

# **Enterprise-Grade Cyberthreat Protection for SMBs in the Defense Industrial Base (DIB)**

WHITEPAPER

## OVERVIEW

Small-to-medium-sized businesses (SMBs) supporting America's national security and economic interests are on the frontlines of an active cyberwar. They face highly advanced, nation-state adversaries and cybercriminals who seek to steal, extort or disrupt.

Seventy-six percent of SMBs report that experiencing at least one cyberattack and 86% feel they lack adequate protection to defend themselves from future attacks. SMBs supporting America's Defense Industrial Base (DIB) and Critical Infrastructure (CI) uniquely at risk, face motivated and highly advanced nation state cyberthreats that seek to steal their innovation.



Department of Defense (DoD)-driven compliance requirements such as CMMC aim to address this risk by requiring SMBs in the DIB to significantly improve their cyber protection and defense capabilities. These requirements, and the advancing external threat environment, will require SMBs to advance beyond basic threat protection measures. SMBs need to extend their protection by adding layers of defense to realize secure maturity operations - historically a human-heavy and tech-heavy investment few can afford.

RADICL protects SMBs by delivering managed security operations via its AI-powered Xtended Threat Protection (XTP) Platform. With RADICL XTP, endpoints are protected, attack surfaces shrink, and intrusions are quickly detected and mitigated. RADICL becomes the security operations team, delivering extended threat protection as a turn-key managed offering. RADICL fortifies cybersecurity maturity, ensures compliance requirements are met, and protects SMBs from the extended threat landscape that includes nation-state actors seeking to steal inventions and disrupt operations.

\*Connectwise; State of SMB Cybersecurity 20222

\*\*Accenture; 'The state of cybersecurity resilience', 2021

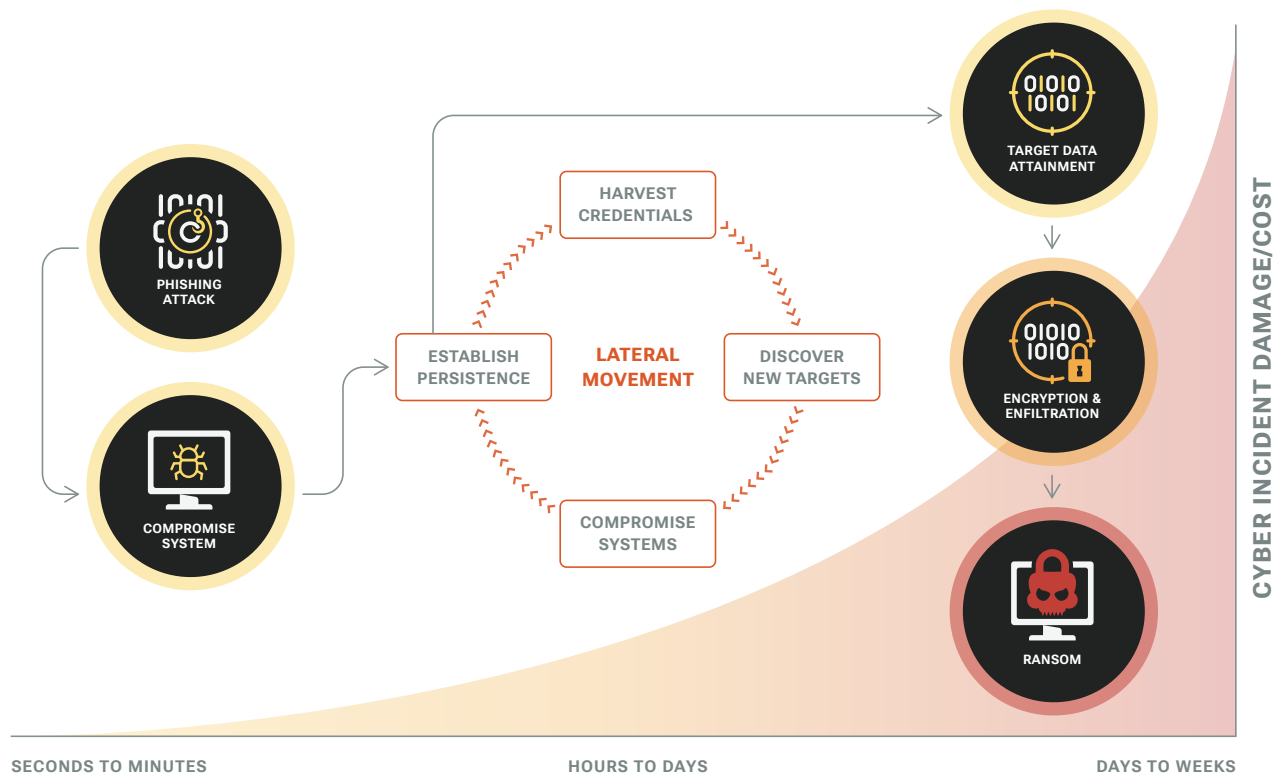
## THE NEED FOR EXTENDED THREAT PROTECTION

