cloudpurge.

API PROTECTION DATA SHEET

About CLOUDPURGE

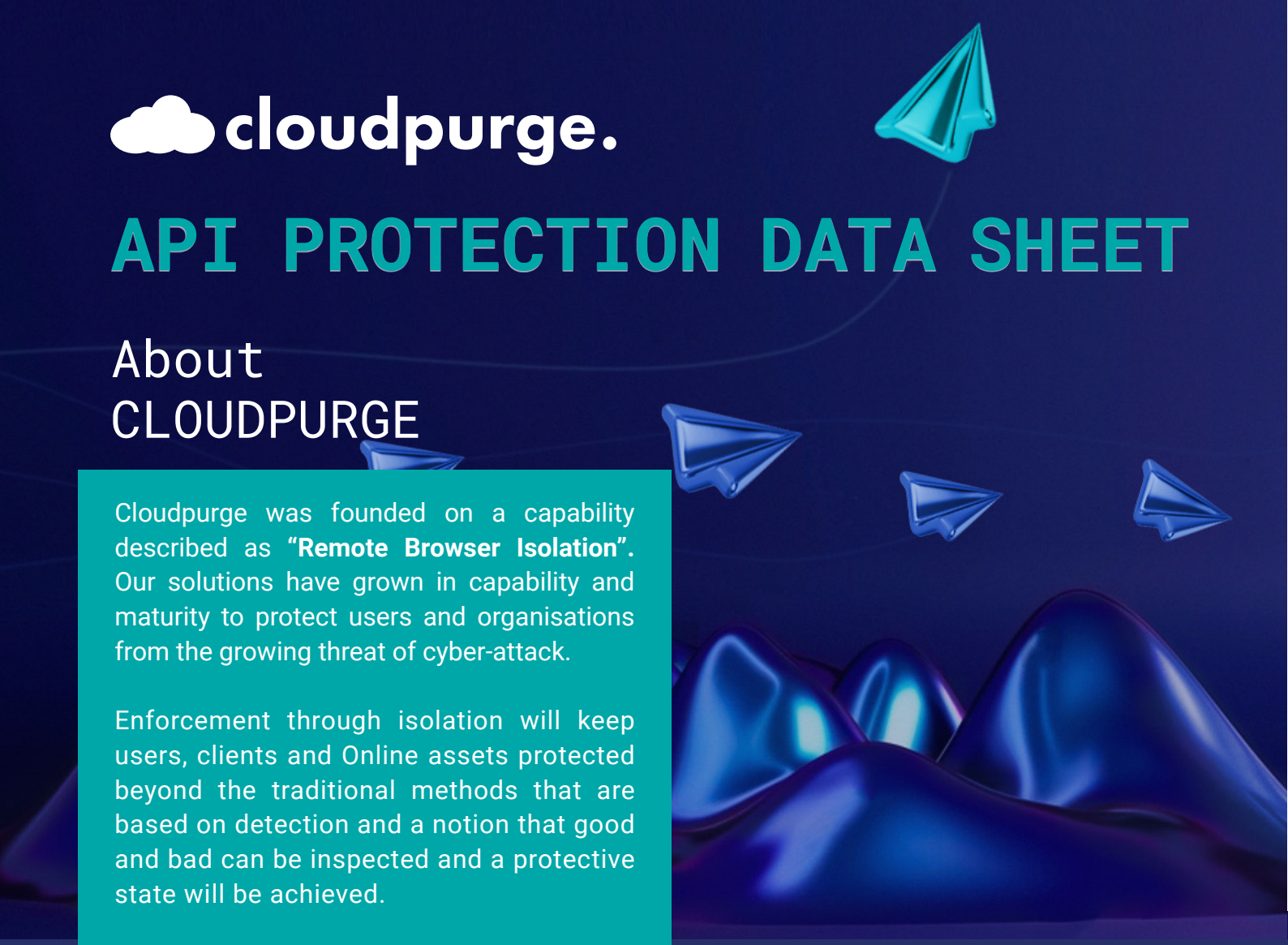
Cloudpurge was founded on a capability described as **"Remote Browser Isolation".** Our solutions have grown in capability and maturity to protect users and organisations from the growing threat of cyber-attack.

