PRAETORIAN

Professional Services Overview

INFORMATION SECURITY ASSESSMENT AND ADVISORY

NETWORK | APPLICATION | MOBILE | CLOUD | IOT

Praetorian Company Overview

HISTORY

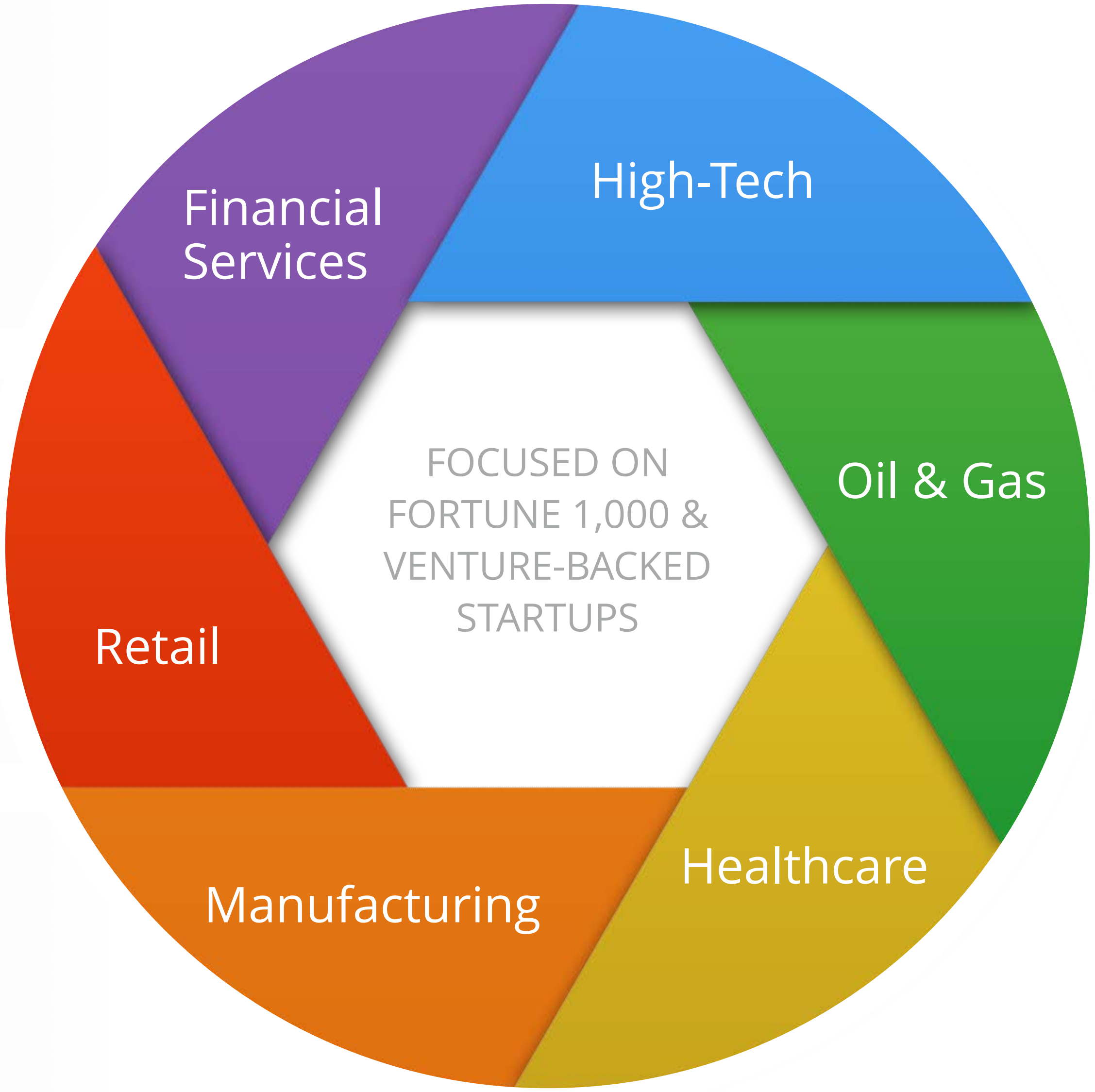
- Founded in 2010
- Headquartered in Austin, TX
- Self-funded
- Profitable since inception

ATTRIBUTES

- Superior technical prowess
- Comprehensive reporting
- Trusted business acumen
- Advanced, time-tested methodologies

PROPOSITION

- Praetorian provides a suite of security assessment and advisory services that help clients protect their most important assets from evolving cyber threats.



An Established and Growing Services Firm

When you're constantly advancing your industry and helping to secure today's leading organizations, **people notice**.

Inc. 5000 2015

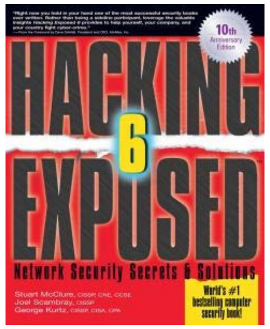
Inc. 5000 2014

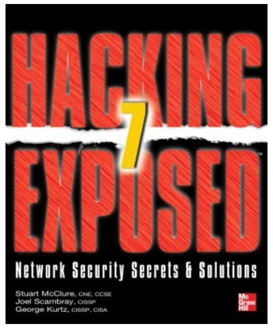
CYBERSECURITY 500 WORLD'S HOTTEST SECURITY COMPANIES

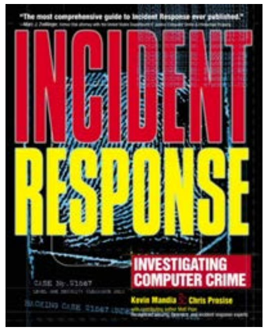
CIO Enterprise Security Consulting 2014
20 Most Promising Enterprise Security Consulting Companies