The unfortunate reality is that network and systems compromises happen—and will continue to happen. IT is complex. Businesses move fast. People make mistakes. Threat actors will continue to capitalize on these realities and, for the foreseeable future, there will be no absolute protection against successful intrusions and compromises. What can be prevented, however, are intrusions that become cyber incidents that damage businesses and brands.

Unmitigated intrusions are costly and ultimately lead to data theft, operational disruption, financial fraud, or extortion through ransomware. However, most headline-making cyber incidents could have been prevented by quickly detecting and controlling the initial intrusion. When intruders are given time to persist, they will compromise additional systems and user accounts until their ultimate target is obtained.

Ideally, intrusions are avoided in the first place. This requires effective attack surface management, to understand and address the technological and operational weaknesses attackers leverage to gain a foothold in the environment and expand their presence.

The below graphic illustrates a typical ransomware incident. Regardless the type of threat, almost all incidents unfold in a similar way. The threat actor compromises an initial system, goes unnoticed and establishes backdoor persistent access to the environment. If left undiscovered, they start expanding their foothold by moving laterally, leveraging harvested credentials, and compromising additional systems. This pattern continues until the threat has obtained its target. If the threat is ransomware, data is typically exfiltrated and encrypted, after which ransom can be demanded.



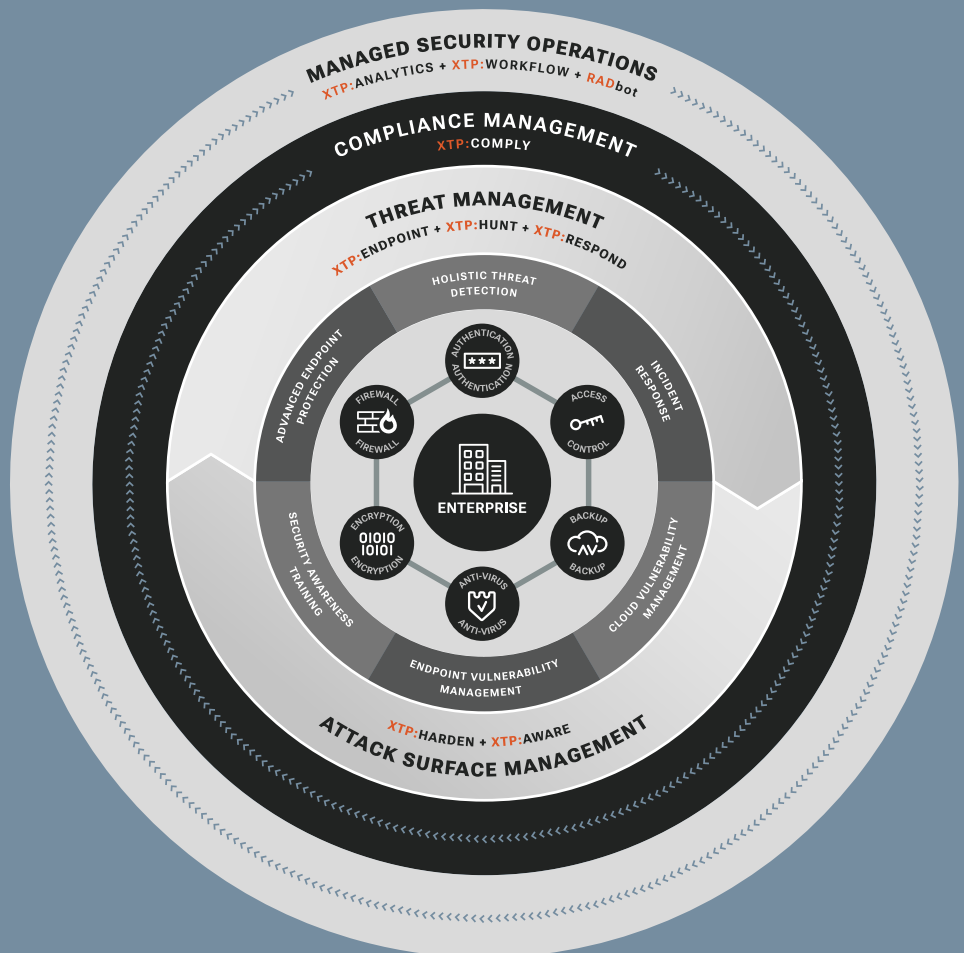
Ransomware, data theft, and other damaging incidents are avoided via rapid detection through active attack surface management.