Enforcement through isolation will keep users, clients and Online assets protected beyond the traditional methods that are based on detection and a notion that good and bad can be inspected and a protective state will be achieved.

The approach of Good Vs Bad is always going to be challenged, the dynamic state of emerging technology trends and threats and the requirement and dependency for more specialised resources to manage these numerous technologies is now just overwhelming for most organisation.

The Security community and market are becoming fatigued, a 2022 ESG report (1) has a large representation of organisations claim that security tools designed to protect corporate applications can often add complexity, Specifically, 36% say security tools are ineffective and 32% indicated their organisation had too many security tools.

Cloudpurge will change the game, we will play on our terms and now address this feedback with solutions that deliver outcomes that can be measured whilst providing unparalleled simplicity and protection.



The API LANDSCAPE

APIs provide a foundation for innovation and digital transformation, and this will only continue to grow given the flexible nature of the accelerated engagement possibilities that are now offered.

This value is undeniable, but so is the realization that this now creates for a highly prized and very focused and targeted attack vector. API breaches are common, and securing your APIs requires holistic architecture across the software development lifecycle and **ensuring the right security controls are deployed.**

KEY FEATURES

Discovery

Understand your Risk

- **Where is the Risk?**
  Provide clear context on Risk and remediation Strategies to be applied.
- **Build a Baseline**
  Understand what is normal and build a baseline to measure against

Prevention

End to End Protection including

- **WAF**
  A fully Managed WAF to provide Gateway Control
- **Authentication**
  Pre-Existing can be implemented or Cloudpurge provided
- **File Scanning**
  Inbound/Outbound
- **DLP**
  Data is uniquely weighed. Exfiltration Capture.
- **Machine Learning**
  AI approach to enhance protection and behavior.
- **Encryption**
  The only communication to backend API Server is via an encrypted channel between our Isolator.
- **Event Logging**
  Onforwarding of Events into Logging or SIEM Engine for Analyst review in Real Time

Remediation

Deviation from normal is immediately flagged, all whilst still being protected

- **Dev Ops Feed** (CI/CD Pipeline)

OUR APPROACH

cloudpurge.

With 57% of organizations of the view that they will use API's in most of their applications, the delivery and impact on business and business systems is a major consideration the opportunity to immediately protect exposed APIs against the threat of a malicious attack has never been simpler with Out Of the Box Protection with Cloudpurge API Protection.

