CMMC ensures that defense contractors and subcontractors comply with existing information protection requirements for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The program also aims to protect sensitive unclassified information at a level commensurate with the risk from cybersecurity threats.

The CMMC program went into effect on December 16, 2024, and should begin appearing in contract requirements in mid-2025 following a phased introduction.

CMMC will significantly impact the entire DIB. Are you ready?

This white paper explores cybersecurity requirements for the three levels of CMMC. It also looks at how Keysight cybersecurity and test products can help you meet your CMMC requirements at every level.

Why Keysight

- Twenty-two of the 25 top aerospace and defense contractors use Keysight.
- Over 20% of Keysight's $4.98 billion revenue in FY24 was in aerospace, defense, and government.
- Keysight customers include Lockheed Martin, BAE Systems, Boeing Leonardo, the US Naval Research Lab, and the US government.
- All Keysight network packet brokers are listed with Common Criteria, Federal Information Processing Standard (140-2) (FIPS 140-2), and Department of Defense Information Network Approved Products List (DoDIN APL).

How Keysight helps you meet CMMC requirements

Keysight, a world leader in cybersecurity testing, can help organizations meet 30 CMMC requirements across the three levels of CMMC compliance, including the following:

- Access control
- Awareness and training
- Audit and accountability
- Configuration management
- Identification and authentication
- Incident response
- Risk assessment
- Security assessment
- System and communications protection
- System and information Integrity

Keysight supports security testing requirements found in National Institute of Standards and Technology (NIST) Special Publications 800-171 and NIST SP 800-172 needed for CMMC Level 2 and CMMC Level 3.

Although CMMC Level 2 requirements align with NIST SP 800-171 Revision 2, Keysight products can also help you meet the NIST SP 800-171 Revision 3 enhancements and changes when they go into effect.

By testing the performance of your network applications and services, you can quickly identify potential issues, ensuring smooth and reliable operations.

Proactive testing is vital for resilience and security, helping you pinpoint vulnerabilities, meet compliance requirements, and improve incident response times. As cyberthreats increase and become more sophisticated, it is crucial to implement proactive security measures to safeguard your organization's sensitive data and mitigate potential risks.

As your environment becomes more hybrid and distributed, it is also important to validate performance, scalability, and robustness. Testing determines exactly how well your environment can handle growing traffic loads and adapt to changing user demands.

Keysight offers high-performance solutions with realistic application workloads, traffic mixes, dynamic payloads, threat simulation, and evasions. Our solutions replicate your environment in action and support a wide range of protocols and applications with real-world test scenarios.

Risk Assessment – How Keysight Can Help

Keysight provides a portfolio of cybersecurity products to help you meet several Risk Assessment requirements for CMMC Level 2 and Level 3. These products support a range of security requirements aligned with NIST SP 800-171 and 172.

CMMC Level 3: RA.L3-3.11.5 security solution effectiveness

Threat Simulator (as seen in figure 1) helps you assess the security efficacy of your cyber security controls and identify shortcomings. It can help you provide prioritized remediation recommendations, enabling teams to operate more efficiently while focusing on higher value work.

Figure 1. Keysight Threat Simulator

Threat Simulator complements traditional vulnerability scanning and penetration testing by providing automated, recurring assessments updated daily so you can keep up with the latest threats.

It is safe to run in a production environment, allowing for continuous assessments to proactively identify and fix vulnerabilities.

Threat Simulator proactively assesses the effectiveness of security solutions and can automate any security assessment, enabling nuanced testing and repeatability. The platform contains a comprehensive set of attack and testing scenarios and use cases. It is easy to use, has an intuitive interface, and provides visualization capabilities that make it simple to build complex attack paths. By incorporating automation, Threat Simulator enables teams to do the following:

- Conduct more simulations faster.
- Test the efficacy of security control points continuously.
- Create a more consistent security posture despite a dynamic threat landscape.

