# **//RADICL™**

# CYBERSECURITY-AS-A-SERVICE (CSaaS) vs. LEGACY MANAGED SECURITY SERVICES

## BACKGROUND

The managed security services market has significantly evolved over the past few decades. Managed service providers (MSPs) were the first to take on some capabilities, such as firewall management. In the early 2000s, the Managed Security Service Provider (MSSP) was born. MSSPs aimed to provide essential defense mechanisms as threats became more widespread. They established the concept of a Security Operation Center (SOC) delivered as a 24/7 managed service. About 15 years later, the next evolution was introduced in the form of Managed Detection and Response (MDR). MDR providers leveraged advancements in Endpoint Detection and Response (EDR) technology to proactively and more effectively detect and respond to threats intersecting with endpoint devices.

CSaaS is the next evolution of managed cybersecurity services. CSaaS is born in the modern tech world to deliver managed services and operations in a cloud and AI enabled manner. CSaaS builds on the depth of MDR and adds additional layer of protective value, while also driving security best practices and regulatory compliance. The remainder of this paper illustrates the primary differences between CSaaS and legacy managed security service options.

## CSaaS vs. MSP/MSSP/MDR

### TECHNOLOGY STACK AND OPERATIONS STAFF

CSaaS providers own the technology and roadmap for the platform powering their offering and delivering the customer user experience (UX). CSaaS providers are not staffed by jack-of-all trade IT workers who have obtained training and certifications across various fields. Instead, their Security Operations Centers are staffed by career experts in all necessary domains, backed by years of in-field experience in a particular domain.
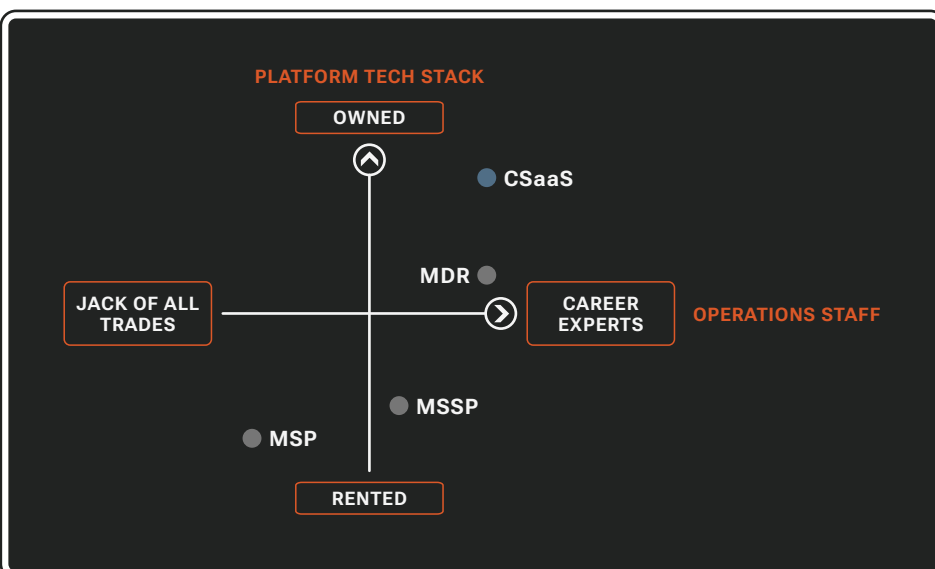


## CSaaS PRINCIPAL MANAGED OPERATIONS

CSaaS offerings should minimally provide the following as managed operations.

### HARDEN OPERATIONS

Hardening focuses on reducing the attack surface, making it more difficult for adversaries to penetrate and expand within your environment.

### DETECTION OPERATIONS

Detection capabilities increase visibility into your IT environment and employ various techniques to identify potential threats and anomalies.

### RESPONSE OPERATIONS

Response capabilities ensure swift and effective action when potential incidents are identified, minimizing damage and restoring normal operations.

### COMPLIANCE OPERATIONS

Compliance operations ensure new and existing cybersecurity regulatory requirements are met.

