MANAGED CONTENT FILTERING

KEY SERVICE COMPONENTS

Email Content Filtering

- Ongoing addition, modification and removal of customer's filtered email domains
- Ongoing management of enforced email encryption**
- Policy management of email content filters governing: -
  - o Unsolicited Bulk Email (UBE)
  - o Spam detection policy controls and alerts
  - o Anti-malware policy controls and alerts
  - o Image controls (applies to images in email content)
  - o Impersonation controls
  - o URL filtering (applies to URLs in email content) controls
  - o Sandbox delay controls
  - o Geo-location controls
  - o Data protection and compliance controls for vendor predefined templates (custom data-protection templates may be provided at additional Professional Services charges)
- Domain/Sender/Recipient/Destination whitelisting and blacklisting
- Auto-remediation and Clawback controls (applies to delayed removal of emails & attachments found to be malicious post-delivery)

Web Content Filtering

- Ongoing management of access- and URL filtering policies
- Custom Proxy Auto-Configuration (PAC) file creation and maintenance
- Custom Whitelist and Blacklist creation and ongoing maintenance
- Custom 'Block Page' creation and maintenance
- Ongoing management of antivirus/antimalware policies
- Management of remote user's VPN content security policies
- Ongoing management of web isolation policies enforcing potentially hazardous websites to be opened in contained, cloud-based environments disabling active

Data Loss Prevention

- Management of vendor-provided compliance-based policies (custom policy creation and management may incur additional Professional Service charges)
- Whitelisting of false-positive blocked files

SERVICE DESCRIPTION

With the web browser and email reader the frequent target of hackers and social engineering, the rise of malicious web sites and emails has been exponential. Content security has traditionally been thought of in the context of protecting against HTTP & HTTPS web traffic, the lines between browser-delivered content and mail-client delivered content have blurred with HTML email just as much a target as HTML webpages.

Content filtering does not necessarily only apply to inbound web- or email traffic however. Outbound filtering, as part of a holistic approach to 'Content', mandates that documents and spreadsheets being sent to Software-as-a-Service (SaaS) applications, hosted Infrastructure-as-a-Service (IaaS), hosted Platforms-as-a-Service (PaaS) and third parties be filtered so that confidential information isn't published or shared in violation of regulatory compliance obligations or corporate policy.

The pace of change of content filtering technologies and the overhead for managing upgrades, patches and rule changes requires skills many companies don't have. Our fully managed Content Filtering service removes the complexity of continuous rule-base management allowing in-house IT teams to focus on the tasks the business needs. The service increases visibility into user behaviour, network- and application-layer traffic with the intention of extending protection against web-based and mail-client attacks thereby reducing the risk of malware infection. The services further extend to exposing outbound content to the IT team and preventing egress of sensitive data.

KEY BENEFITS & DELIVERABLES

- **Incident Alert:** Identification and notification of issues related to device availability
- **Proactive Monitoring**: Subject to contract, 24x7x365 proactive monitoring of key device metrics
- **Service-desk Support:** Subject to contract, 24x7x365 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) Assistance with the creation and implementation of changes
- **Business continuity:** Weekly backups of device policies and hardware configuration

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