Our simulations are realistic, with exploits that target specific vulnerabilities, making the threat intelligence more relevant. Our behavioral assessments target the Common Vulnerabilities and Exposures (CVE) and validate them from the endpoint.

In addition, Keysight provides detailed remediation advice and instructions. Our recommendations provide the entire JavaScript Object Notation file with details of every Indicator of Compromise (IOC), and we provide the entire Structured Threat Information Expression bundle, plus all the relationships with the indicators.

Keysight provides network-based vendor-specific recommendations, enabling you to validate their change management lifecycle. We can also provide the signature ID applicable to the specific problem in the network.

CMMC Level 2: RA.L2-3.11.2 vulnerability scan

Keysight IoT Security Assessment (Figure 2) helps you scan for vulnerabilities in organizational systems and applications, including Internet of Things (IoT) devices. This powerful tool combines a range of vulnerability assessments, including network-based audits, industry-leading protocol fuzzing, and our new firmware analysis under an integrated user interface or REST API. This solution also includes comprehensive reporting on discovered security flaws.

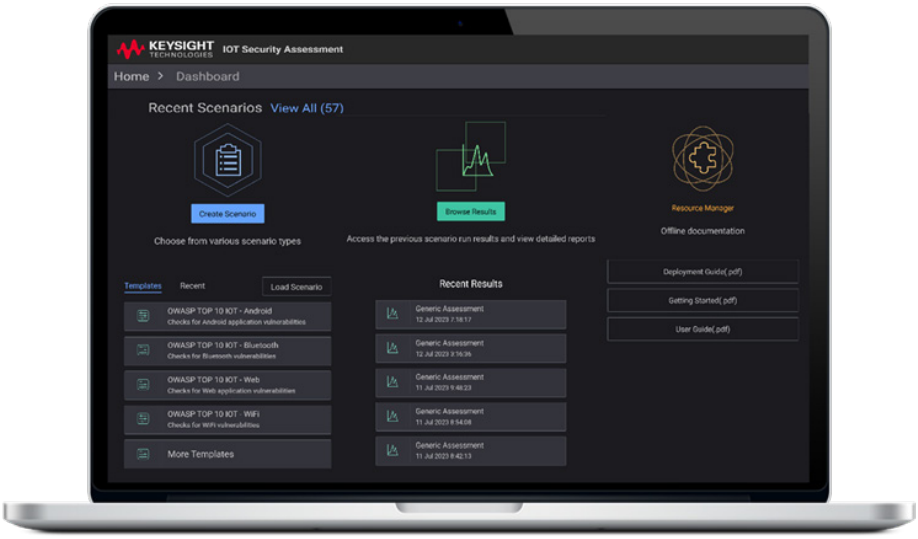

Figure 2. Keysight IoT Security Assessment

Our firmware analysis module inspects IoT device firmware, identifies third-party components, and maps them to known CVEs. It continuously monitors these components, providing daily reports on newly discovered vulnerabilities. The module also analyzes binary files in the firmware to detect potential unknown vulnerabilities in compiled C codes. Additionally, IoT Security Assessment includes network-based audits and fuzzing modules to identify IoT device vulnerabilities in a test environment.

Although this CMMC Level 2 requirement aligns with NIST SP 800-171 Revision 2 requirements for vulnerability scanning, the wide-ranging capability of IoT Security Assessment means that it can also help you meet NIST SP 800-171. The Revision 3 security requirement addresses vulnerability monitoring and scanning, and it helps with ongoing monitoring and remediation.

Discover how to protect your IoT devices from a 400% surge in malware attacks to ensure you are ready for upcoming cybersecurity standards in this solution brief.

CMMC Level 3: RA.L3-3.11.6 supply chain risk response

The firmware analysis module (Figure 3) in the IoT Security Assessment solution helps support the analysis of supply-chain risk. It also helps an organization identify IoT components that may require additional supply-chain risk mitigations. Keysight analyzes IoT device firmware, identifying Software Bills of Materials (SBOMs) and mapping them to known CVEs.