Reliably detecting intrusions, quickly mitigating them when they occur, and continuously shrinking the attack surface is what RADICL refers to as extended threat protection. The goal is to ensure an organization is protected from all cyberthreats across the entire IT landscape, including cloud. RADICL's Xtended Threat Protection (XTP) goes beyond basic threat protection to provide additional layers of defense. In its fullest maturity, extended threat protection is realized when the following can be technologically and operationally achieved:

- Deploying and managing advanced endpoint protection.
- Hunting for evasive and embedded threats.
- Responding to potential incidents 24/7.
- Identifying vulnerabilities and guiding remediation efforts.
- Providing your employees with security awareness training.
- Ensuring general IT security best practices are in place via guided compliance adherence.

Attaining extended threat protection is a daunting effort typically only achievable by large enterprises. The hefty cost of deploying the necessary technologies (e.g., SIEM, SOAR, EDR) combined with staffing needs has been out of reach for the SMB.

RADICL's cost-effective, managed XTP offerings are designed to quickly mature your cybersecurity posture, address compliance needs, and when appropriate, defend against highly capable and motivated nation-state adversaries.





## RADICL XTP OFFERINGS

RADICL XTP subscriptions are priced based on the number of **protected people** and **protected machines**.

- A **protected person** is an employee or long-term contractor who leverages the IT infrastructure daily. They have a login and an email address.

- A **protected machine** is a system or device where XTP:ENDPOINT will be installed, including Windows/Mac workstations/laptops and Windows/Linux physical, virtual, and cloud servers.

	PRODUCT	DESCRIPTION	PRICING
XTP: CORE	XTP:ENDPOINT	Deployment and management of CrowdStrike Falcon, the leading enterprise-grade endpoint protection and detection platform.	 PER PROTECTED MACHINE
	XTP:HARDEN	Identification of vulnerabilities via CrowdStrike Falcon Spotlight and prioritized management of patch remediations.	
	XTP:HUNT	Automatic and manual (i.e., via hunting) detection of known and novel (e.g., zero-day) attacks across the IT environment.	 PER PROTECTED PERSON
	XTP:RESPOND	24x7 monitoring of threat indicators and alarms with managed qualification, investigation, containment, and incident response support.	
	XTP:AWARE	Knowledge and exercise-based training of employees to reduce targeted attack (e.g., phishing), system compromise, and fraud.	
		XTP:COMPLY	Expert-based guidance and tracking of compliance requirements, ensuring audit preparedness and compliance adherence for CMMC Level 1 & 2, and NIST 800-181.

## PROTECTION DELIVERED

RADICL XTP is designed to protect customers from all classes of cyberthreats and their resultant incidents. Regardless the type of threat, successful attacks will be avoided or quickly discovered. Following are some specific types of cyberthreats and risks RADICL XTP protects against.



### RANSOMWARE

It's a known fact that the deployment and (expert) configuration of advanced endpoint protection significantly reduces the risk of ransomware installation. **XTP:ENDPOINT** has you well covered here. In the event ransomware does get through, **XTP:HUNT** will quickly identify any signs of infestation or lateral movement. **XTP:RESPOND** will quickly neutralize the ransomware before it can do any real damage.

### PHISHING

Employees will make mistakes. RADICL **XTP:AWARE** will help reduce and prevent them. Security awareness training and phishing simulations significantly reduce the risk of employee mistakes becoming compromises. However, if a mistake is made, RADICL **XTP:ENDPOINT** will block the installation of known malware. **XTP:HUNT** and **XTP:RESPOND** provide extra layers of defense against highly advanced, custom malware.



