Crayon Cloud Security Assessment Service Overview.

Crayon

crayon.com

Cloud Security is a Growth Opportunity.

Cloud investment will remain strong over the next 18-24 months, and businesses are allocating larger budgets to engage cloud services partners.

Offering a Crayon Cloud Security Assessment positions our partners to benefit from this continued market confidence. Here's why:

Appropriate configuration of cloud platforms to address cybersecurity risks is the #1 challenge for those using public cloud

Concerns about security, privacy concerns, and a lack of governance is the #2 challenge faced by SMBs using private cloud

Security is the #1 investment priority for SMB buyers in Asia Pacific

66% of SMBs intend to increase investment in cloud security solutions

88% of all SMBs intend to increase budget allocations for third party service providers

Source: The Future of Operations: Maximise Value From The Cloud With A Strategic Mindset – a commissioned Forrester Consulting study conducted on behalf of rhipe, 2023.

What does this mean for our partners?

- SMB IT decision makers are aware their cloud platforms may be operating in ways that create hidden risk.
- They are ready and budgeted to do something about it.
- Decision makers are actively looking for partners that can help address their cloud security challenges.

The Crayon Cloud Assessment Service provides partners with an opportunity to respond quickly, with an effective and affordable offering.

Address Security Concerns. Lock in Customer Loyalty.

The security challenges and concerns for SMBs can reduce their ability to drive maximum value out of existing cloud platform investments. Perceived security risks also present barriers to adoption in other cloud solution portfolios.

A Crayon Cloud Security Assessment can provide your SMB customers with increased confidence in both regards. This supports your position as their preferred provider, ahead of planned adoptions and increased spending

What is the Crayon Cloud Security Assessment?

Crayon Cloud Security Assessments follow the internationally recognized CIS v8 (Center for Internet Security) framework. The service is designed to help partners and customers using Microsoft 365 and Microsoft Azure.

Framework and Scoring Methodology

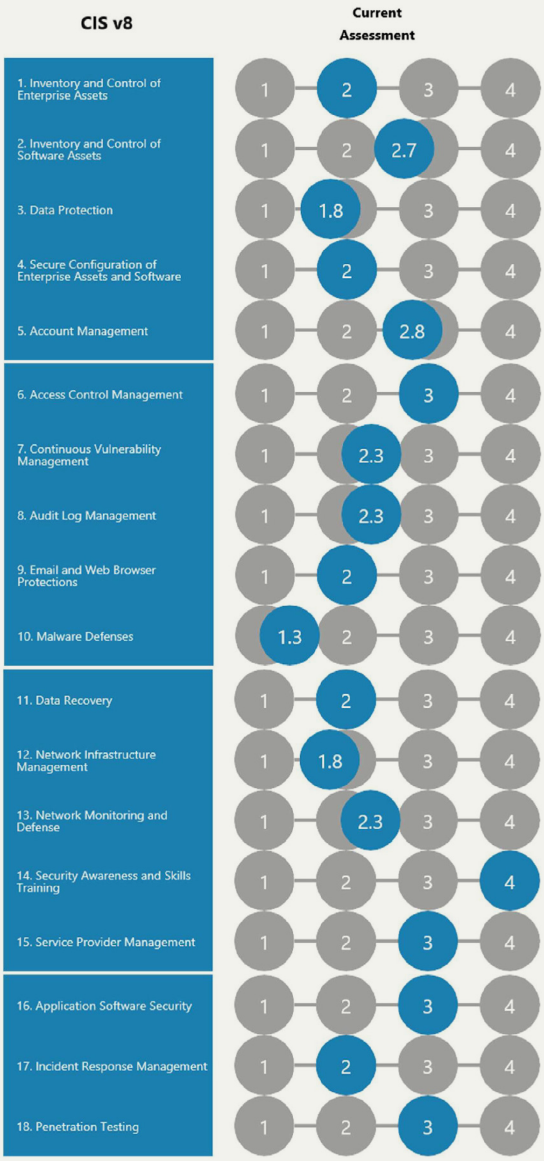
Through data-driven evaluation and analysis, the assessment defines and identifies weaknesses and risks, such as missing security controls, vulnerabilities and configuration issues that can make these platforms vulnerable, and

The assessment then provides actions needed to reduce risk and groups these into low, medium, high priority categories. This provides you and your customer with a clear, actionable security roadmap to follow.