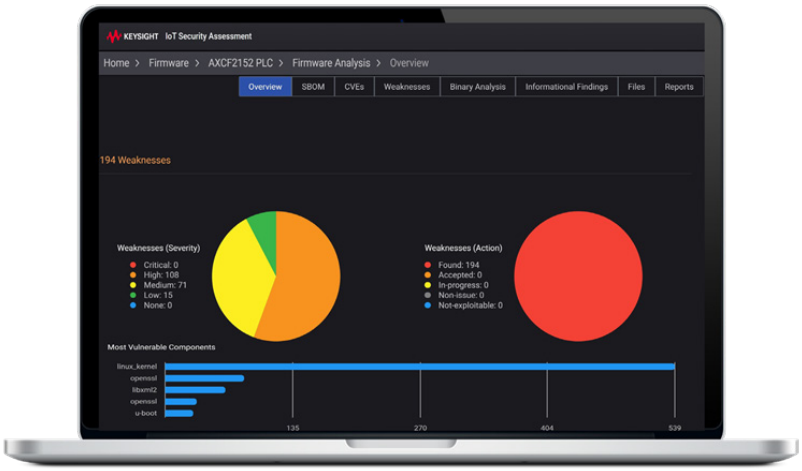

Figure 3. Keysight IoT Security Assessment

The solution identifies vulnerabilities in the device's operating code, including extracting the SBOMs and uncovering associated vulnerabilities. It detects hard-coded credentials that pose unauthorized access risks, pinpoints configuration flaws, identifies weak or expired cryptographic keys and certificates, and finds vulnerable scripts and binary code. This approach enables a comprehensive and proactive security posture assessment, ensuring that you can identify and mitigate vulnerabilities before malicious actors can exploit them.

Learn how Keysight's automated IoT firmware security analysis can uncover hidden vulnerabilities and ensure your devices meet evolving cybersecurity standards in this application note.

For more information on IoT Security Assessment visit our webpage.

Defense Contractors Should Prepare Now

The CMMC program Title 32 final rule went into effect on December 16, 2024, formally establishing CMMC as an official DOD program.

The Title 48 rule will implement the CMMC program as a requirement for DOD contracts in a phased rollout beginning in mid-2025.

Contracts requiring Level 1 CMMC will be in the first phase, expected to start in the second quarter of 2025. Level 2 CMMC will follow in 2026, although a provision in the rule gives contracting officers latitude to require the CMMC Level 2 certification earlier than that. Finally, Level 3 CMMC will occur by 2027.

The Title 48 rule incorporates CMMC into Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7021, requiring contractors to obtain CMMC certification prior to contract award.

DFARS 7021 requires all defense contractors to achieve CMMC certification at the level specified in their contract by the time of award. Failure to get certified means contractors will not be eligible for future contracts and may be in breach of existing contracts.

DIB companies outside the US must meet the same standards as US contractors. Managed security service providers offering services to defense contractors will also need to ensure they are ready to meet CMMC requirements.

It is wise to be prepared, even if you do not know the exact timing of the contractual requirement. If you wait until you see the requirement in a request for proposal, it will be too late, and there is a good chance you will not have the time to respond. Failure to certify may exclude you from desirable business, resulting in significant financial consequences.

CMMC requires that security integrators serving the US federal government as primary contractors or subcontractors be compliant if they plan to do any business with the DOD. Companies that have not already started the accreditation process should begin before they potentially lose business.

Companies may use their certification status as a competitive differentiator, particularly if they achieve the status early. The pace of contractual implementation is increasing, and contractors will regard it as a business necessity.

It will take time to prepare for a CMMC assessment, so you should start now.

