SASE & Zero Trust Network Access
- Full stack security moves to the cloud, using an optimised private global network with Zero Trust Network Access to replace legacy VPNs.

- Users have access only to the applications that they need, when they need them, with adaptive authentication. Security, performance, cloud scalability.

Attack Surface Management
Understand and manage your internet and network assets. Endpoints, IoT devices, websites… What do you have? Is everything correctly patched and configured?

Web Application Firewall (WAF)
WAF with specialised modules for RASP (Runtime Application Self Protection) and management of DoS/DDoS attacks and 'bad bots'

SaaS Security Posture Management
Proactively find and remediate weaknesses across your SaaS platforms, and maintain continuous security for all global settings and user privileges

Brand intelligence and online threat management
Fake websites and typosquat domains, malicious activity on social media and dark web forums, brand mentions and impersonations. Discover, monitor and take down online threats against your organisation.

Data protection and insider threat detection
Discover, classify and manage access to sensitive data; compliance with data privacy regulations and security frameworks

XDR (Extended Detection and Response)
Behavioural analysis and data correlation across all endpoints and operating systems for a complete picture of activity on your network. Better than a SIEM?

OT/Industrial Control Systems (ICS) Security
Discover, classify and assess connected assets on your OT network and mitigate threats to them; industrial implementation of Zero Trust including dynamic network segmentation

Security Testing
Breach Attack Simulation (BAS) tests your organisation's defences along the attack chain - including the lateral movement and data exfiltration stages.

Crowd sourced penetration testing that combines human ingenuity and flexibility with the thoroughness of automated approaches

(Updated: November 2021)

Kiowa
INFORMATION SECURITY