Our Consultants Are “The Security Experts”

- Top 5% of the industry
- Certified expertise includes: CISSP, CISA, CSSLP, CEH, GCIH, GSEC, GNSA, GCIH, GCFW, GWAPT, GAWN, GCFE
- Respected authors, researchers, federal security policy contributors, patent holders and open-source developers
- Speakers at major security conferences and professors at major universities
- Educational backgrounds in computer science, engineering, and information systems







Recognized by Industry and the Media

- Expertise and comment regularly leveraged by media
- Recently named one of the **20 Most Promising Security Companies** by CIO Review Magazine
- Security research cited by major institutions, including NASDAQ and Dept. of Homeland Security

We Are Fanatical About Service Execution

Project Management

- Timely communication and regular status updates

Knowledge Transfer

- Close working relationship and always available by email/phone

Comprehensive Reporting

- Digestible by executive and technical leadership
- Actionable strategic and tactical recommendations

Using Efficiencies Built from the Ground Up

- Builders make the best breakers
- Our **engineering culture** drives powerful efficiencies that enable us to deliver more for less
- Our time tested methodologies are paired with a unique suite of **custom tools**, which delivers more value across every engagement
- We are obsessed with **efficiencies** and continuous improvements

Proprietary Tools & Software

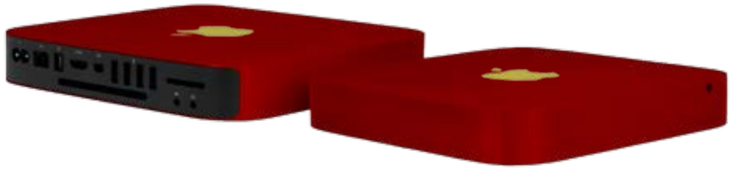
Our security engineers are equipped with a suite of custom tools and software. If a new solution is needed to solve a unique problem, we build it.

Advanced Reporting System

Custom reporting tools and capabilities reduce reporting time by up to 50% allowing more effort to be spent on technical testing.

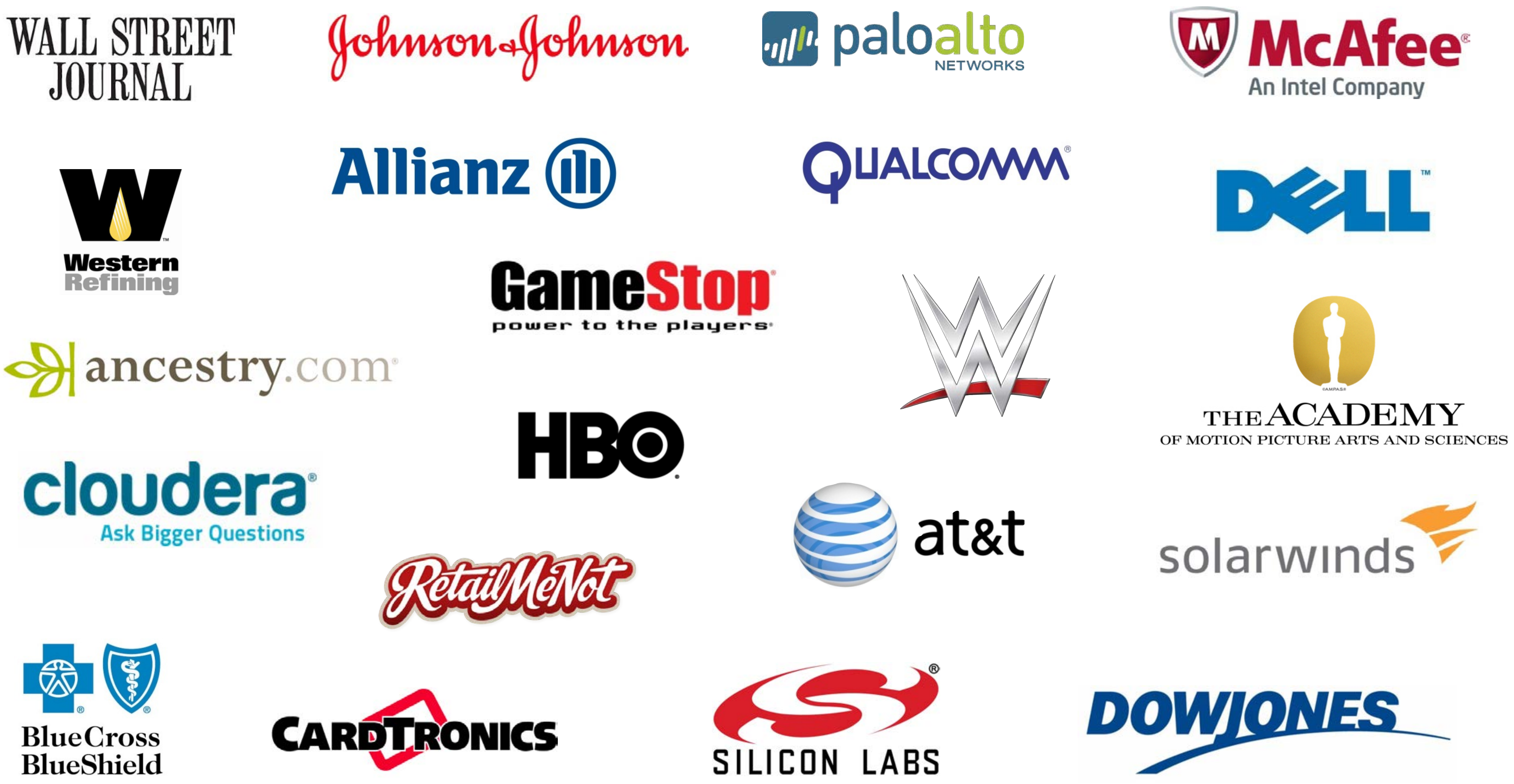
iPentest™ Device

Custom plug-and-play technology allows our team to perform onsite work remotely. This minimizes logistics and travel costs for clients, while extending testing time.



