MANAGED APPLICATION DELIVERY, SECURITY & ACCESS

KEY BENEFITS & DELIVERABLES

- **Incident Alert:** Identification and notification of issues related to device availability
- **Proactive Monitoring:** 24x7x365 pro-active monitoring of key device metrics
- **Help Desk Support:** 24x7x365 help desk support to remediate issues in normal operation of scoped appliances
- **Patching, Updates & Upgrades:** Where performed remotely, full deployment of patches, updates and upgrades to the device specific software
- **Change Assessment:** Assessment of risk to business-as-usual by requested changes
- **Change Management:**
  a) In coordination with change processes and change windows specific to the customer business and,
  b) Assisting with the creation and implementation of changes
- **Business Continuity:** Weekly backups of device policies and hardware configuration

SERVICE DESCRIPTION

Applications, both web- and discreet, are the life blood of most organisations, serving customers, third parties, partners and internal users on a 24x7x365 basis. It is therefore business-critical that they are able to be delivered on-demand. Applications are also a primary source of risk for organisations, with hackers targeting applications in increasingly sophisticated ways

Application availability & load balancing solutions judge routing decisions based on the content of the application, availability of the application's host servers, where the requests originate from, network conditions and several additional factors. This reduces response times, maximises throughput and makes optimal use of available resources

Application Security goes beyond traditional network firewalling providing control at the application layer. This security is brought about by configuring rules based on applications such as: -

- which users should have access from which devices
- rules based on application behaviour and structure
- geolocation rules allowing or restricting access by country or region
- DoS and DDoS rules preventing applications from being taken offline
- SSL traffic inspection

Application Access refers to creating and maintaining granular controls to ensure that only permitted users have access to discreet applications. These applications may be internal to the organisation or public-facing, such as Outlook Web Access, but need to have tight access restrictions imposed on their use.

KEY SERVICE COMPONENTS

Application Delivery Management Components

- Application and on-going management of separate client-server architecture(s) ensuring optimised application delivery
- Provision of application-server performance visibility displaying response times, network conditions & user context
- Implementation and on-going management of up to 39 monitors to detect application delivery latency or failure
- Creation and maintenance of custom scripts for bespoke application delivery (additional charges may apply)
- Application Traffic Management with intelligent static and dynamic load-balancing to eliminate single points of failure
- Implementation and on-going management of up to 19 delivery methods ensuring reliable delivery and availability
- Ongoing monitoring of synchronisation status to ensure transparent failover through connection mirroring

Application Security Management Components

- Implementation and management of attack signatures, including the OWASP Top Ten, as released by the vendor and in accordance with customer change-control processes
- Management of IP intelligence linked with IP shunning (accelerated blacklisting) protecting from malicious sources
- Implementation and management of application-layer DoS and DDoS detections
- Implementation and management of 'virtual-patching' signatures to protect application servers' Operating Systems or web-server layers until patched as requested by the customer
- Ongoing application-policy tuning enabling rapid detection of & protection against emerging threats (additional charges may apply)
- Installation of SSL certificates and ongoing monitoring of certificate validity
- Implementation of SSL termination policies, allowing inspection and mitigation of concealed threats
- Ongoing application awareness, monitoring client connections and server responses to mitigate threats based on security and application parameters

Application Access Management Components

- Provisioning and on-going management of secure remote- and mobile access to corporate resources from all networks and devices
- Definition and management of multi-layered profiles allowing access to different resources for users depending on the device type, authentication mechanism, location or device security status
- Definition and on-going management of access policies for authentication and authorisation to enforce user compliance with corporate policies and industry regulations
- Host checking functionality that ensures connecting devices comply with defined requirements and blocks or limits access by at-risk devices
- Configuration of flexible single sign-on & identity federation support allowing authenticated users automatic sign-on to back-end applications and services
- Installation of SSL certificates and ongoing monitoring of certificate validity

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com