## THREAT DETECTION SCOPE AND DEPTH

CSaaS providers strive for comprehensive and holistic visibility across the entire IT infrastructure enabling extended threat detection and response. This capability, often referred to as 'XDR,' ensures that threat actors have no place to hide if they infiltrate or emerge from within. CSaaS providers also execute deep hunts to root out embedded threats. They leverage threat intelligence on the tactics, techniques and procedures (TTPs) used by advanced threat actors vs. relying on simple indicators of compromise (IOCs) that more advanced threats don't leave behind.

**VISIBILITY**

XDR

● CSaaS

● MSSP

IOCs — TTPs **THREAT HUNTING**

● MDR

● MSP

EDR
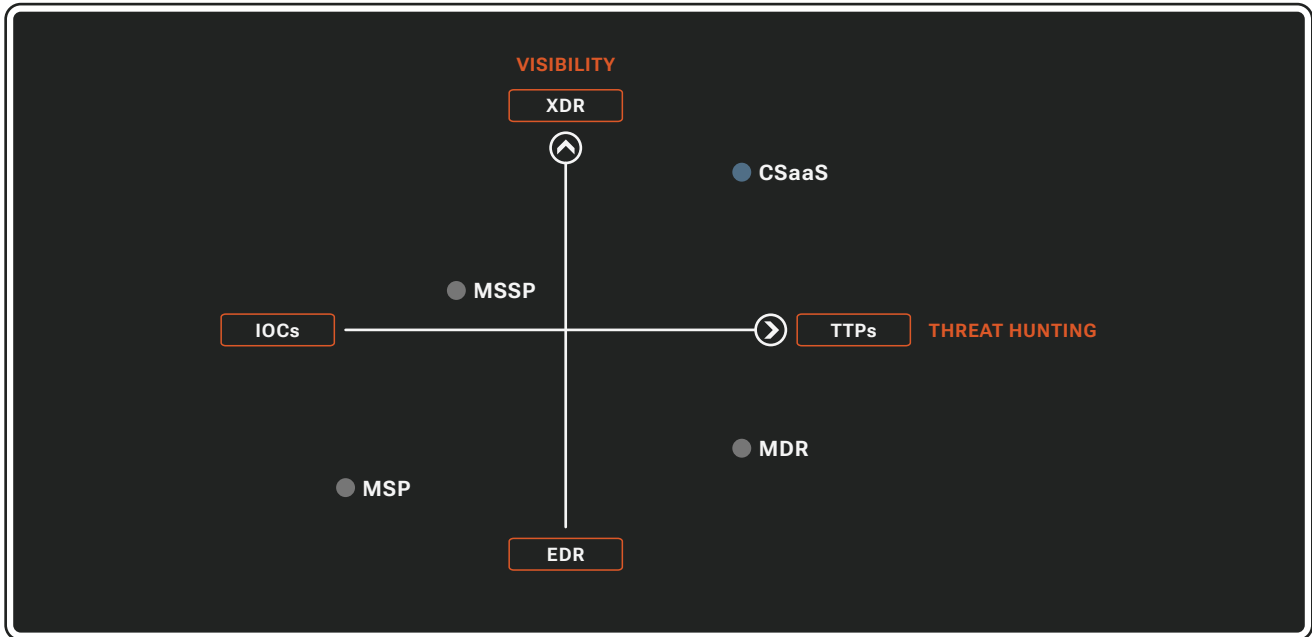
## INCIDENT RESPONSE SCOPE AND DEPTH

CSaaS providers deliver end-to-end incident response operations. They do not just monitor alarms and pass the buck to the customer. Instead, they triage, investigate, respond and oversee the complete incident response process. If actions are required of the customer or a third party (e.g., MSP), CSaaS defines and tracks the work to completion, serving as the overall incident response project manager. CSaaS providers also maintain in-house digital forensics expertise to ensure they can completely and competently respond.