Once actioned, you will have played a vital role in enabling your customer to mature their organisational security approach.

Our service enables you to:

- Get a documented understanding of your customer's current security maturity and posture
- Innovate safely with full confidence in your customer's cloud security posture
- Progress with confidence in your customer's Zero Trust journey following achievable and prioritised steps
- Helps your IT customers gain support from business stakeholders for ongoing security and cloud initiatives
- Achieve compliance across all relevant security standards



CIS v8	Current Assessment
1. Inventory and Control of Enterprise Assets	2
2. Inventory and Control of Software Assets	2.7
3. Data Protection	1.8
4. Secure Configuration of Enterprise Assets and Software	2
5. Account Management	2.8
6. Access Control Management	3
7. Continuous Vulnerability Management	2.3
8. Audit Log Management	2.3
9. Email and Web Browser Protections	2
10. Malware Defenses	1.3
11. Data Recovery	2
12. Network Infrastructure Management	1.8
13. Network Monitoring and Defense	2.3
14. Security Awareness and Skills Training	4
15. Service Provider Management	3
16. Application Software Security	3
17. Incident Response Management	2
18. Penetration Testing	3

Key deliverables

The Cloud Security Assessment Report includes:

- An Executive Summary
- Security Maturity Score out of 4
- List of key findings and recommendations
- Customer suggested roadmap for the immediate mid and long term
- Detailed ratings and security scores and maturity scores by key CISv8 controls
- Actionable recommendations and remediation steps

Can all partners use the Crayon Cloud Assessment Service?

The Crayon Cloud Security Assessments program is perfect for partners that want to help their clients improve their cyber security posture but may not have security analysis capabilities in-house.

Any partner with clients running Microsoft 365 and/or Azure can benefit from this service. The assessment is designed to identify vulnerabilities on these platforms, and recommend the actions needed to remediate.

The service allows you to offer expert advisory and recommendations around the findings of an assessment, by leveraging an expert security operations capability.

#	Findings	Recommendations
KF1	Multi-factor Authentication is missing for a high number of users across all account types, including administrator and Global Admin accounts. Threat: Account theft, unauthorized access, sensitive data loss, lateral movement	• Verify reason for lack of MFA and enforce MFA on all administrator accounts, and then on all user accounts. Periodically review the state of MFA • Roll-out proper conditional access policies • Refer to Crayon Secured Identity Accelerators
KF2	All client endpoints are missing proper security baselines and some of them are missing key security controls. Threat: account theft, unauthorized access	• Define minimum security baseline and configurations for employee devices, recommended to use Intune compliance policies and configuration profiles • Extend conditional access to devices • Refer to Crayon Secured Endpoints Accelerators for support
KF3	Many Azure resources are exposed due to insecure configurations. Several network security groups are too permissive. A high number of storage accounts are allowing old TLS versions and are publicly exposed. Threat: unauthorized access, sensitive data loss, lateral movement	• Introduce more restricting rules to the Azure network security groups protecting Azure Virtual Machines • Review the reason for storage account public access, disallow where possible. At minimum, disallow public access at container level • Enforce at least TLS version 1.2 for all storage accounts
KF4	Modern security capabilities and routines are missing across Azure subscriptions. Threat: unauthorized access, lateral movement, undetected security incidents	• Roll-out vulnerability management solution and endpoint protection for at least production servers • Review and implement a security incident management process and make sure it covers public cloud resources as well • Refer for Crayon Security Posture Accelerators
QW	Quick Win findings: • Attack surface reduction rules are not enabled • Tamper protection is off • Users are allowed to consent to all apps Threat: loss of sensitive data, unauthorized access, lateral movement	• Turn on tamper protection for protecting endpoint protection solution • Review if there is any usage for legacy authentication. Implement policy to block them • Allow users to consent to only trusted apps • Turn on ASR rules on audit mode

What is the ideal customer profile?