Security requirements for CMMC are mapped to three maturity levels (Figure 4): Level 1 Foundational based on FAR 52.204-2); Level 2 Advanced), based on NIST SP 800-171 Rev. 2); and Level 3 (Expert), based on NIST SP 800-172.

Keysight can help you start work today. Our advanced technology can ensure that your network and security fully meet CMMC compliance.

CMMC model

	Model	Assessment
Level 3	134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual affirmation
Level 2	110 requirements aligned with NIST SP 800-171 r2	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs • Annual affirmation
Level 1	15 requirements aligned with FAR 52.204-21	• Annual self-assessment • Annual affirmation

Figure 4. Cybersecurity maturity model certification

Level 1: Foundational

This level is for organizations that only have FCI. It is based on 15 controls found in FAR 52.204-21 and requires annual self-assessment, certification, and affirmation.

Level 2: Advanced

For organizations that manage CUI, this level requires the implementation of 110 cybersecurity controls and practices found in DFARS clause 252.204–7012. This aligns with NIST SP 800-171 Rev. 2 and requires assessments every three years by a certified third-party assessment organization and annual affirmation. Triennial assessment and annual affirmation apply for select programs.

Although CMMC Level 2 requirements align with NIST SP 800-171 Rev. 2, Keysight products can also help you meet the NIST SP 800-171 Revision 3 enhancements and changes.

Level 3: Expert

This level addresses organizations with high-priority CUI. It requires them to meet all 110 cybersecurity controls from Level 2 and an additional 24 enhanced practices based on a subset of NIST SP 800-172. Level 3 requires government-issued assessments every three years and annual affirmation.

How Keysight Can Help You at Every Level of CMMC

Domain	Practice no.	Requirement name	CMMC level	Keysight support	Keysight product
Access control	AC.L2-3.1.3	Control CUI flow	2	◐	CyPerf
Awareness and training	AT.L2-3.2.2	Role-based training	2	●	Cyber Range
Awareness and training	AT.L3-3.2.1	Advanced threat awareness	3	●	Cyber Range
Awareness and training	AT.L3-3.2.2	Practical training exercises	3	●	Cyber Range
Audit and accountability	AU.L2-3.3.1	System auditing	2	◐	Network packet brokers
Audit and accountability	AU.L2-3.3.7	Authoritative time source	2	●	TimeKeeper

Legend: ● – Keysight can address; ◐ – Keysight can partially address.

Domain	Practice no.	Requirement name	CMMC level	Keysight support	Keysight product
Configuration management	CM.L2-3.4.4	Security impact analysis	2	●	BreakingPoint, Threat Simulator, and CyPerf
Configuration management	CM.L3-3.4.1	Authoritative repository	3	◐	Threat Simulator
Configuration management	CM.L3-3.4.2	Automated mechanisms to detect misconfigured or unauthorized components	3	●	Threat Simulator
Configuration management	CM.L3-3.4.3	Automated inventory	3	●	Network packet brokers
Identification and authentication	CM.L3-3.5.1	Bidirectional authentication	3	●	CyPerf and Keysight Eggplant
Incident response	IR.L2-3.6.1	Incident handling	2	●	Threat Simulator, Keysight Cyber Range, and our Flyaway Kit equipped with packet brokers and network taps
Incident response	IR.L2-3.6.3	Incident response testing	2	●	Threat Simulator and Keysight Cyber Range
Incident response	IR.L3-3.6.1	Security operations center	3	◐	Threat Simulator, Keysight Cyber Range, and network packet brokers
Incident response	IR.L3-3.6.2	Cyber incident response team	3	◐	Threat Simulator and network packet brokers
Risk assessment	RA.L3-3.11.1	Vulnerability scan	2	●	IoT Security Assessment
Risk assessment	RA.L3-3.11.1	Threat-informed risk assessment	3	◐	Threat Simulator
Risk assessment	RA.L3-3.11.2	Threat hunting	3	●	Threat Simulator and network packer brokers

Legend: ● – Keysight can address; ◐ – Keysight can partially address.