And that just scratches the surface of our unique capabilities…

Trusted by Today's Leading Organizations



Just Ask Our Extraordinary Clients

QUALITY OF REPORTS

“The content is top notch, the presentation is complete and clear.”

AGILE & EFFICIENT

“[Your consultants] are available at all times of the day, and are all over the assessments.”

TECHNICAL TALENT

HIGHLY ENGAGED

QUALCOMM®

ACCOMMODATING

PRODUCT AGNOSTIC

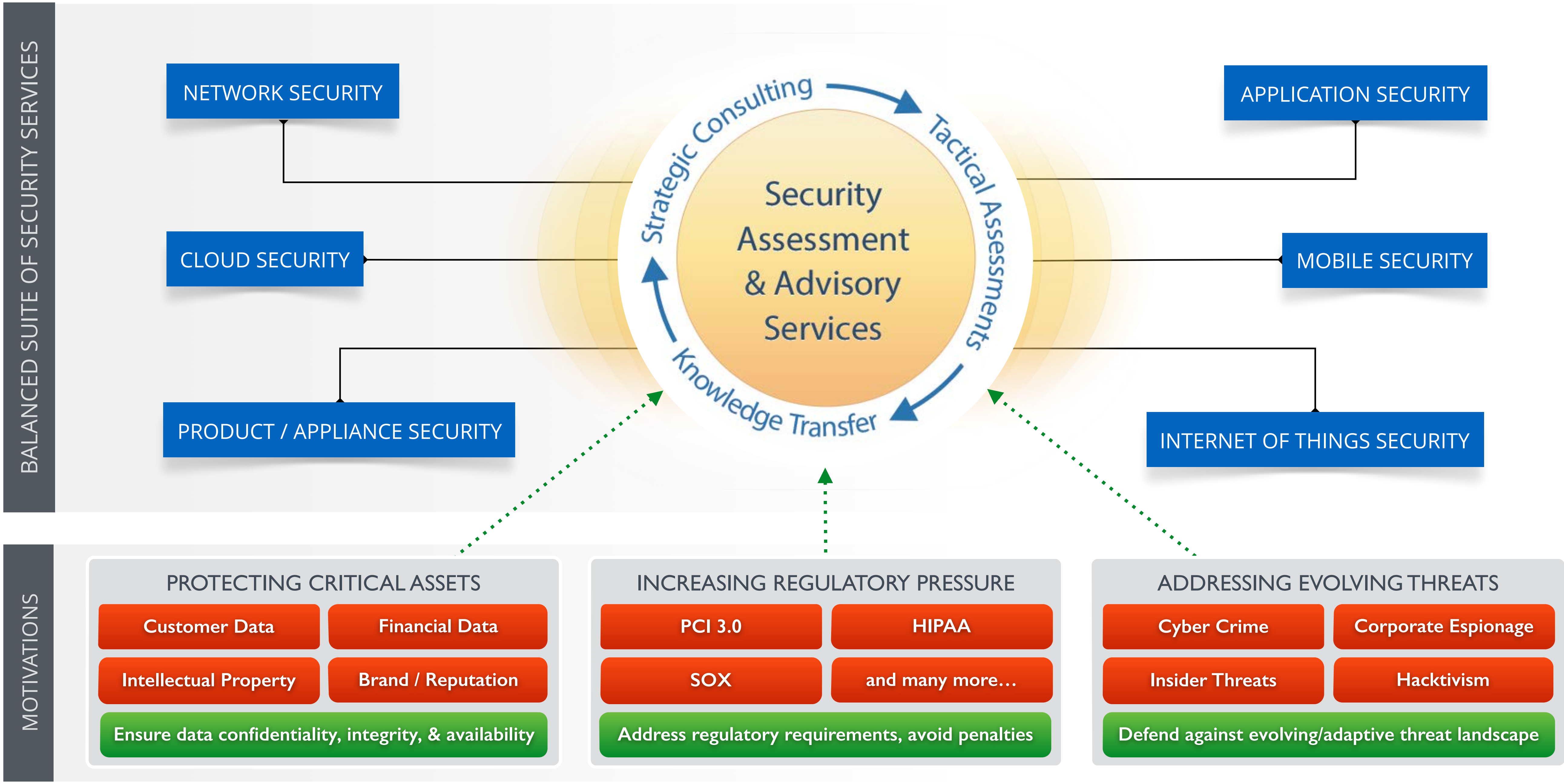
EASE OF WORKING TOGETHER

“You and your team have always been very supportive [of] the broader set of enterprise services that we have here at Qualcomm so that the reports can be actionable by the people who are getting them.”

CONSISTENCY

“You have the same people over time. When we come back after time we get people who were on our past contracts and we’ve already developed a level of comfort with.”

