RADICL™

Cybersecurity-as-a-Service (CSaaS) Primer for Cybersecurity Risk Leaders

INTRODUCTION

Small and medium-sized businesses (SMBs) are increasingly under attack by motivated cyber criminals and nation-state threat adversaries. Incidents like ransomware, business email compromise, and financial fraud are on the rise. Insurers have taken note and are increasingly requiring SMBs to adopt higher levels of cyber threat defense and protection. To avoid brand damage, financial loss, or uninsurability, SMBs need to attain a class of cyber threat protection previously available only to large and mature enterprises. Cybersecurity-as-a-Service (CSaaS) provides SMBs with the "enterprise grade" cybersecurity they need and deserve – at an attainable price point and ideal delivery model.

WHY SMBs NEED CYBERSECURITY-AS-A-SERVICE

Realizing an enterprise-grade cybersecurity posture is a significant investment, one that most SMBs cannot afford to achieve on their own. There are three principal gaps that typically preclude an SMB from realizing a mature "enterprise-grade" defense-in-depth cybersecurity posture.

1 TECHNOLOGY GAPS

Mature defense requires investment in various sophisticated and purposeful technologies such as security information and event management (SIEM), endpoint detection and response (EDR), security orchestration and automation (SOAR), and vulnerability management. Best-in-class technologies are expensive to procure and require ongoing maintenance and tuning to ensure ideal protection.

2 EXPERTISE GAPS

Mature defense requires deep expertise in various areas. This expertise is hard and expensive to come by and takes the form of security analysts, incident responders, threat hunters, and security engineers. Most SMBs are unable to hire a single dedicated cybersecurity headcount, much less a team of people that have expertise across all domains.

3 OPERATIONS GAPS

Mature defense requires continuous and on demand 24/7 operations. Absent modern technology and expertise, SMBs typically lack day-to-day operational capability and capacity to proactively improve their defenses and respond to emerging or active threats.

CSaaS BENEFITS

Materially Reduced Cyber Incident Risk
Your IT environment and people will be less vulnerable to attack. If attacks are successful, they will be quickly detected and mitigated, limiting damage and costs.

IT Resource Optimization
Your IT resources can refocus time supporting business productivity and profit. There cybersecurity knowledge and skills will also be up leveled.

Reduced Cyber Insurance Premiums
Increased cybersecurity maturity and reduced incident risk should result in easier attainment of cyber insurance and reduced premiums.

Regulatory Compliance Adherence
The hardest to achieve requirements will be taken off your plate. Experts proactively shepherding and guiding compliance efforts reduce audit risk.

Consolidated & Predictable Spend
Spend across multiple vendors can be consolidated. Subscription-based pricing delivers predictable spend and budget clarity.

CSaaS addresses SMB cybersecurity gaps **by bringing the necessary technology, expertise and operations** to realize proactive protection and layers of defense.

CSaaS PRINCIPAL MANAGED OPERATIONS

CSaaS is a technology enabled service that delivers “managed operations”. Via the CSaaS platform and what is often referred to as a virtual Security Operations Center (vSOC), their team should seamlessly become your team, proactively managing and driving cybersecurity operations on your behalf. There are 4 principal managed operations a CSaaS provider should minimally deliver.

HARDEN OPERATIONS

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

- **Server and Workstation Protection:** Deploy advanced protection and monitoring technologies on endpoints and servers to block known and emerging attack vectors.
- **Security Awareness Training:** Continuously educate employees on modern cybersecurity practices and test their resilience against social engineering attacks.
- **Vulnerability Management:** Identify, prioritize, and remediate vulnerabilities in your IT infrastructure on an ongoing basis to minimize exploitable weaknesses.

DETECTION OPERATIONS

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

- **Visibility:** Centralize collection and processing of log, event, and alert data from across your IT and cloud environment to support effective security analytics.
- **Detection Analytics:** Develop and deploy advanced detection rules and anomaly detection capabilities to identify a wide range of threat tactics and techniques.
- **Threat Hunting:** Proactively search for hidden threats within your environment using human expertise combined with threat intelligence and analytics.