Domain	Practice no.	Requirement name	CMMC level	Keysight support	Keysight product
Risk assessment	RA.L3-3.11.5	Security solution effectiveness	3	●	Threat Simulator, CyPerf, and BreakingPoint
Risk assessment	RA.L3-3.11.6	Supply-chain risk response	3	◐	IoT Security Assessment
Security assessment	CA.L2-3.12.1	Security control assessment	2	●	Threat Simulator and CyPerf
Security assessment	CA.L2-3.12.3	Security control monitoring	2	●	Threat Simulator and network packet brokers
Security assessment	CA.L3-3.12.1	Automated penetration testing	3	●	Threat Simulator
System and communications protection	SC.L1-b.1.x	Boundary protection (FCI)	1	●	Network packet brokers
System and communications protection	SC.L2-3.13.1	Boundary protection (CUI)	2	●	Network packet brokers
System and information integrity	SI.L1-b.1.xii	Flaw remediation (FCI)	1	●	Threat Simulator
System and information integrity	SI.L2-3.14.1	Flaw remediation (CUI)	1	●	Threat Simulator
System and information integrity	SI.L2-3.14.6	Monitoring communications for attacks	2	●	Network packet brokers
System and information integrity	SI.L3-3.14.3	Specialized asset security	3	◐	Industrial network packet brokers and taps
System and information integrity	SI.L3-3.14.3	Threat information related to specific threats (for example, TTPs)	3	◐	Threat Simulator and Application Threat Intelligence

Legend: ● – Keysight can address; ◐ – Keysight can partially address.

Spotlight: Awareness and Training with Cyber Range

Keysight gives security professionals access to hands-on cyber skills and enables them to test an organization's security posture.

CMMC Level 3: AT.L3-3.2.2 practical training exercises

Keysight Cyber Range (Figure 5) delivers practical exercises tailored to the tactics, techniques, and procedures (TTP) of the threat, helping you meet CMMC requirements and prepare your workforce. By providing a secure environment, teams can work together and respond to attacks without threatening real-world production sites, networks, or users.

The Keysight platform offers a simulated, hyper-realistic, live-fire cyber range with gamification and capture-the-flag scenarios. It is customizable, enabling you to create your own content for your team, and includes tools to monitor and evaluate team members' progress over time.

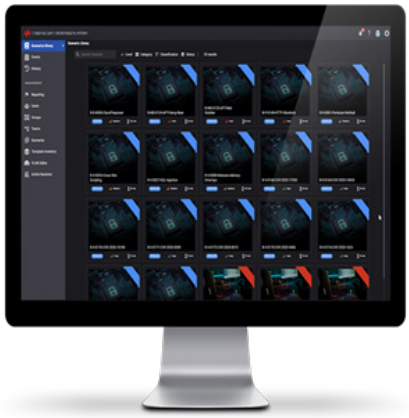

Figure 5. Keysight Cyber Range

Cyber Range provides the most effective methods for training your personnel to defend against cyberattacks. The virtual environment provides simulated real-world attacks that test multiple dimensions and engage stakeholders in diverse environments.

Explore how the Keysight Cyber Range solution can equip your security team with hands-on skills to tackle real-world cyberthreats and close the cybersecurity skills gap. For more information on Cyber Range, review this.

Spotlight: Identification and Authentication with CyPerf

Keysight provides an instantly scalable zero-trust test solution for distributed clouds.

CMMC Level 3: IA.L3-3.5.1 bidirectional authentication

Keysight CyPerf (Figure 6) proactively tests your identification and authentication requirements to ensure that your security policies work as they should. CyPerf validates security efficacy in distributed and hybrid networks while proactively testing legitimate users, restricted users, and malicious users. By safely assessing complex security environments such as zero-trust networks and associated next-generation firewalls, CyPerf helps assess whether the right users with the right privileges have access to the right applications.