Services That Address Your Specific Needs



BALANCED SUITE OF SECURITY SERVICES

NETWORK SECURITY

CLOUD SECURITY

PRODUCT / APPLIANCE SECURITY

APPLICATION SECURITY

MOBILE SECURITY

INTERNET OF THINGS SECURITY

Security Assessment & Advisory Services

Strategic Consulting

Tactical Assessments

Knowledge Transfer

MOTIVATIONS

PROTECTING CRITICAL ASSETS

- Customer Data
- Financial Data
- Intellectual Property
- Brand / Reputation

Ensure data confidentiality, integrity, & availability

INCREASING REGULATORY PRESSURE

- PCI 3.0
- HIPAA
- SOX
- and many more…

Address regulatory requirements, avoid penalties

ADDRESSING EVOLVING THREATS

- Cyber Crime
- Corporate Espionage
- Insider Threats
- Hacktivism

Defend against evolving/adaptive threat landscape

Network Security Services Overview

PENETRATION TESTING

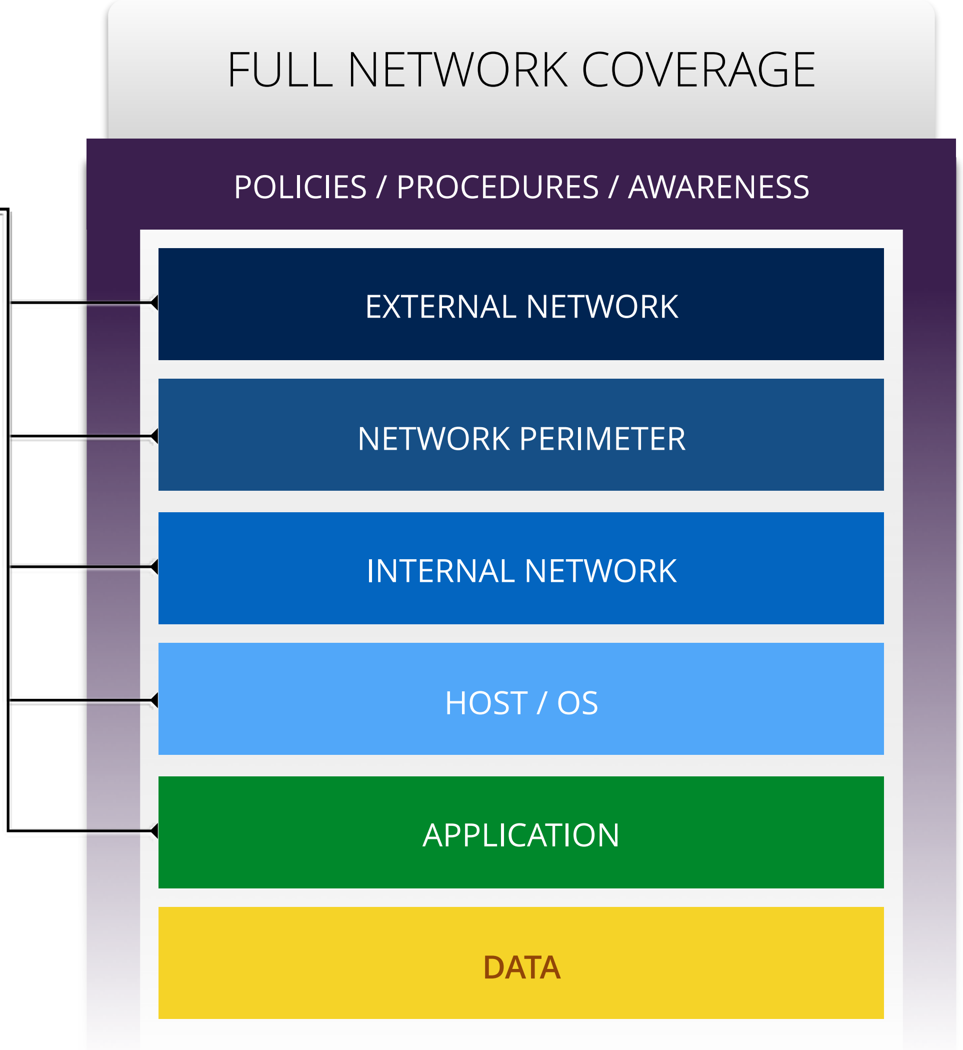
Demonstrate Risk by Simulating Real-world Attacks	External Penetration Testing Internal Penetration Testing Wireless Penetration Testing

SUPPLEMENTAL SERVICES

Evasion & Detection Exercises
Spear Phishing Campaign
Social Engineering Test
Denial of Service (DoS) Test
Sensitive Data Flow Analysis

COMPLIANCE GAP ANALYSIS

POLICY & PROCEDURE REVIEW



FULL NETWORK COVERAGE

POLICIES / PROCEDURES / AWARENESS

EXTERNAL NETWORK

NETWORK PERIMETER

INTERNAL NETWORK

HOST / OS

APPLICATION

DATA

IT SECURITY AUDITING

DESIGN SECURITY REVIEWS

Network Architecture Review
Active Directory Review
Mobile Device Review
VoIP Review
Wireless Review

HOST & DEVICE REVIEWS

Firewall Review
VPN Review
Router/Switch Review
Critical Server Review
Virtualization Review

Defensive components and security controls should be tested at all levels to ensure they are effectively working together to protect critical assets.

PCI DSS 3.0 Security Assessment

PCI Data Security Standard – High Level Overview		
Build and Maintain a Secure Network and Systems	**1** **2**	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3** **4**	Protect stored cardholder data Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5** **6**	Protect all systems against malware and regularly update anti-virus software or programs Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7** **8** **9**	Restrict access to cardholder data by business need to know Identify and authenticate access to system components Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10** **11**	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an Information Security Policy	**12**	Maintain a policy that addresses information security for all personnel

PCI 3.0 DSS SERVICES

PENETRATION TESTING

External Penetration testing

Internal Penetration Testing

Wireless Penetration Testing

Web App Penetration Testing

SECURITY REVIEWS

Network Architecture Review

Sensitive Data Flow Analysis

Firewall Review

VPN Review

Router/Switch Review

Critical Server Review

Virtualization Review

Obtain an accurate understanding of your security and risk posture, while **ensuring compliance with industry regulators** and information security best practices.