### EMAIL AND ACCOUNT COMPROMISE

**XTP:AWARE** provides knowledge and exercise-based employee training to reduce the probability of targeted attacks (e.g., phishing), system compromises, and fraud exposure. From ongoing training on cybersecurity concepts and best practices to simulated phishing attacks, employees improve their personal and professional cyber hygiene and learn how to spot and avoid attacks used against them.

### DATA THEFT

Data theft and exposure can forever damage your brand and market competitiveness. Threats that have compromised the perimeter will masquerade as internal users. Employees or contractors can go rogue or be manipulated. **XTP:HUNT** ensures suspicious user and data activity gets noticed. **XTP:RESPOND** ensures incidents are quickly mitigated before damage is done. **XTP:HARDEN** and **XTP:AWARE** significantly reduce the risk of incidents ever occurring at all.

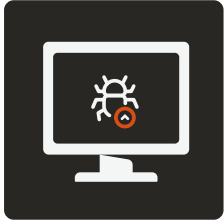


### FINANCIAL FRAUD & EXTORTION

Cyber-related financial fraud is harder than ever to detect as threats leverage AI to better impersonate executives and employees. **XTP:AWARE** helps prevent employees from being fooled and manipulated. **XTP:HUNT** monitors email and user activity for suspicious activity. **XTP:RESPOND** ensures suspected fraud is immediately investigated and stopped before wires get sent.

### COMPLIANCE FAILURE

**XTP:COMPLY** helps guide the compliance journey to ensure preparedness at audit time. Expert-driven workflows ensure incremental and continuously-improved compliance posture. Compliance dashboards provide leadership with real-time visibility into current compliance posture and risks.



### ADVANCED PERSISTENT THREATS (APTS)

Nation-state-sponsored threats - typically referred to as Advanced Persistent Threats, or APTs - are the highest class of threat adversaries. They will leverage all available attack methods and persistently attack until they succeed. RADICL XTP's fullest arsenal of current and future capabilities is designed to protect against this class of adversary. Our complete set of capabilities makes it increasingly difficult for an APT to find footing, take ground, and stay hidden.

## SECURE AND COMPLIANT

RADICL **XTP:COMPLY** accelerates and helps ensure regulatory compliance adherence, taking the guesswork and pain out of being compliant.

RADICL directly addresses many of the hardest-to-meet requirements. For all other requirements, it provides guided steering to incrementally bring an organization into complete compliance.

These requirements typically demand cybersecurity-specific technologies operated by cybersecurity experts. The cost of procuring, integrating, maintaining, and operating these technologies is typically cost prohibitive for most SMBs.

**90**

Days to CMMC Level 1  
Readiness

**30**

CMMC Level 2 Controls  
Fully or Partially Addressed  
via RADICL XTP

**100%**

CMMC / NIST 800-171  
Controls Managed to  
Adherence

RADICL's **XTP:COMPLY** provides visibility into the current state of all requirements and controls for its supported compliance mandates.