**DIGITAL FORENSICS**

EXPERT

● MDR     ● CSaaS

● MSSP

MONITORING — END-TO-END **INCIDENT RESPONSE OPS**

● MSP

NOVICE
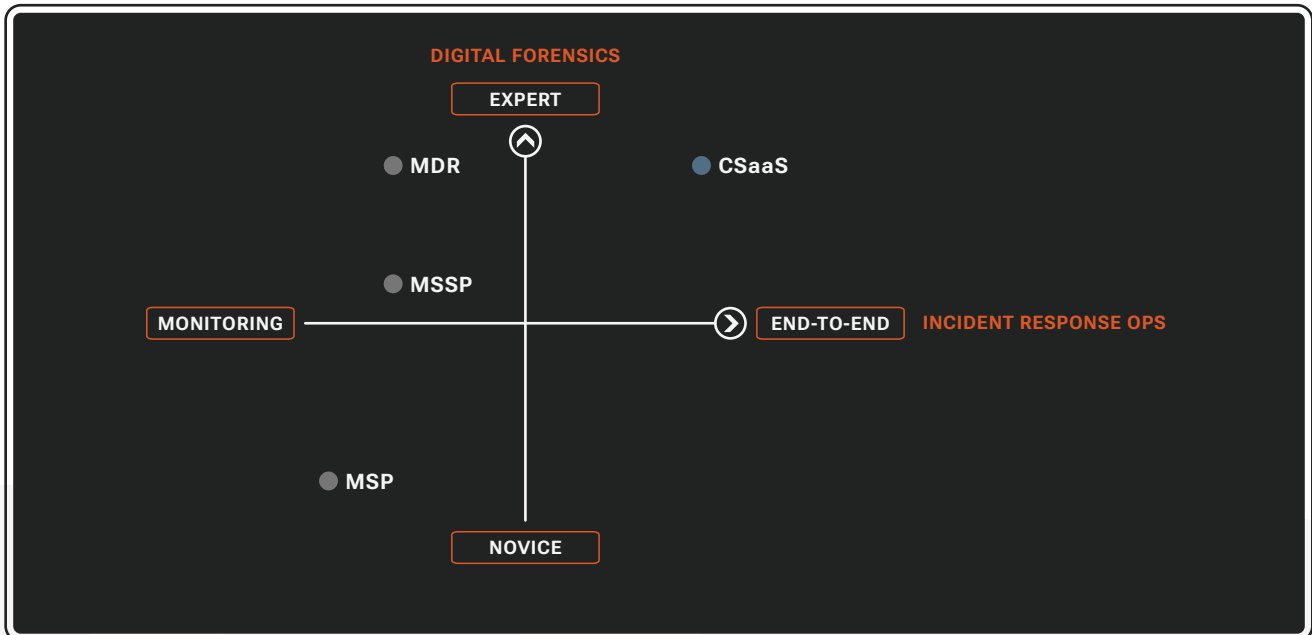
## SECURE COLLABORATION AND OPERATIONAL TRANSPARENCY

CSaaS providers operate with a zero-trust mindset, assuming that day-to-day communication channels (e.g., email, text) might be compromised. They ensure all communications and collaboration