Establishing or Improving a Cybersecurity Program

TOP 20 SECURITY CONTROLS

1. 🔵⚪ Asset Inventory
2. 🔵⚪ Software Inventory
3. 🟣⚪ Secure Hardware and Software Configurations
4. 🔵🟡🔴 Continuous Vulnerability Assessment & Remediation
5. 🟣🟡 Malware Defenses
6. 🟣⚪ Application Software Security
7. 🟣⚪ Wireless Access Control
8. 🟢⚪ Data Recovery Capability
9. 🟣⚪ Procedures and Tools
10. 🟣⚪ Secure Configurations for Network Devices (FW, Routers, Switches)
11. 🟣⚪ Limitation and Control of Network Ports, Protocols, and Services
12. 🟣⚪ Controlled use of admin privileges
13. 🟡⚪ Boundary Defense
14. 🟣🟡🔴 Maintenance, Monitoring, and Analysis of Audit Logs
15. 🟣⚪ Controlled Access based on Need to Know
16. 🟣🟡 Account Monitoring and Control
17. 🟣⚪ Data Protection
18. 🟡🔴 Incident Response and Management
19. 🟣⚪ Secure Network Engineering (Network Architecture)
20. 🔴🟢 Penetration Tests and Red Team Exercises

- National Institute of Standards an Technology (NIST) has identified the five major functions of a Cybersecurity Program
- SANS/CSC has mapped the top 20 security controls to these functions implemented

FUNCTIONS

🟦 IDENTIFY

- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

🟪 PROTECT

- Access control
- Awareness and training
- Data security
- Info protection and procedures
- Maintenance
- Protective technology

🟨 DETECT

- Anomalies and events
- Security continuous monitoring
- Detection process

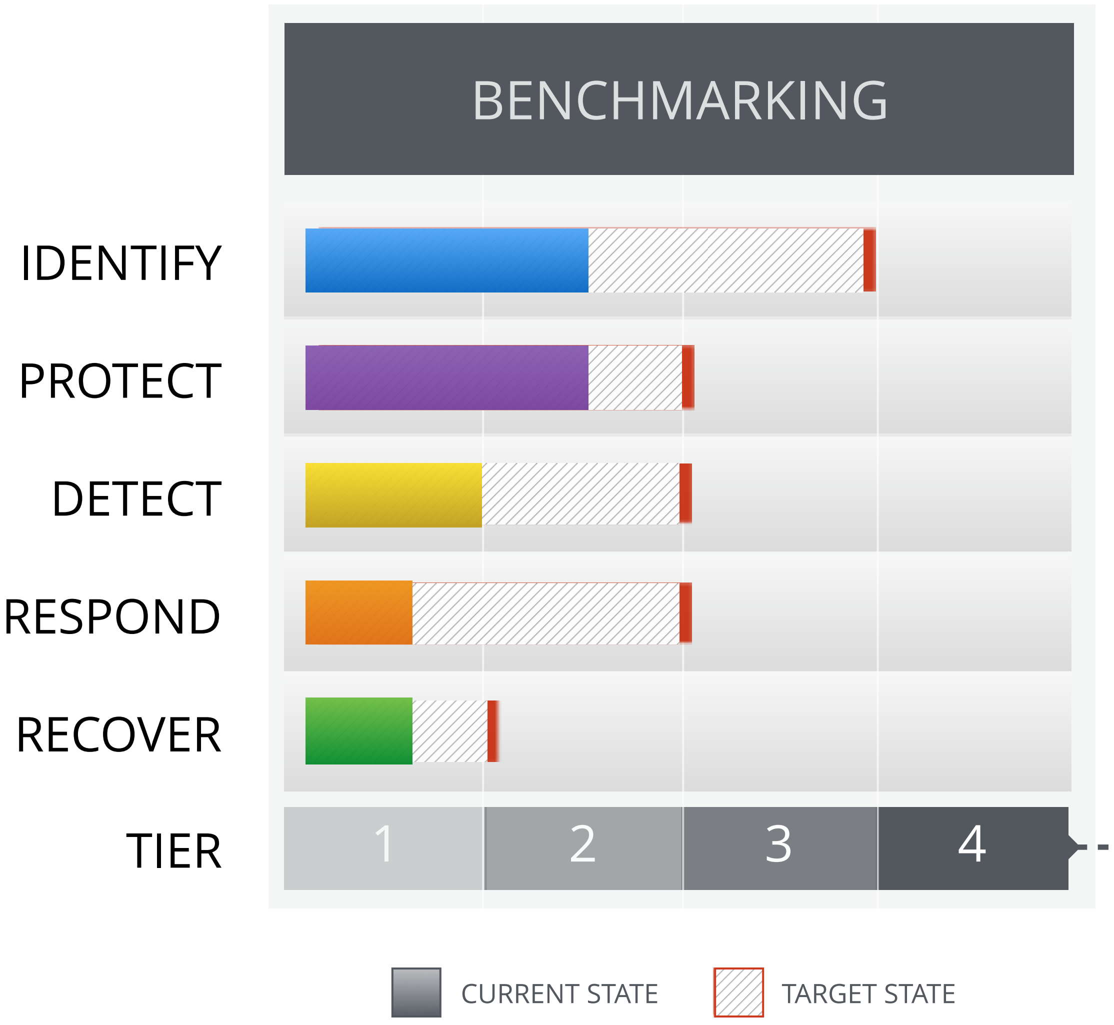
🟥 RESPOND

- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

🟩 RECOVER

- Recover planning
- Improvements
- Communications

NIST Cybersecurity Framework Benchmark



- A Tiered rating system measures the extent to which these controls have been implemented

1	PARTIAL
2	RISK INFORMED
3	REPEATABLE
4	ADAPTIVE

Source: http://www.nist.gov/cyberframework/index.cfm

Leverage the **NIST Cybersecurity Framework** as an overlay for your organization's existing practices and Praetorian's recent assessment activities.