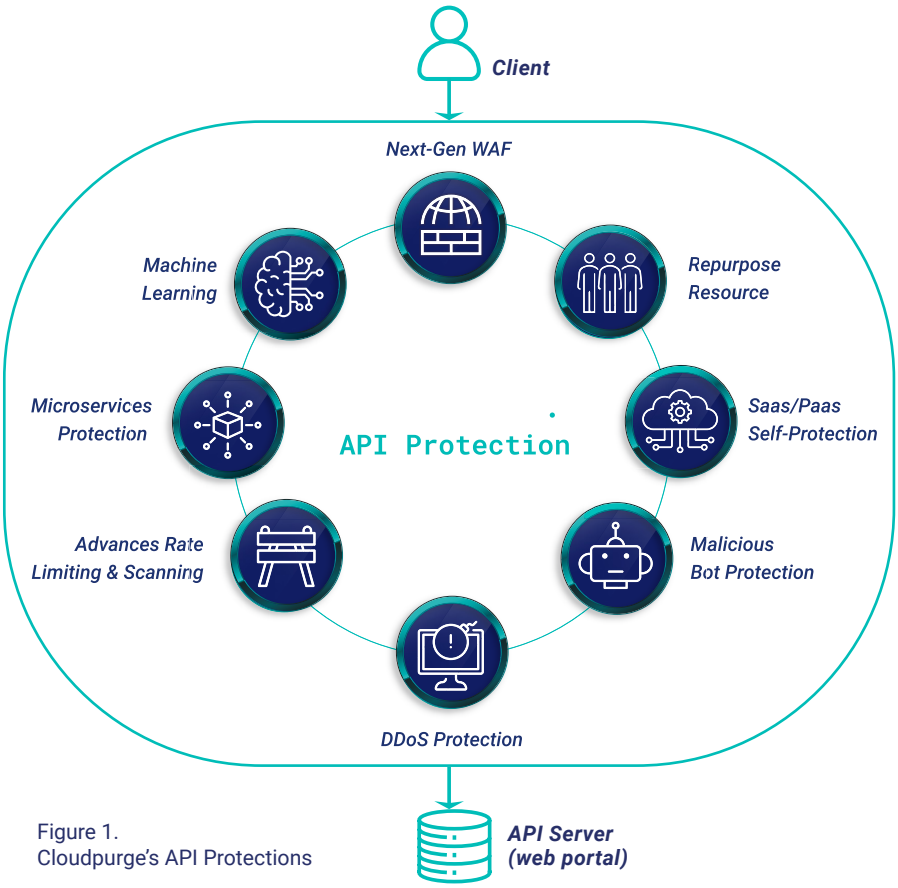


Figure 1.
Cloudpurge's API Protections

A key difference in the approach we have taken is to limit the exposure of a direct connection between the client and the API server. We have built the platform to encompass a number of strict controls that collectively offer clients an End-to-End API Protection strategy.

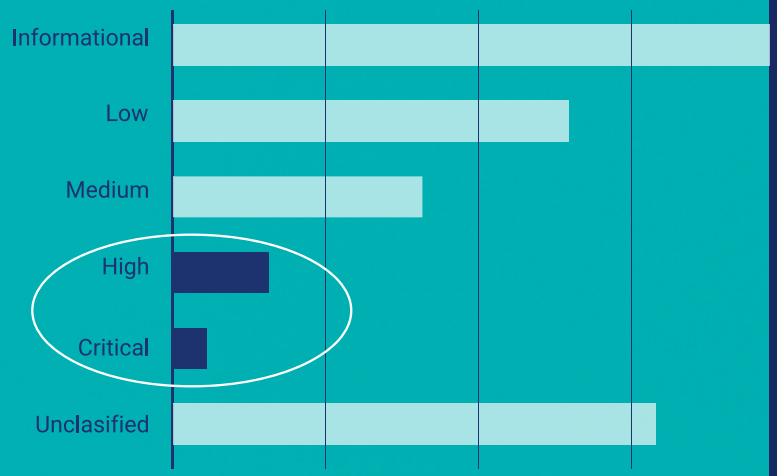
We monitor inbound and outbound activity, our visibility is reflected in the customizable dashboards offered through the client Admin Portal. Reports can be extracted and integration to CI/CD pipelines or a JIRA Backlog can be facilitated for Dev Ops Teams.

BEFORE & AFTER CLOUDPURGE

cloudpurge.

WITHOUT

cloudpurge.



WITH

cloudpurge.

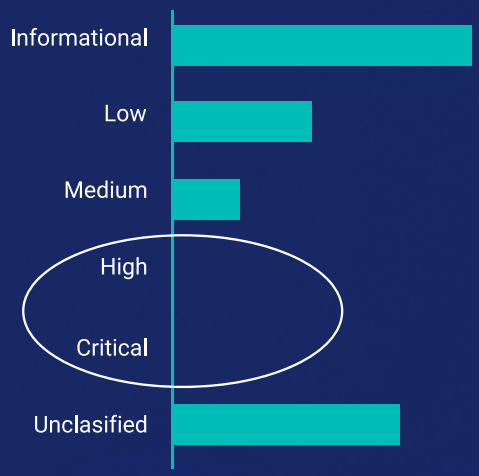


Fig 2 Before & After Exposed Vulnerabilities (Sample Report)

SOLUTION CAPABILITY

- **Simplified Deployment**
- **Operate in a Protected**
- **Ecosystem**
- **Measure the Value**
- **Fully Manages Security Offering**
- **Hands Off Approach to Cyber**

All Organizations encounter a persistent and growing list of cyber exposures that demand immediate attention. Despite their best efforts, the rate at which new critical exposures surface exceeds the pace at which security teams can address them. Consequently, staying ahead of the game is a daunting task, and a remediation backlog exists where the number of vulnerabilities far outstrips the capacity to remediate them in a timely manner, if at all. It's not sufficient for Dev Ops and Security teams to acquire more visibility and more security tools. What they need is a fresh remediation strategy that immediately empowers them to outpace the attacker and not disrupt the business operations.

What is needed is a fresh remediation strategy that immediately empowers organisations to outpace the attacker and not disrupt the business operations.

Contact us for a free Demonstration | Cloudpurge.com