Security

OVERVIEW

With the rise of cloud computing, another layer of data security has been introduced that must be understood, addressed, and proactively managed. As a result, many organizations today are fortifying their applications, using strong passwords and authentication measures, and implementing automated identity and governance procedures.

But that's not enough. Security policies and technology must be strategic, layered, dynamic, and interoperable with your critical applications. Security also needs to be tied in with inherently agile processes and maximum performance, rather than just helping you meet compliance requirements.

We guide you through the process of identifying risk, including shadow IT penetration, as well as building intrusion prevention, detection, and response strategies both in and out of the public cloud. Our experts help you implement and automate policy enforcement and architect an agile immune system to meet your critical business, governance, and compliance needs.

The First Step: Security Assesment

Creating awareness is the first step to developing a defensible security strategy. This typically starts with a Security Assessment specifically geared toward your industry, goals, and compliance requirements. During this process, we include an examination of Shadow IT and a micro and macro view of your public cloud usage. Our assessment helps you:

- Understand your information security risk and meet your critical business, governance, and compliance requirements.
- Gain dynamic visibility into Shadow IT penetration, contextual access controls, and application security.

The Second Step: Governance

Our diagnostic assessment results provoke critical answers to visibility, risk management, and threat detection, which lead to the second step in the process: Governance. Data Strategy and our clients work collaboratively to create a vendor risk assessment workflow, identifying control and remediation technologies along with integration to ingress/egress devices.

A significant subcomponent of our Security Team's work focuses on Identity Governance and Access (IGA) management. IGA is a main pillar of security, and addresses the organizational vulnerabilities and inefficiencies responsible for most data breaches.

Understand Shadow IT penetration, manage Security by user context at the application level, and address Cloud intrusion and protection.

CAPABILITIES & EXPERTISE

In addition to security engineers who specialize in CASB, we have engineers who have the following certifications:

- CISSP—Certified Information Systems Security Professional
- CPTE—Certified Penetration Testing Expert
- CEH—Certified Ethical Hacker
- CHCP—Certified Hacking and Countermeasures Professional
- CCE—Certified Computer Examiner
- CGEIT—Certified in the Governance of Enterprise Information Technology
- ISO/IEC 27001—Information Security Management System Lead Implementer
- CISM—Certified Information Security Manager
- CISA—Certified Information Systems Auditor
- PCI QSA—Qualified Security Assessor for Payment Card Industry GSEC —GIAC Security Essentials Certification
- CRISC—Certified in Risk and Information Systems Control
- FAIR—Certified Risk Analyst

SECURITY SERVICES

Based on your assessment, we provide a range of in-depth security services customized to your specific security needs and goals.

Security Labs

- Network Penetration Testing
- Vulnerability Scanning and Assessments
- Social Engineering
- Incident Response
- Digital Forensics
- Application Security

Advisory Services

- General Security Assessments
- Security strategy and risk register creation
- Gap Analysis and Risk Registry Operationalization
- PCI DSS and Payment Systems Risk Report
- HIPAA, HITECH, HyTRUST, ISO 27001, FFIEC, FISMA, NERC, CIP, FedRAMP, 3PAO SOC and SSAE 16 Assessments
- Cloud and Virtualization Security Strategies
- Policy and Procedure Development

Business Continuity

- Active/Active Data Centers
- Disaster Avoidance
- Disaster Recovery
- Offsite Replication
- Backup & Archiving
- Recovery Optimization including Cloud-based
- Runbook Automation

Security as a Service

- APT and Behavior Analytics
- Data loss / leak prevention
- Intrusion Detection and Response
- Identity and Access Management on premise and in the cloud
- Multi-Factor Authentication
- BYOD & Mobile Device Management; MDM/EMM
- Distributed Firewalls | North/South & East/West
- Proxies and Unified Threat Management services
- Antivirus & Malware

CASB SERVICES

Cloud Access Security Brokers (CASB) are on-premise or cloud-based software solutions that serve as a control point to secure cloud services. CASB solutions offer encryption, auditing, data loss prevention (DLP), access control, and anomaly detection services.

Data Strategy implements solutions based on software from leading CASB provider Skyhigh Networks, which offers solutions used by 15 million users in 450 enterprises. Our CASB use cases include:

- Visibility and portfolio management for all sanctioned and unsanctioned cloud services, across all devices
- Detection and alerting on anomalous human and packet behavior, via data correlation analytics and heuristic machine learning across 30 million+ users
- Automated policy creation and application
- Auto-creation of blocking scripts and/or automated blocking of high risk or unsanctioned services
- DLP, Encryption, and access controls for cloud services

THE RESULT: A LAYERED SYSTEM TO PROTECT YOUR DATA

Using our unique approach and expertise in Cloud Security, Data Strategy operationalizes risk, governance, compliance, and security technologies and policies to the Cloud Service Providers (CSPs) in use across your organization. We even help you extend the most stringent DLP, Encryption, and Access Controls to your mission critical CSPs.

The end result? A complete organizational immune system, comprised of new policies, tools, and automation focused on data risk, compliance, governance, and enterprise security. This work future-proofs data from breaches, facilitates adherence to regulatory requirements, and detects and prevents compromised accounts and insider threats.