can be easily and effectively performed in platform, driving confidentiality. CSaaS providers also operate in an ''open kimono'' philosophy, delivering direct customer access to their platform and full visibility into all actions and operations delivered on their behalf. Transparency drives accountability and trusted delivery.
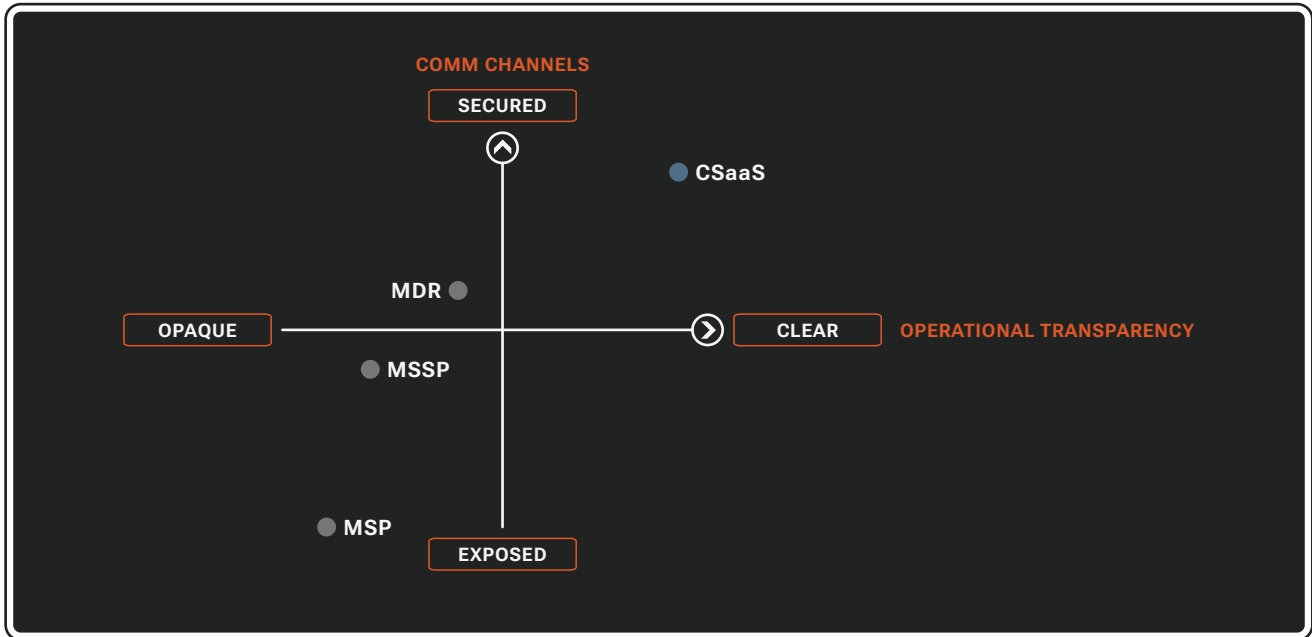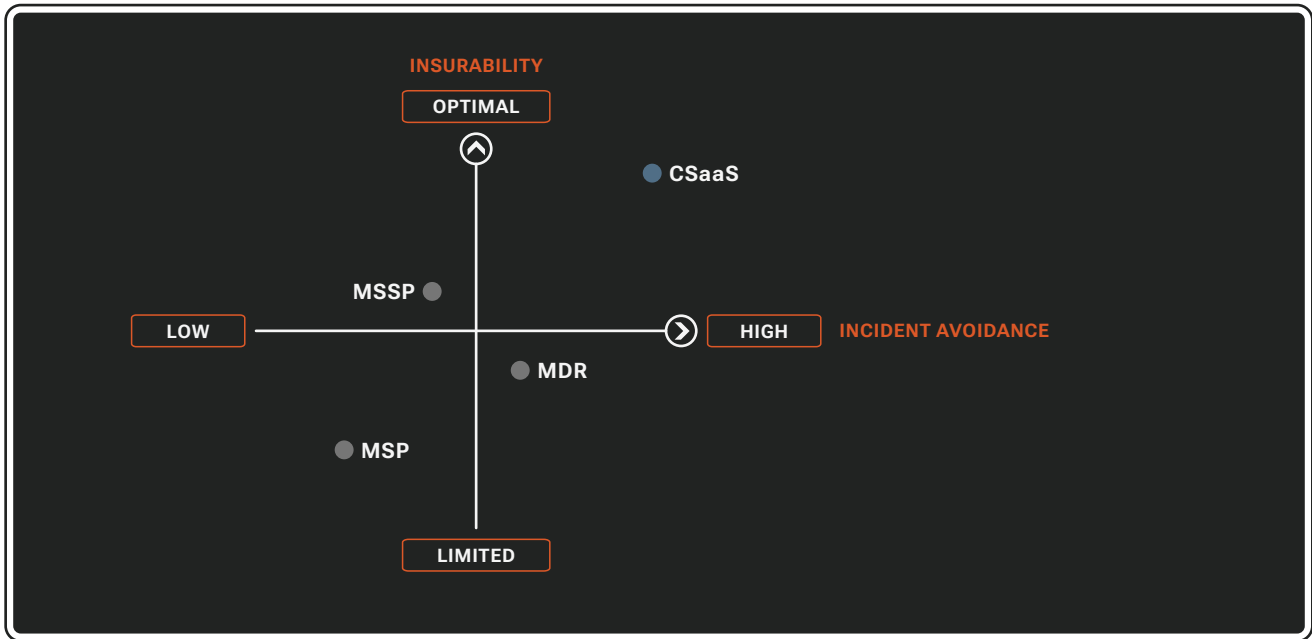


