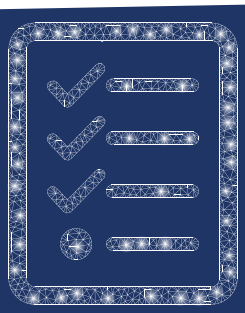
RISK ASSESSMENT



ARE YOU CONFIDENT YOU'RE SPENDING CORRECTLY?

Our expert security engineers are trained to quickly discover and reduce risk, and our efficient, compliant processes will meet the necessary requirements for your industry. Additionaly, our buy-in allows leaders and tech to get on the same page for intelligent spending. On average, cybersecurity makes up only 8% of the IT budget. Here are the top security spending drivers:

63%	56%	31%
PROTECTIVE OF SENSITIVE DATA	REGULATORY COMPLIANCE	REDUCING INCIDENTS & BREACHES

OUR 5 PHASES OF RISK ASSESSMENT

1 - DATA COLLECTION

A review of your existing information and documentation, including - but not limited to - general enviornment, existing security policies, procedures and known vulnerabilities.

2 - INTERVIEW

Meeting with key individuals to ask security-related questions. This phase enables us to understand how your organization currently deals with information security controls and management.

3 - EXAMINATION

As assessment of your organization for technical and non-technical vulnerabilities. This on-site portion of the assessment evaluates both strengths and weaknesses within your organization.

4 - EVALUATION

A compilation of your data and analysis of the results. These results are then compared to standard security requirements, recommended and configurations and security benchmarks.

5 - REPORTING

A formal report containing an overview of the risks identified and recommended solutions is delivered to the client at the end of the process.