For more information on CyPerf, visit our web page.

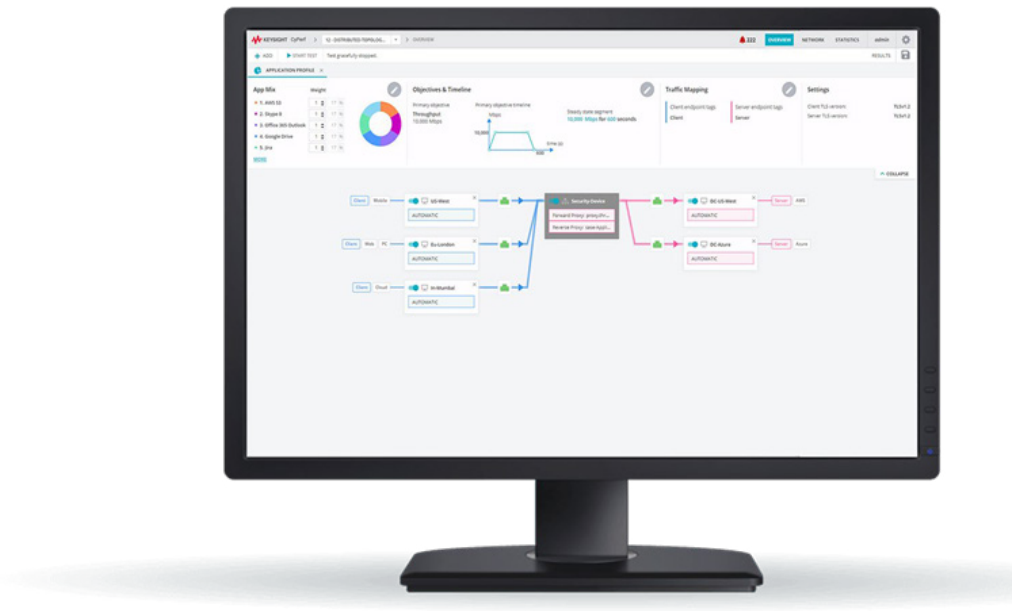

Figure 6. Keysight CyPerf

Spotlight: Proactive Security Assessment with Threat Simulator

The Keysight platform, supported by a dedicated team of researchers, helps you monitor your systems and simulate threats to stay ahead of cybercriminals.

CMMC Level 2: CA.L2-3.12.3 security control monitoring

Keysight Threat Simulator (Figure 7) helps you meet monitoring requirements to ensure the continued effectiveness of security controls. With the latest automation, Threat Simulator helps you continuously test security defenses. The level of detail in remediation guidance enables you to easily generate reports about assessments and remediation suggestions. Integration with numerous platforms and leading security information and event management solutions ensures that monitoring and specific remediation suggestions are simple to accommodate with Threat Simulator.

