# Cyberlytic

# Intelligent Web Application Security

**High profile media cases show that relying on conventional web application firewalls is ineffective. Conventional firewalls rely on manually updated rules and curated "RegEx" lists of known attack signatures. Whilst signature detection is important, it is not nearly enough to keep a company safe. Zero-Day attacks and polymorphic code will defeat these reactive, signature-based products.**

Once detected, most security solutions rely on the skill and expertise of security teams to identify which attacks are high risk amongst the vast majority that are not. This business critical triage function is typically subjective and inconsistent. As the volume of attacks continues to grow, it becomes infeasible for cyber security teams to reliably and accurately assess the risk of every alert.

Cyberlytic offers a revolutionary approach to detecting and preventing web injection attacks, such as SQL injection and cross-site scripting (XSS). The **Profiler** is an expert learning threat detection tool that uniquely prioritises attacks depending on the risk they pose to your data. Because it does not use rules or signatures, it will detect attacks overlooked by conventional web application firewalls and allows security teams to respond immediately to high-risk attacks. Risk impact reports provide senior management with a concise overview of their web application security activity and the information security risk situation.

The **Defender** is an intelligent, cloud-based firewall that protects web servers from threats, by applying Cyberlytic's patented machine learning algorithms.

Both products are designed to be used either as a standalone web application security solution or integrated to improve detection and intelligence of existing security systems.

> "Cyberlytic's innovative approach to web application security is disruptive and will challenge more established players to think about their own approach"
>
> – PwC, Cyber Threat Detection and Response

## Detection

"The UK is the fourth most targeted country for web application attacks. SQL Injection attacks have risen 62 percent since the previous year and are up 19 percent since the last quarter alone."
SC Magazine Nov 2017

Cyberlytic's patented machine learning algorithms provide advanced, self-learning threat detection.

## Zero Maintenance

82% of respondents report a shortage of cybersecurity skills.

71% of respondents report the shortage in cybersecurity skills does direct and measurable damage.
McAfee Report 2017

Cyberlytic products that are easy to deploy and require minimal maintenance to operate.

## Visibility

"You should put procedures in place to effectively detect, report and investigate a personal data breach. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself."
Information Commissioners Office

With GDPR organisations need to imrpove situational awareness. Risk-based compliance reporting demonstrates web compliance.

Cyberlytic
intelligent web application security

For more information contact:
info@cyberlytic.com | +44(0) 203 290 0011 | www.cyberlytic.com

Cyber security supplier to: HM Government

"Cyberlytic was founded on the belief that security intelligence should enable security teams to be more efficient and reduce the demand on human operators. Through research originally completed for the UK Ministry of Defence, Cyberlytic is the originator and owner of intellectual property relating to real-time risk assessment and prioritisation of cyber-attacks"

## Features

### AI for Anomaly Detection & Classification

- Detects web injection attacks without the creation or maintenance of firewall rules
- Detects sophisticated and zero-day web injection attacks
- DDOS protection
- Machine learning continuously learns and adapts to your web server environment, reducing risk of compromise

### Team Efficiency

- Cloud deployment. No local integration required
- Instant web threat protection
- Zero-maintenance and simple training
- Configurable alerting to respond to dangerous attacks

### Visibility of Threats

- Real-time risk assessment of all web traffic
- Compliance reports provide a clear picture of historic attack activity
- Intuitive interface and presentation of data for incident response

"The data science based approach that Cyberlytic has adopted to create the Cyber Threat Profiler, helps us protect our application servers against the most sophisticated attacks"

– Stephen Jackson, Head of Internal Systems, Tessella Limited

## Benefits

### Attacks are prioritised

- Detects web injection attacks without the creation or maintenance of firewall rules
- Can detect polymorphic and zero-day web injection attacks
- Machine learning continues to improve the accuracy of the analytics engine, further reducing the risk of compromise

### Actionable Intelligence

- Effectively triages false positives and detects anomalous web traffic
- Classifies web injection attacks to determine the risk in an efficient and consistent manner
- Increases the efficiency of critical IT resources

### Improves existing security strategies

- Demonstrates effective security controls and security compliance
- Impact reports offer management a clear picture of recent attack activity and InfoSec risk
- Compatible with and complementary to existing SIEMs
- Increases ROI of existing security solutions

Cyberlytic
Intelligent web application security

For more information contact:
info@cyberlytic.com | +44(0) 203 290 0011 | www.cyberlytic.com

Cyber security supplier to: HM Government