SECUREDATA
TRUSTED CYBERSECURITY EXPERTS

Symantec

MANAGED CONTENT FILTERING

KEY FEATURES & BENEFITS

- Reduces malware risk: An estimated 92% of malware is delivered via email[1]. Filtering email reduces the risk of spyware, ransomware or cryptominer infection
- Maintains regulatory compliance: Compromise via spyware leading to data theft, or distribution of confidential information by employees, may result in violation of regulatory compliance obligations. Filtering of inbound and outbound traffic minimizes the risk of prosecution
- Enhances user-behaviour visibility: Reporting on websites visited, SaaS applications being used and document uploads reveals potentially hazardous user behaviour
- Increases productivity: Web- & email content filtering prevents employees spending hours cleansing inboxes of spam and excessive use of non-work related websites
- Improves infrastructure performance: Disallowing access to streaming or video-on-demand content reduces bandwidth consumption

[1]Verizon DBIR 2018

SERVICE DESCRIPTION

Content security has traditionally been thought of in the context of protecting against HTTP & HTTPS web traffic but the lines between browser-delivered content and mail-client delivered content have blurred with HTML email just as much a target as HTML webpages.

Web content security devices are the best way of enabling secure access to web content by inspecting web traffic for malicious content thereby enforcing corporate Internet browsing policies.

Email filtering solutions similarly bring an additional layer of security to content delivery by filtering out the majority of unsolicited email whether in the form of marketing-related spam, email content containing hyperlinks to legitimate-looking malicious or emails containing malware disguised in harmless looking documents and spreadsheets.

Content filtering does not necessarily only apply to inbound traffic however. Outbound filtering, as part of a holistic approach to 'Content', mandates that documents uploaded 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.

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 and, through filtering of outbound content, the risk of compliance violation through the malicious or unintentional distribution of confidential information.

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

TECHNICAL COMPONENTS

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 connections allowing content security policies to be enforced on office-based and remotely connected users
- Ongoing management of web isolation policies enforcing potentially hazardous websites to be opened in contained cloud-based environments disabling active content from running in web browsers**
- Web browsing / Download performance speed monitoring (subject to dedicated AffinitySECURE system being in place)

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 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

Cloud Access Audit & Filtering

Ongoing management of policies enforcing**: -

- o Accessible/blocked SaaS and IaaS environments
- o Files allowed to be uploaded or downloaded from SaaS and IaaS environments
- o Content (e.g. audio, video, attachments, instant-messaging) permitted

- Ongoing management of email content uploaded or downloaded from SaaS environments**

Date 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

* Additional Professional Service charges may apply.

** Subject to technology/licenses purchased

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

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 Threat Advisory service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who will deal with incidents affecting attempted access to and help ensure continuous availability.

Extensive security insight
SecureData's Greater Intelligence platform processes over 30 billion 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 mindset. We use this information to ensure our Managed Threat Advisory customers are as secure as they possibly can be.

Vendor insights
Our close partnership with numerous vendors 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 Threat Advisory service and strengthen your security posture, including Managed Firewall, 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 CONSULTANCY

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