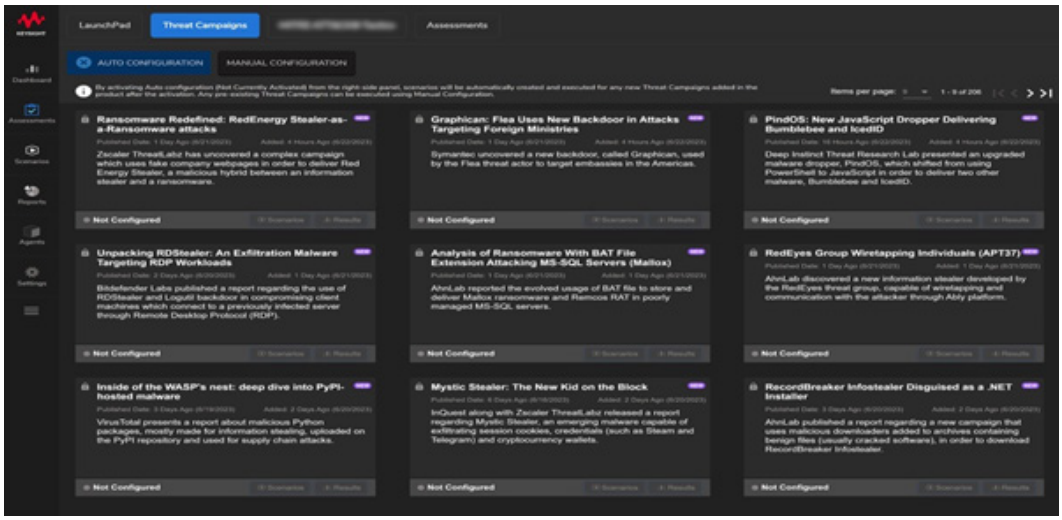

Figure 7. Threat Simulator

In today's ever-evolving cybersecurity landscape, merely being aware of new threats is no longer sufficient to safeguard your most valuable assets: your people, data, and reputation. Our expert team at the Keysight Application and Threat Intelligence (ATI) Research Center is constantly on the lookout for new threats. Our threat intelligence-gathering capabilities enable us to create simulations of new vulnerabilities within hours of their discovery.

We have thousands of simulations to help you test your security controls with the latest threats. These carefully crafted simulations replicate real-world scenarios, enabling you to test your controls manually or automatically. Testing helps you ensure that your security posture is ready and well-prepared, armed with identifiable IOCs. Our solution also offers the ability to filter and prioritize threats based on your specific regional and industry preferences. This tailored approach enables you to focus on the threats that matter most to your organization.

For more information on Threat Simulator, visit our web page.

Spotlight: System and Information Integrity with a Network Packet Broker

Keysight Network Packet Brokers (NPB), seen in Figure 8, help you monitor your communications for attacks.

Your monitoring infrastructure might feature network and application performance monitors, data recorders, and traditional network analyzers. Your defenses may leverage firewalls, intrusion prevention systems, Data Loss Prevention (DLP), anti-malware, and other point solutions.

Regardless of how specialized your security and monitoring tools are, they all have two things in common:

- They must know exactly what is happening in the network.
- Their output is only as good as the data they receive.

An NPB resides downstream from taps and SPAN ports. It collects packets from multiple locations in the network and efficiently delivers data of interest to analysis tools.

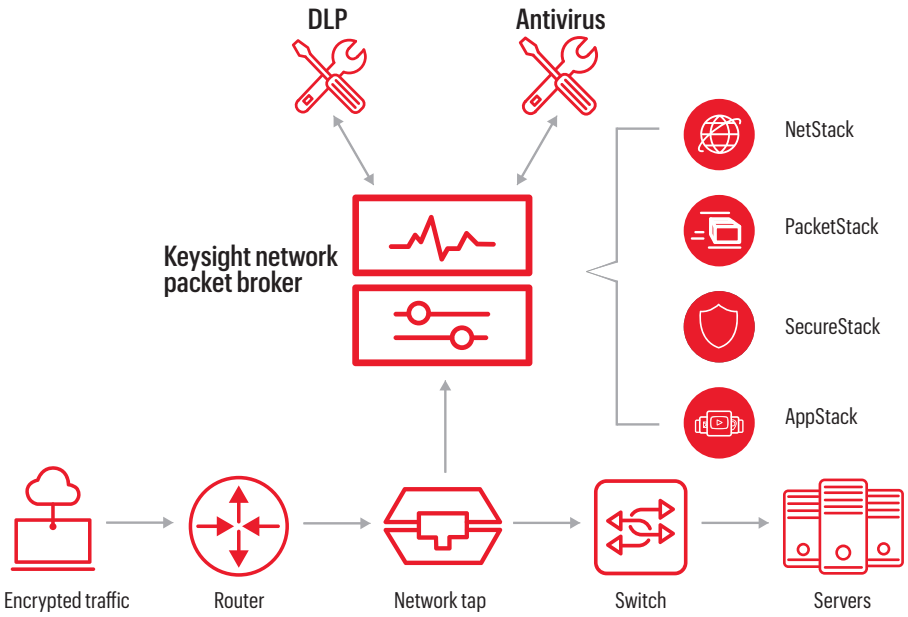

Figure 8. Keysight network visibility hardware and software components.