Application Security Assessment Services

WEB | MOBILE | IOT

DESKTOP | APPLIANCE

TACTICAL ACTIVITIES

Penetration Testing

Security Code Review

Developer Interviews

Threat Modeling

Requirements Mapping

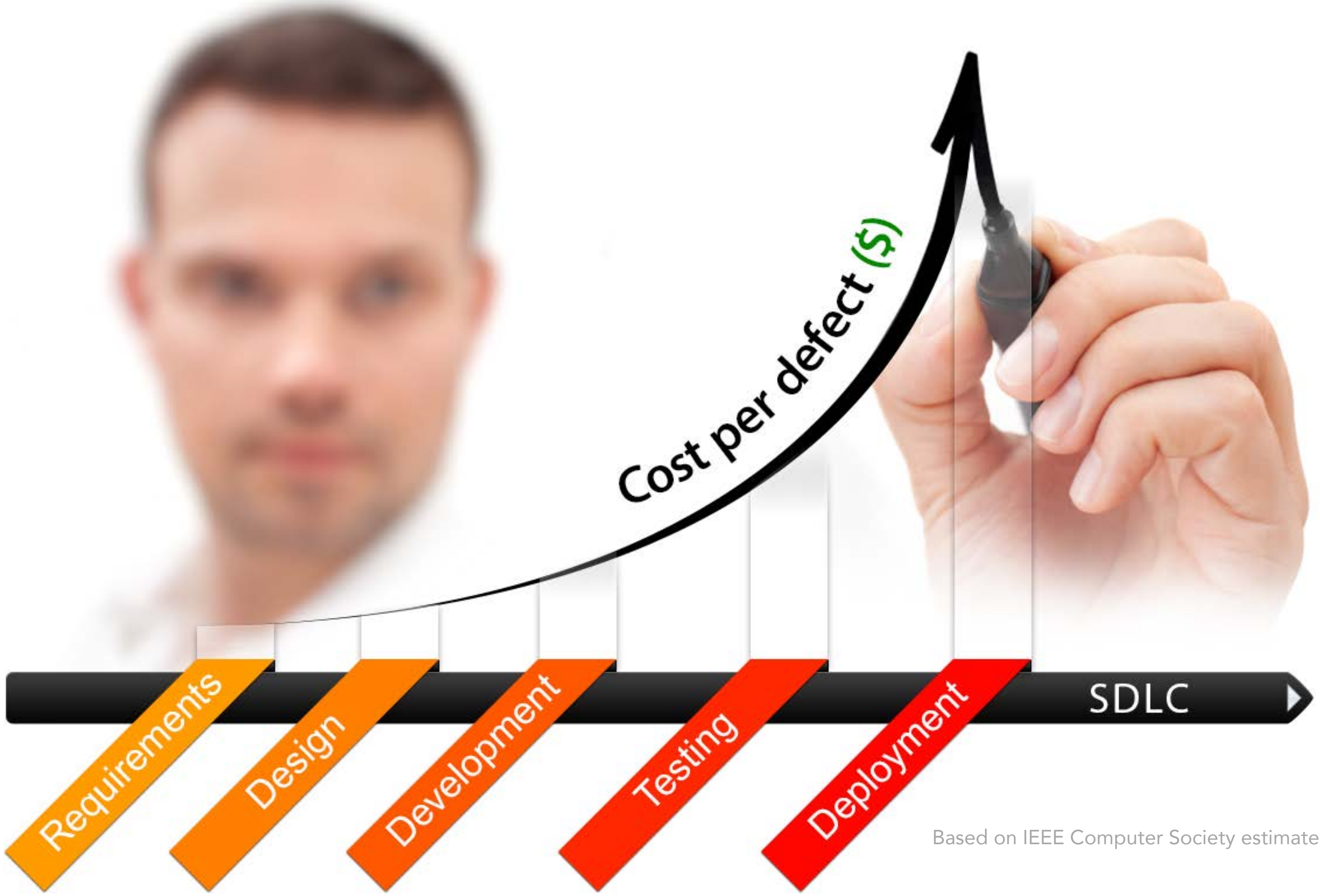
STRATEGIC INITIATIVES

Software Development Lifecycle Review

Software Assurance Maturity Modeling

Secure SDLC Program Development

Developer Security Training



Based on IEEE Computer Society estimates

Identify and remediate software vulnerabilities early and often to generate software maintenance savings that reduce overall development costs.

Application Security Assessment Services

WEB MOBILE IOT DESKTOP APPLIANCE

TACTICAL ACTIVITIES

- Penetration Testing
- Security Code Review
- Developer Interviews
- Threat Modeling
- Requirements Mapping

STRATEGIC INITIATIVES

- Software Development Lifecycle Review
- Software Assurance Maturity Modeling
- Secure SDLC Program Development
- Developer Security Training

Praetorian follows the OWASP ASVS standard, which normalizes the range in coverage and level of rigor applied to each application.

LEVEL 0
Cursory

Level 0 (or Cursory) is an optional certification, indicating that the application has passed some type of verification.

