RECON™ ProServ

What is the **RECON**™ Security Suite?

The **RECON** Security Suite is a set of subscription or consulting based security solutions which solve unique challenges for customers, covering a range of security threat vectors. The **RECON** Security Suite offers emerging growth vendors and partners the opportunity to leverage the Tech Data brand to promote their solution alongside complementary security offerings, solving a more comprehensive security challenge for end-users. The products in the **RECON** Security Suite are not intended to compete with the more complete portfolios of an established security vendor, but to provide partners with new and alternative approaches to securing their customers by leveraging emerging growth security vendors which are positioned by capability and aligned to the NIST Cybersecurity Framework.

What is **RECON** ProServ?

The services chosen for the **RECON** Security Suite were identified based on commonly requested services and those which complement the security solutions in the Tech Data portfolio. Security services are occasionally delivered by Tech Data resources, but are more commonly delivered by trusted Tech Data partners. If you are a Tech Data partner and wish to participate in the **RECON** ProServ program, please email securityservices@techdata.com.

RECON ProServ Offerings

Category	Service	Description
Assessment	Penetration Testing	Real world simulation of how an attacker would gain access to a customer network. This service leverages both technical and social engineering penetration testing techniques that an attacker may leverage in order to penetrate the customer's network. A report is generated and delivered to the customer that details how our attack penetrated the network. Not only does this service help our partners identify new security solutions opportunities, it also lays a path to help the customer on their security posture maturity.
Assessment	Vulnerability Assessments	This service identifies how susceptible a customer's network is to a cyber-attack. We leverage best-in-class scanning toolsets and techniques to identify detailed vulnerability findings. The results are reviewed by our security experts, then a detailed report is generated for the customer. This is designed to help end customers reach a superior security posture as it identifies where they have risks and exposures in order to secure their network from advanced cyber threats.

Assessment	Vertical Assessment	A free and non-intrusive service that measures a customer's security readiness against various types of security threats, which is delivered via an interview and discussion with the customer's IT leadership team. A comprehensive report is generated that identifies where the customer is over-under in their security capabilities and compares their security readiness to their peers' in their vertical (Healthcare, Retail, Public Sector, Education). This service helps identify or validate security solutions needed to improve the customer's security posture as well as help build a security solution roadmap for a customer.
Assessment	CISCO DCLOUD (POV)	Cisco Managed Security Proof of Value (POV) Assessment is a no cost security assessment over a two week period. This service leverages an onsite Cisco ASA which acts as a sensor with Firepower Services enabled. The collected data is then transmitted to a Cisco Firepower Management Center in the cloud. A risk report is then generated by our Security Engineers and reviewed in detailed with our Tech Data partner. This service helps to position Cisco Security Solutions to customers as it delivers threat-focused protection, real-time network visibility, and is the most robust next-generation firewalls and threat remediation systems in the industry with no need to purchase subscription licenses.
Assessment	GDPR Assessments	Service that provides a customer's organization with an accurate and detailed assessment of where they stand in relation to the controls outlined in the GDPR framework. This service delivers both an executive summary document and a detailed technical report that describe all of the findings and technical recommendations needed to be compliant to GDPR. This assessment helps your customer ensure that they are prepared to be GDPR compliant as it applies to any company processing personal data or otherwise monitoring behavior of European Union (EU) residents.
Compliance	PCI Audit	PCI compliance audit is a routine audit required of merchants that process credit card transactions to make sure that they are compliant with the Payment Card Industry Data Security Standard (PCI DSS) set up by various credit card companies. This service examines the customer's environment, identifies vulnerabilities in order to prevent data from being compromised as it relates to a customer's point of sale system and delivers a detailed risk assessment report and guides customers to address problem areas that will improve data security. This service gives companies that must comply with the Payment Card Industry Data Security Standard (PCI DSS) a risk assessment that shows them where they stand in terms of PCI compliance.
Compliance	Governance, Risk and Compliance (GRC)	Governance, Risk, and Compliance (GRC) is intended to help customers properly apply security controls and regulations within their organization that they must be compliant to, but find that their current security controls are disorganized, unnecessarily complex and fragmented. This service helps your customer first understand their risk tolerance and gaps, and then provide a plan of action to mitigate risks, achieve compliance against their required regulation, and maintain security posture through a Continuous Monitoring Strategy. This GRC complaint service is tailor-made for your end customer's enterprise so they can adopt a GRC program that quickly identifies risks automatically, helps them maintain compliance, as well as prepare for the next generation of GRC innovation.
Implementation	McAfee	Consulting implementation services that help customers with architecture, deployment, and operation services across the McAfee security portfolio.
Implementation	IBM Guardium	Consulting implementation services that help customers with architecture, deployment, and operation services for IBM Gaurdium. Other available services includes managed services to support the Gaurdium and Big Data Security apps together.
Implementation	IBM BigFix	Consulting implementation services that help customers with architecture, deployment, and operation services for IBM BigFix.

To learn more about how you can leverage RECON ProServ in your security practice, contact your Tech Data sales representative or email SecurityServices@techdata.com.