CMMC Levels 2 and 3 require the highest standards of security integrity from government agencies, military, contractors, and subcontractors. That is why Keysight NPBs are listed with Common Criteria, FIPS 140-2, and DoDIN APL. Keysight can help you meet NIST 800-171 Rev. 2 and 800-172 requirements, including system and information integrity, by keeping your networks safe.

Visit the Keysight visibility solutions and government certifications page to learn more.

Why the Aerospace and Defense Industry Chooses Keysight

Keysight, an S&P 500 technology company headquartered in California, is committed to helping customers and partners achieve CMMC 2.0 compliance. Founded in Silicon Valley as Hewlett Packard, Keysight is a large and established US company with corporate roots dating back to 1939.

FY24 total revenue was more than $4.98 billion, with over 20% coming from the aerospace, defense, and government. This sector continues to be a major focus for Keysight as we help modernize defense technology, electromagnetic spectrum operations, radar, security, and satellite solutions.

Keysight's 15,000 employees include a large security and professional services group with deep industrial expertise in government and defense. As an expert in security with a distinguished record in security excellence of more than 20 years, the Keysight global Application and Threat Intelligence (ATI) Research Center stays on top of the latest vulnerabilities.

Aerospace and Defense (A&D) are the backbone of modern commercial innovation. The internet, wireless communications, satellites, space, navigation, and electrification all evolved from A&D. Pushing the boundaries of technical limitations requires a combination of in-depth knowledge and imagination to explore new possibilities. Keysight fuels leading-edge technology innovations in A&D that enable commercial applications, opening new areas of innovation in A&D.

Keysight has a long history in A&D, providing chipset design and manufacturing, device development, networking and operations design, network performance monitoring, and security.

Keysight's diverse and broad portfolio delivers customized design, emulation, network, IoT, and security visibility and test solutions that span a range of areas (Figure 9). Keysight solutions deliver everything from secure military communications to 5G and beyond, enabling engineers to push the limits in space and satellite communications, radar, avionics, electronic warfare, and signals intelligence while withstanding harsh environments in the field. Keysight also provides complex signal generation and analysis for electromagnetic spectrum operations, spectrum monitoring, and signal analysis for military intelligence and homeland security.

Keysight services for Aerospace, Defense, and Government

Communications	RF	Government research
Cybersecurity	EW / radar	5G / 6G
Tactical radio	Space / satellite	Quantum
Visibility / intercept	NTN	Energy EV
Spectrum monitoring and signal analysis	Advanced emulation and design (digital twin)	

Figure 9. Keysight portfolio for aerospace and defense.

- Advances digital transformation of defense workflows and mission-critical operation.
- Enables sovereign investments in technology and research.

> Lockheed Martin is leveraging our expertise in the commercial sector to rapidly and affordably scale, adapt and integrate 5G technology in mission-critical operations across land, sea, air, space, and cyber domains. Keysight's end-to-end 5G test platforms allow us to develop customized solutions that meet the stringent requirements of the defense industry.
>
> Dan Rice, Vice President, 5G.MILPrograms, Lockheed Martin

Conclusion

Start the certification process today and let Keysight help you test your network and security to determine whether your security posture meets the requirements.

With a long-standing and rich history in the aerospace, defense, and government sectors, Keysight has dedicated itself to safeguarding sensitive information and vital government contracts. US government contractors should take the necessary compliance steps today to ensure continued DOD business.

For more information, contact us.

Keysight is your partner for CMMC compliance.