LEVEL 1
Opportunistic

Level 1 (or Opportunistic) certified applications adequately defend against security vulnerabilities that are easy to discover.

LEVEL 2
Standard

Level 2 (or Standard) verified applications adequately defend against prevalent security vulnerabilities whose existence poses moderate-to-serious risk.

LEVEL 3
Advanced

Level 3 (or Advanced) certified applications adequately defend against advanced security vulnerabilities, and demonstrate principles of good security design.

Identify and remediate software vulnerabilities early and often to generate software maintenance savings that reduce overall development costs.

Application Security Assessment Services

WEB | MOBILE | IOT | DESKTOP | APPLIANCE

TACTICAL ACTIVITIES

Penetration Testing
Security Code Review
Developer Interviews
Threat Modeling
Requirements Mapping

STRATEGIC INITIATIVES

Software Development Lifecycle Review
Software Assurance Maturity Modeling
Secure SDLC Program Development
Developer Security Training

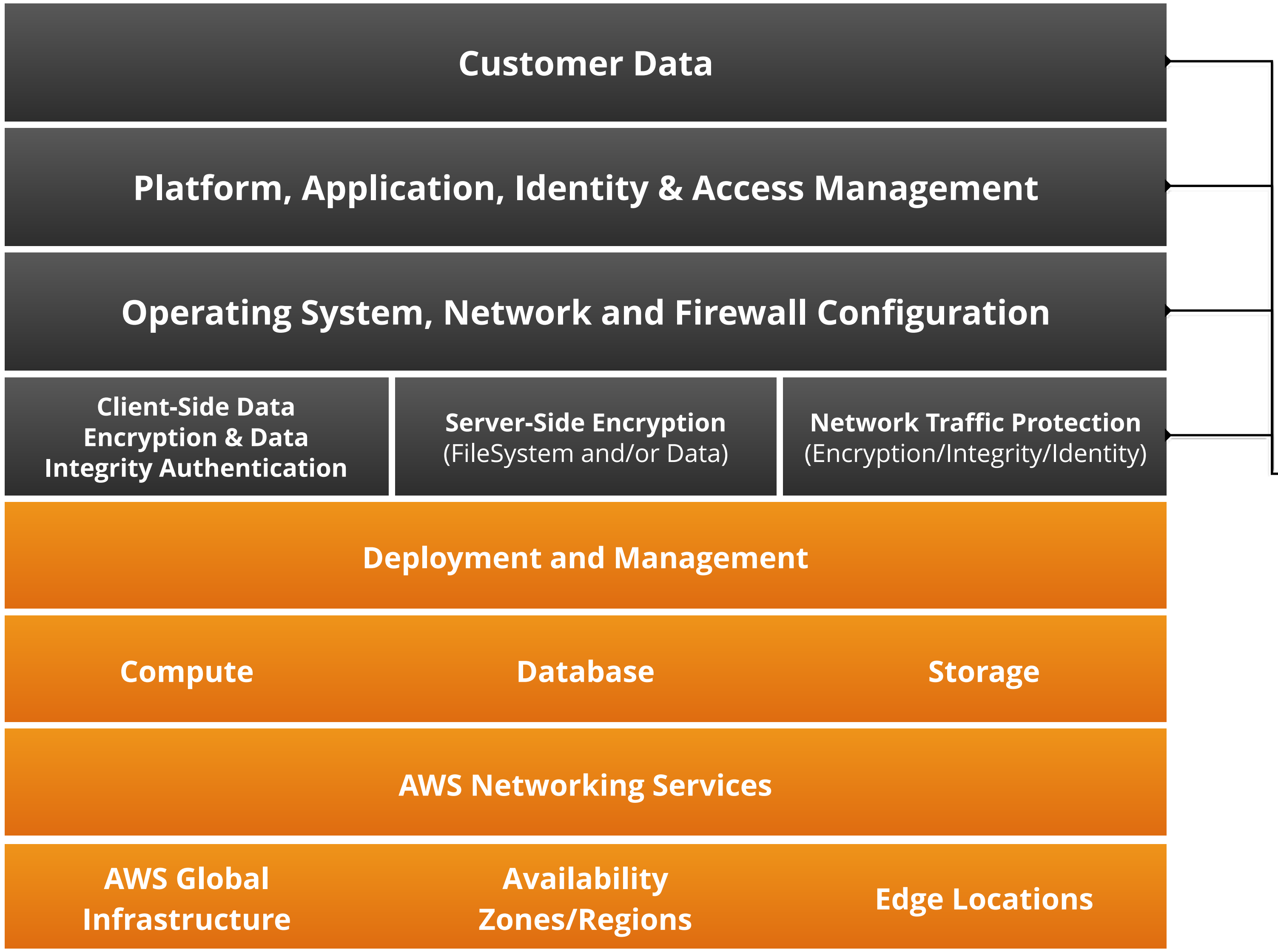
Praetorian follows the OWASP ASVS standard, which normalizes the range in coverage and level of rigor applied to each application.

OWASP ASVS defines the following security requirements areas:

- Authentication
- Session Management
- Access Control
- Malicious Input Handling
- Cryptography at Rest
- Error Handling and Logging
- Data Protection
- Communications Security
- HTTP Security
- Malicious Controls
- Business Logic
- File and Resource
- Mobile

Identify and remediate software vulnerabilities early and often to generate software maintenance savings that reduce overall development costs.