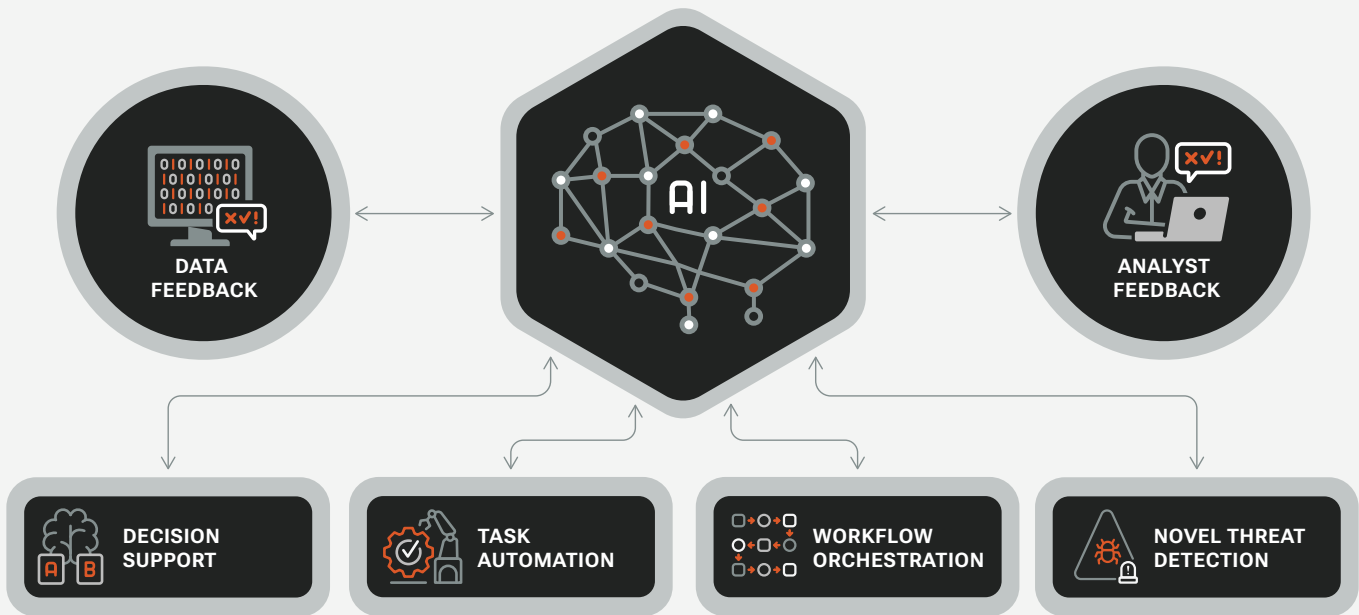
## THE RADICL XTP PLATFORM

RADICL has created a purpose-built platform to deliver extended threat protection as a turn-key managed offering, ideally suited for SMB customers. The platform has been intentionally designed to harness the power and potential of AI. Through the application of AI, RADICL continuously improves the speed and efficiency of its cybersecurity operations. This is critical to maintain affordability while delivering enterprise-grade protection from nation-state threat actors.

RADICL's AI-augmented XTP Platform continuously learns from data and human-driven workflows to improve analytics accuracy and automate service delivery capabilities. As the AI learns, it will assume and automate 90%+ of manual workflows, ensuring speed of response can outpace speed of threat.

### PERVASIVE APPLICATION OF AI

The application of Artificial Intelligence (AI) is critical across the whole of our platform to improve the accuracy of decisions, to automate actions, and to detect extremely advanced threats. Security operations and threat detection must move from human speed to software speed. Adversaries aren't slowing down, neither will RADICL.