RESPONSE OPERATIONS

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

- **24x7 Monitoring:** Maintain round-the-clock vigilance to evaluate high-risk indicators of intrusion and compromise within minutes of occurrence.
- **Threat Investigation:** Thoroughly investigate potential incidents to determine their scope, impact, and root cause using forensic analysis and log review.
- **Incident Response:** Rapidly contain threats, develop and execute comprehensive response plans, and manage communications with stakeholders during security incidents.

COMPLIANCE OPERATIONS

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

- **Self Assessments:** Drive and guide periodic self-assessments to determine whether gaps exist or have been introduced.
- **Gap Remediations:** Identify, develop and drive necessary remediation actions to close any regulatory gaps and reduce associated risks.
- **Audit Preparation:** Ensure evidence of compliance is appropriately gathered and safeguarded to ensure a fast and successful audit.

OPTIMIZED IT SECURITY SPEND

Migrating to or starting with a CSaaS offering should result in more efficient IT security spend. Budget across the following technologies can be consolidated into a single vendor relationship.

- ✓ Endpoint Detection & Response (EDR)
- ✓ 24/7 Monitoring & Incident Response Services
- ✓ Vulnerability Management
- ✓ Security Awareness Training
- ✓ Managed Detection & Response (MDR)
- ✓ Security Information and Event Management (SIEM)
- ✓ Penetration Testing
- ✓ Governance, Risk, Compliance (GRC)

5 CRITICAL CHARACTERISTICS OF A CSaaS PROVIDER

When evaluating Cybersecurity-as-a-Service (CSaaS) providers, the following five characteristics are critically important to evaluate. The quality and capability with which these criteria are realized will directly influence the degree of protection and risk reduction realized.

1 PROPRIETARY TECHNOLOGY PLATFORM AND ROADMAP

The provider should have their own technology platform and control their roadmap. The quality of the technology enabling the provider will determine the results and value realized for their customers. A modern CSaaS provider must be a technology company heavily investing in R&D, their platform, and their roadmap to ensure success today and in a rapidly evolving cyber threat future.

2 ABILITY TO ATTRACT AND RETAIN INDUSTRY EXPERTS

The CSaaS provider must be able to attract and retain industry experts. Folks in the cybersecurity industry want to work for the best. Skills such as threat hunting and incident response are in high demand. You want to ensure your CSaaS partner can attract and retain top talent. The quality of their staff will greatly impact the quality of service and protection delivered to you.

3 LEVERAGE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence is accelerating everything. Threats are becoming faster and harder to detect. To counter this, CSaaS providers must also heavily harness the power of AI to improve the pace and quality of all operations. Only AI-powered CSaaS providers will be equipped to stay abreast of, and ahead of, AI-enabled attackers.

4 BEST-IN-CLASS TECHNOLOGY PARTNERS

When third-party technologies are required (e.g., EDR) in support of the CSaaS offering, they should be best-in-class. There are many outdated and insufficient products that have made their way into the SMB market. CSaaS providers should be working with a select set of 3P technologies that are ideal for purpose and in which they have acquired deep expertise. The best results are realized with the best tools.

5 OPERATIONAL TRANSPARENCY

The best Cybersecurity-as-a-Service (CSaaS) providers practice operational transparency. Don't be dissatisfied, or possibly misled by "black box" offerings. Demand visibility into the actions and activities being taken on your behalf. This is the best way to ensure provider accountability. Transparency also provides learning opportunities for internal IT and security staff, enhancing the cybersecurity competency within your own team.

CONCLUSION

SMBs are high-value targets for motivated threat actors. To combat the increasing risks posted by cybercriminals and nation-state actors, companies must adopt enterprise-grade, defense-in-depth, cybersecurity measures. By leveraging CSaaS, SMBs can bridge the gaps in technology, expertise, and operations, ensuring robust defense and compliance without the high costs of maintaining in-house infrastructure. This approach not only reduces the risk of cyber incidents but also optimizes IT resources, lowers cyber insurance premiums, and ensures regulatory compliance, all while providing predictable and consolidated spend.