## COMPLIANCE COVERAGE AND OPERATIONS

CSaaS offerings provide comprehensive cybersecurity capabilities that directly meet many of the most challenging and costly regulatory requirements. These include log management, threat monitoring, incident response, vulnerability management, and security awareness training. CSaaS offerings also provide ongoing compliance operations to manage and guide compliance adherence across all regulatory requirements. CSaaS drives periodic self-assessments and tee up necessary remediations with expert guidance. They may also provide templates and tools to further facilitate compliance efforts.
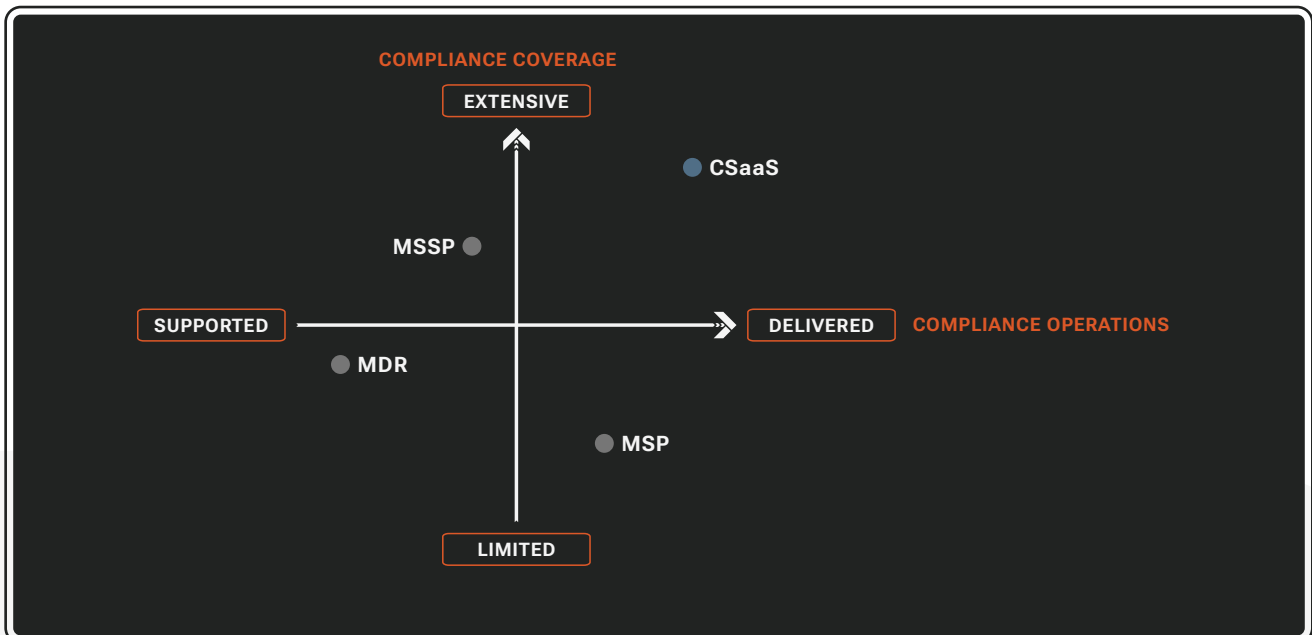
## INCIDENT AVOIDANCE AND INSURABILITY

The comprehensive and mature cybersecurity capabilities of CSaaS materially reduce the risk of experiencing a high-impact incident. Insurers recognize this when evaluating companies for insurability and price. CSaaS meets increasingly stringent insurer requirements and provides optimal options for transferring incident risk.



## CONCLUSION

CSaaS is the next necessary evolution of managed security services and operations. SMBs that consider themselves high-value targets, that want to maximally reduce incident risk, and optimize their insurance and compliance posture, should consider this product category. Figuring out between MSPs, MSSPs, and MDRs who does what well can be daunting. We encourage you to leverage the criteria in this paper to ask probing questions of existing and potential partners to better assess their true capabilities. Entrusting your cybersecurity operations to a third-party is a business-critical decision. The efficacy and expertise of their technology and team will have meaningful impact when it comes protecting your brand, profits, and people.