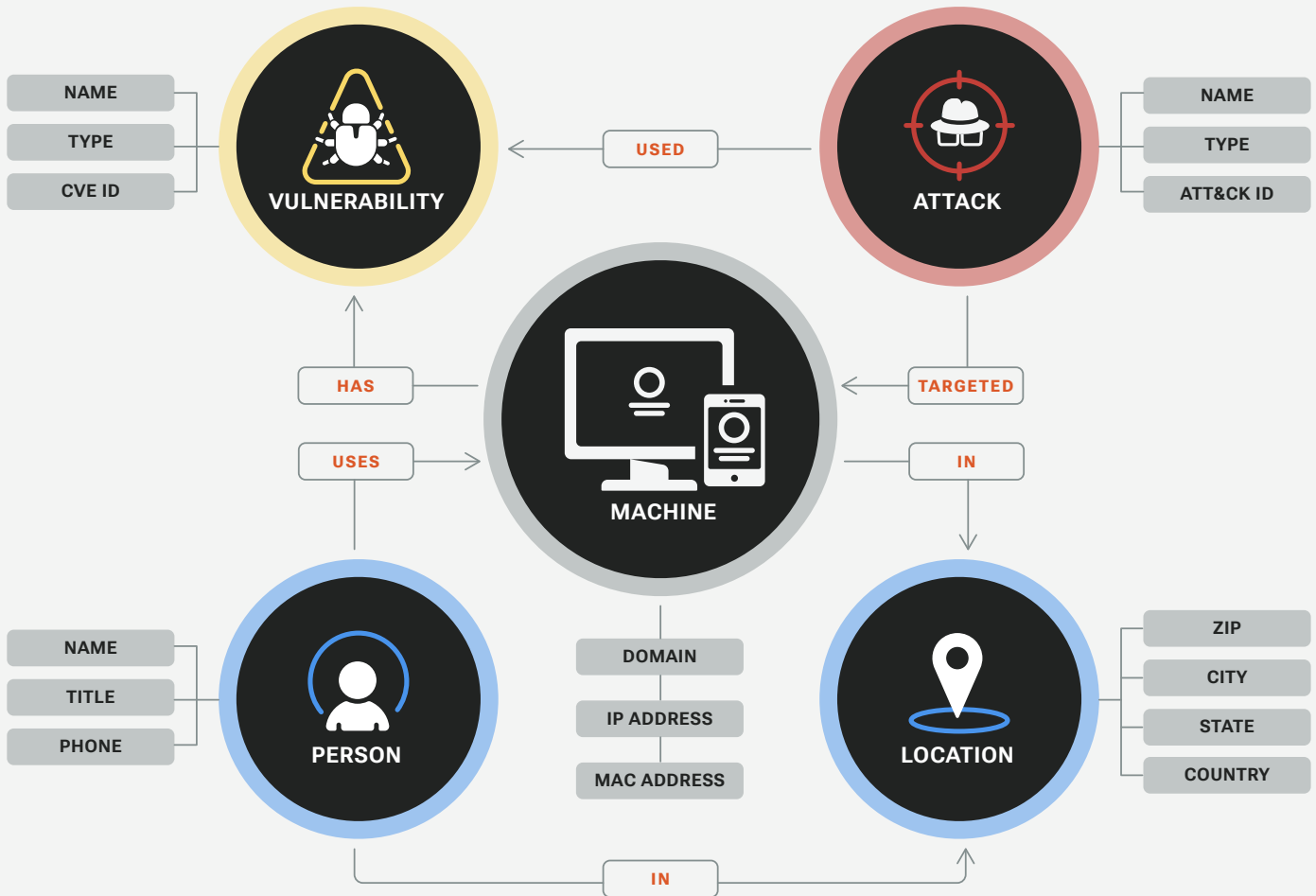
### KEY CAPABILITIES & BENEFITS

- AUTONOMOUS WORKFLOW EXECUTION
- NOVEL (e.g. ZERO-DAY) THREAT DETECTION
- ACCELERATED THREAT RESPONSE
- PREDICTIVE THREAT ANALYTICS



**INTELLIGENCE STARTS WITH DATA QUALITY**

Data quality is paramount to harness the fullest potential of AI and automation. The RADICL XTP Platform rests on novel and proprietary Entity Oriented Data Fabric. This technology allows all collected data and intelligence to be represented in the context of the involved “Entities.” A data fabric underlies all XTP Platform capabilities to enable the unrivaled application of AI, automation, and workflow efficiency.

