Silicon Valley Technology

siliconvalleytec.com

Cyber Security

Dramatically increase your profit margins by offering cyber security services that are in high demand.

Expand your client base by focusing on security conscious verticals including trading exchanges, credit card processing, insurance, healthcare, streaming, gaming, and gambling.

We provide fully managed cloud-based security services with 24 x 7 support.

Sales training is provided to quickly help you reach new clients and accelerate new revenues.

.

.

ISPs and Data Center operators can dramatically create more profitable business models, attract new clients, and grow ARR revenues by providing managed cyber security services.

The security market is rapidly growing and is expected to reach $80 billion in US spending in 2023.

Cyber security products provide new avenues into high growth markets and generate repeatable ARR revenue.

Cyber security solutions expand your reach to acquire new clients as your lead product offering.

Each of our automated Cyber product portfolio products is fully managed and supported 24 x 7. Our professional services staff detect and mitigate the attacks on your clients' environments.

For compliance requirements, our MazeBolt offering will detect open vulnerabilities across your applications. The vulnerabilities can then be closed and remediated providing a secure environment for production DDoS testing.

MazeBolt
DDoS Vulnerability Testing

Mazebolt detects application DDoS vulnerabilities utilizing non-intrusive testing technology. DDoS services have no awareness of any changes to the environments they are protecting. This leaves many vulnerabilities hidden and unknown which can be exploited.

Mazebolt runs thousands of DDoS simulations against production services, to remediate open vulnerabilities, before they can be attacked.

Radware
Cyber Security Services

DDoS
Fully managed 24 x7 service providing Data Center hosted applications protection from volumetric DDoS attacks. Automatically identifies and blocks all attacks, including zero-day attacks, in less than 12 seconds. The only security solution that protects against volumetric RPS attacks.

Web Application Firewall
Keep your clients' applications secure in your data center and in the cloud. Blocking signatures are learned automatically based on monitoring normal use of the application. Any traffic that does not fit normal use of the application is blocked.

BOTs
Intelligent 4th and 5th generation BOTs are extremely difficult to detect. Our powerful algorithms analyze BOT specific behavior to determine if the user is human or a BOT. BOT controlled attacks are then blocked freeing up server resources to restore services.

API Security
Radware API maps the API attack surface by leveraging an automated discovery algorithm to discover API's and generate tailored security policies to detect and block API focused attacks in real time. It also uses a combination of access controls, data leakage prevention, BOT management and DoS mitigation to protect against the growing array of API security threats.