Customers that may benefit from a Crayon Cloud Security Assessment could include:

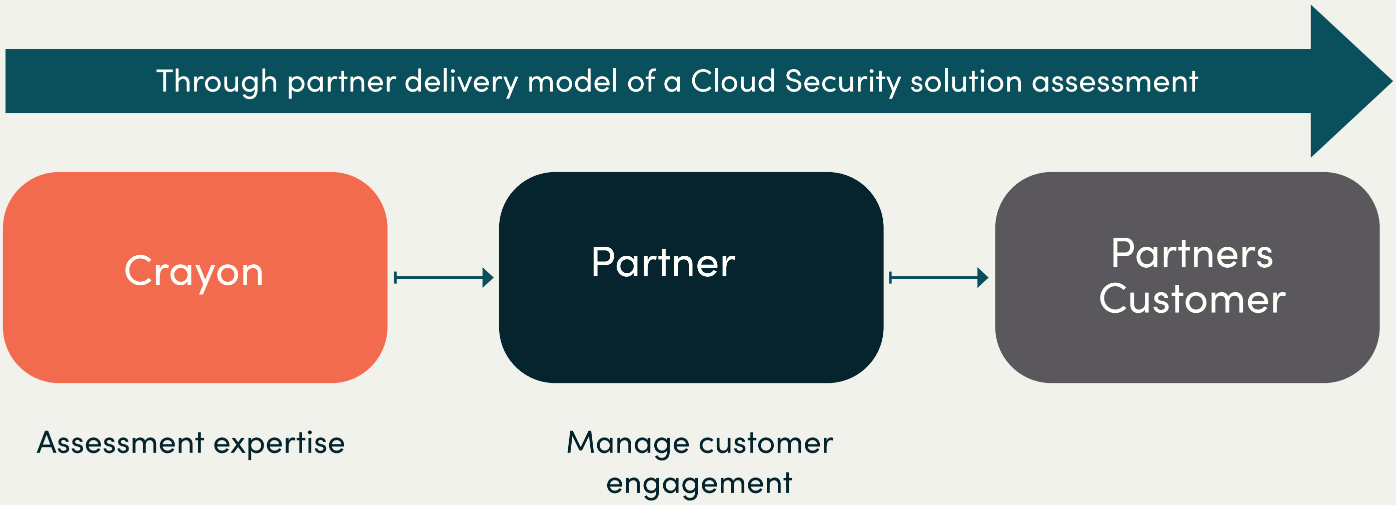
- Businesses with 50 seats or more
- Organisations with a requirement or desire to meet cyber security standards such as ACSC Essential 8, APRA, ISO etc.
- Businesses leveraging M365 Business Premium, M365 E3, M365 E5, A3, A5, F3, F5 and / or have an Azure security need
- Industries such as professional services (legal, accounting), financial services, government (local, state, federal), retail

Our service can help you have a 'right-now' conversation with any Microsoft 365 or Azure customer that has expressed an interest in an improved security posture.

A True Through-Partner Offering.

The Crayon Cloud Security Assessment Service is managed by Crayon. Customer engagements are led by our partners, and service agreements are written on the partners' paper.

Partners pay us for the service and retain a generous margin.



Through partner delivery model of a Cloud Security solution assessment

Crayon → Partner → Partners Customer

Crayon: Assessment expertise

Partner: Manage customer engagement

What is the opportunity for rhipe Partners?

Cloud security is a ubiquitous need for SMB customers. Yet, building security capabilities and competencies takes time. Our service helps partners respond to immediate risks and need for their customers, without the need to invest in practice build.

Equally, partners with have mature specialisations have a lot of ground to cover. Our service is an effective way to get a high volume of smaller accounts on the road to improved security.

The benefits of joining the Crayon Cloud Security Assessment program include:

Access to security experts

Crayon provides an impartial assessment for your client's security. You benefit by leveraging our security expertise and reducing the risk of your customer engaging other external experts.

Sales margin

Partners delivering the service will get a margin when re-selling to their customers.

Clear and immediate action items

The security assessment provides clear actions that should be undertaken to improve the client's cyber security posture, creating immediate ongoing services sales opportunities for partners.

Upsell opportunities

The assessment provides opportunities for a partner to add upsell recommendations to the report.

How do I sign up to the Crayon Cloud Security Assessment program?

To sign up to the program, simply follow the below steps:

1. **Register the opportunity in PRISM**
2. **The Crayon Cyber Security team will contact you to arrange an initial call**
3. **There will be a separate call organized to scope the assessment**
4. **Project kick-off**

Or to find out more, get in touch with your rhipe account representative.

Register Cloud security Assessment in Prism

Qualification call with Crayon

Customer/MSP scoping call

Project kick-off