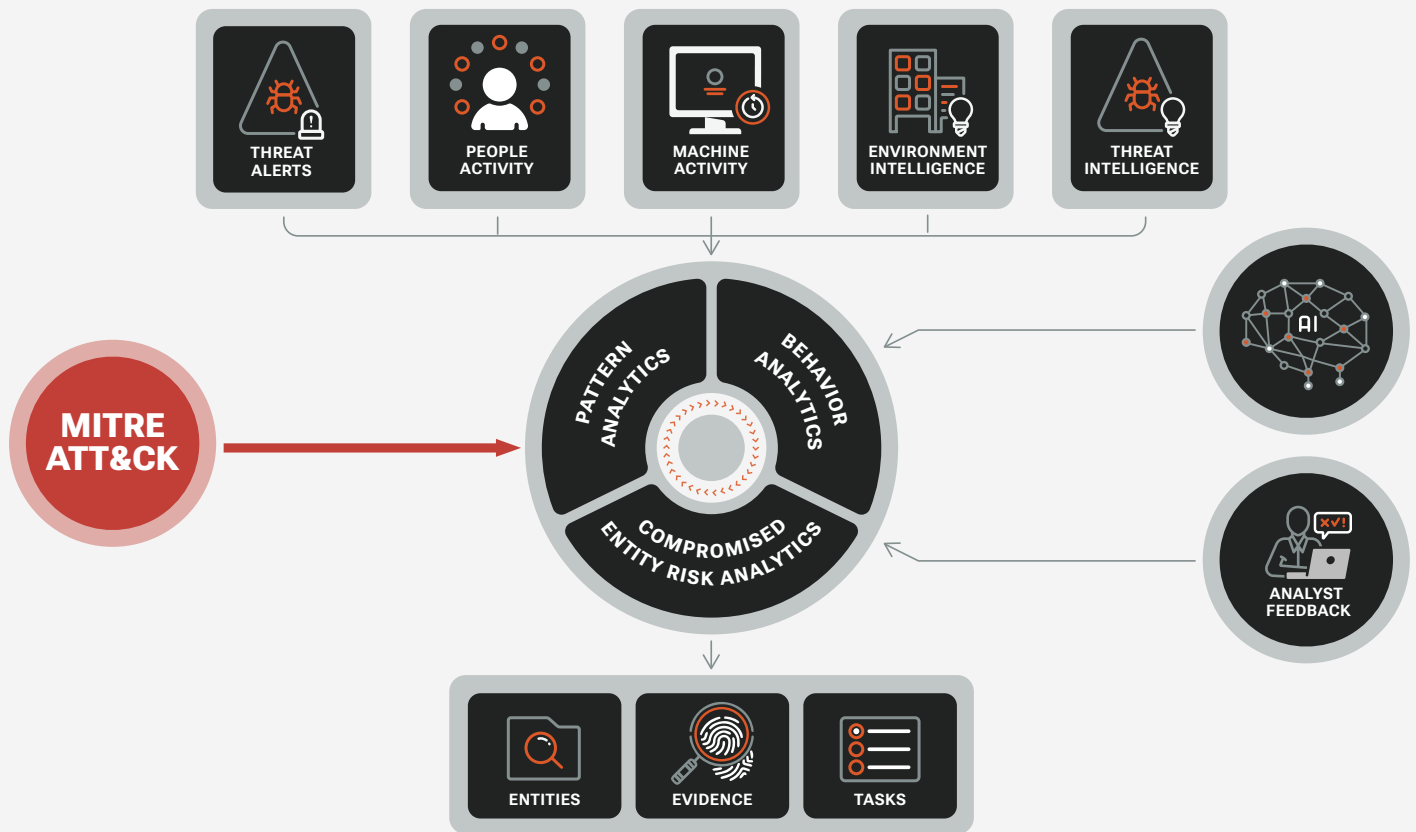


**KEY CAPABILITIES & BENEFITS**

- IMPROVED DATA COMPREHENSION
- FASTER DECISIONS AND WORKFLOW
- INCREASED AUTOMATION POTENTIAL
- INCREASED AI POTENTIAL

## MULTI-METHOD THREAT DETECTION

The RADICL XTP Platform uses a combination of pattern and behavioral analytics models to automatically detect both known and novel (e.g., zero-day) attacks, delivering extended visibility into all attack vectors. Threat hunting is supported by the proprietary RADICL Query Language (RQL). RQL provides an easy to use, yet extremely powerful search experience that allows analysts and AI to hunt in the context of Entities and their relationships, driving faster and more accurate decisions.



### KEY CAPABILITIES & BENEFITS

- EXTENDED THREAT DETECTION
- MORE EFFECTIVE THREAT HUNTING
- FASTER INVESTIGATIONS
- FASTER RESPONSE

## CASE MANAGEMENT

RADICL XTP’s embedded Case Management ensures all threat indicators and incidents are tracked to completion. All workflows are designed to optimize analyst speed and accuracy, with ever-increasing application of AI-driven automation. All activity and evidence is tracked for full transparency and effective collaboration across RADICL analysts and protected clients.