Cloud Security Assessment Services



Customer Data

Platform, Application, Identity & Access Management

Operating System, Network and Firewall Configuration

Client-Side Data Encryption & Data Integrity Authentication

Server-Side Encryption (FileSystem and/or Data)

Network Traffic Protection (Encryption/Integrity/Identity)

Deployment and Management

Compute

Database

Storage

AWS Networking Services

AWS Global Infrastructure

Availability Zones/Regions

Edge Locations

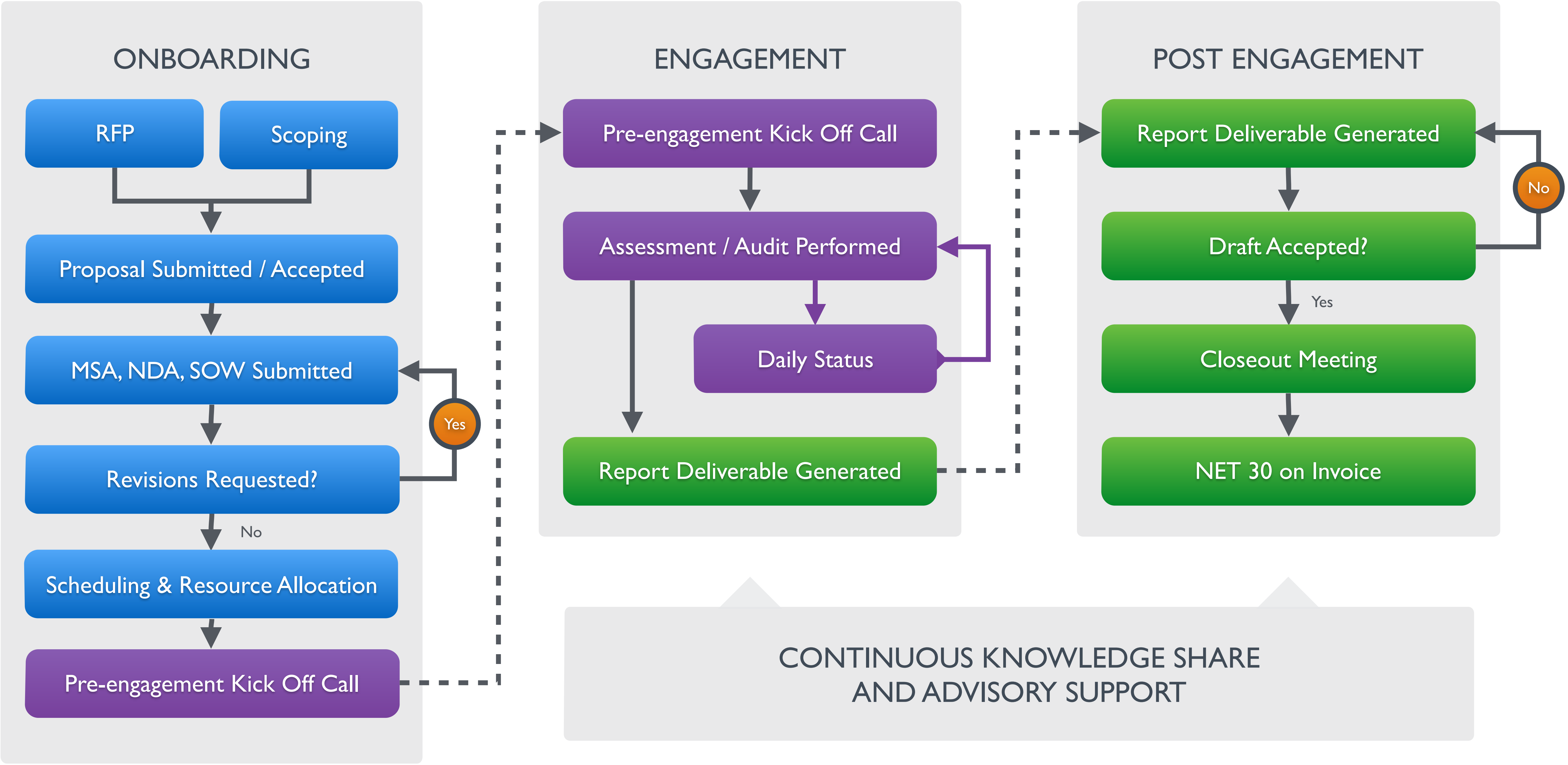
CLOUD SECURITY CONTROL REVIEWS

- Network Firewall Review
- Web Application Firewall
- Load Balancers
- Remote VPN
- Open DNS
- SIEM
- Intrusion Detection System
- Intrusion Prevention System
- Threat Prevention
- Cryptographic Accelerators
- Hardware Security Modules

MANY CLOUD PROVIDERS OWN THE RESPONSIBILITY OF DELIVERING A GLOBAL SECURE INFRASTRUCTURE AND SERVICES

Under a cloud provider's **shared responsibility model** you are responsible for protecting the confidentiality, integrity, and availability of your data.

Praetorian Engagement Workflow


ONBOARDING
RFP
Scoping
Proposal Submitted / Accepted
MSA, NDA, SOW Submitted
Yes
Revisions Requested?
No
Scheduling & Resource Allocation
Pre-engagement Kick Off Call
ENGAGEMENT
Pre-engagement Kick Off Call
Assessment / Audit Performed
Daily Status
Report Deliverable Generated
POST ENGAGEMENT
Report Deliverable Generated
No
Draft Accepted?
Yes
Closeout Meeting
NET 30 on Invoice
CONTINUOUS KNOWLEDGE SHARE
AND ADVISORY SUPPORT

PRAETORIAN

Professional Services Overview

INFORMATION SECURITY ASSESSMENT AND ADVISORY

NETWORK

APPLICATION

MOBILE

CLOUD

IOT