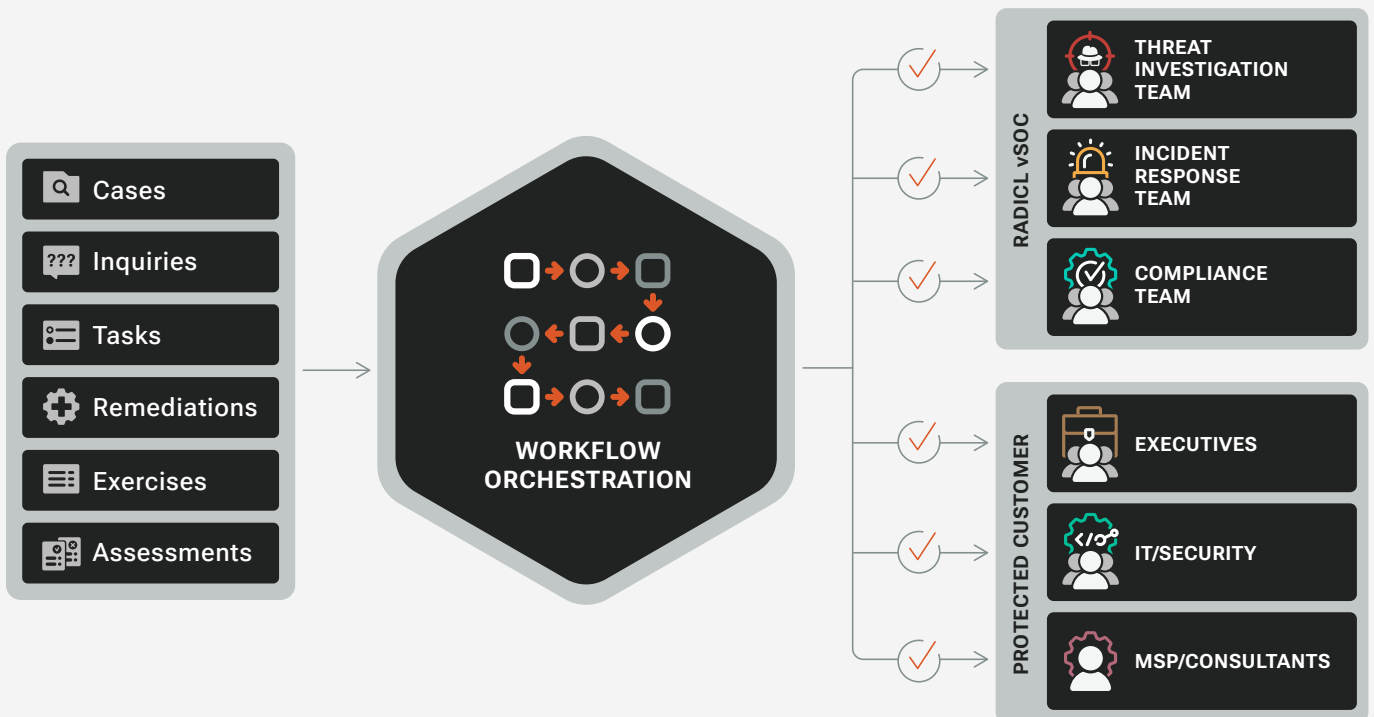


### KEY CAPABILITIES & BENEFITS

- FAST INVESTIGATIONS
- COMPLETE INCIDENT RESPONSE
- REAL-TIME VISIBILITY INTO THREATS AND INCIDENTS
- CHAIN-OF-CUSTODY AND ACTIVITY AUDITING

## MANAGED SECURITY OPERATIONS WORKFLOW

Embedded in the XTP Platform is the industry’s first purpose-built project and task management system specifically designed for managed security operations workflow. Work management allows RADICL to consistently define, drive and track the work that must be performed. The intelligent work-routing architecture automatically assigns tasks to the teams and individuals authorized and capable of doing the work. Work templates leverage RADICL domain expertise, ensuring work gets done right, quickly and with full measurability and transparency.



### KEY CAPABILITIES & BENEFITS

- ACCELERATED INCIDENT INVESTIGATION & RESPONSE
- RISK-BASED TASK PRIORITIZATION
- IMPROVED WORK COMPLETENESS AND QUALITY
- EXECUTIVE VISIBILITY AND METRICS

## ENTERPRISE VISIBILITY AND COLLABORATION

Customer visibility into active incidents and investigations is crucial to ensuring protection and trust. RADICL's work management and modern collaboration capabilities leverage client institutional knowledge to drive quick and accurate decisions. Dashboards allow for full insight into active investigations and incidents, the actions taken by RADICL on the client's behalf and actions that require client support.



### KEY CAPABILITIES & BENEFITS

- EXECUTIVE VISIBILITY INTO ACTIVE CYBER RISK
- IT LEADERSHIP VISIBILITY INTO TASKS REQUIRING PRIORITIZATION AND EXECUTION
- ACCELERATED INCIDENT INVESTIGATION AND RESPONSE
- TRUSTED, SECURE COLLABORATION

# Enterprise-Grade Cyberthreat Protection For SMBs In The Defense Industrial Base (DIB)

WHITEPAPER

RADICL provides SMBs in America's Defense Industrial Base Xtended Threat Protection (XTP). RADICL's purpose-built and proprietary XTP platform delivers SMBs full-spectrum threat protection and compliance management that is quick, easy, and affordable. The RADICL XTP Platform powers an AI-augmented virtual Security Operations Center (vSOC) delivering customers heavily automated and expert-driven threat monitoring, threat hunting, incident response, vulnerability management, security awareness training, and managed compliance adherence. RADICL enables SMBs in the DIB to spend more time running a profitable business to support our country and less time worrying about security and compliance. To learn more about RADICL XTP visit [www.RADICL.com](http://www.RADICL.com)

Boulder, CO  
80302, United States