HUGHES SECURITY

WORLD CLASS PROTECTION FOR MEDIUM SIZED BUSINESSES

HughesON™

MULTI-PRONGED PROTECTION FOR YOUR BUSINESS

Whether you store data on premise or in the cloud, it is vulnerable to accidental or malicious deletion, ransomware and other types of data loss.

The sheer volume of cyberattacks is staggering. Microsoft stops 300 million fraudulent sign-in attempts every day. Billions of potentially malicious emails are sent out daily. It only takes one of them to get through to cause damage – which could cost you a fortune in data loss, downtime or the consequences of privacy breaches. Every 11 seconds, a business suffers a ransomware attack.

Small and medium-sized businesses are especially vulnerable. But most lack the budget, knowledge, and in-house IT expertise to protect themselves. Cybersecurity specialists are scarce and in high demand – and they command very high salaries.

Hughes Network Systems Europe now makes it possible for you to protect your business with Security Operations Centre (SOC) Business Continuity Services and Managed Firewall.

MANY COMPANIES HAVE BEEN THE VICTIMS OF CYBERATTACKS AND WE KNOW THE RISKS. A SECURITY BREACH CAN CAUSE DATA LOSS, LOSS OF CUSTOMERS, LOST PRODUCTIVITY AND DAMAGE TO YOUR REPUTATION.

A COMPLETE SOC WITHOUT THE COST AND OVERHEAD

The high hardware and software cost of cybersecurity alone is daunting, but even more expensive is the process of recruiting, training, and retaining a team of qualified cybersecurity analysts. Instead of building a security operations centre (SOC) on your own with finite resources, **Hughes SOC-as-a-Service** enables you to fortify your defences quickly across distributed sites.

With Hughes SOC-as-a-Service you get the full range of SOC functions via the cloud, together with the expertise and close attention of cybersecurity specialists. You can feel safe and secure in the knowledge that you have given your company world-class protection round the clock at a transparent and manageable cost.

Comprehensive Protection & Incident Reporting

Hughes Europe delivers ISO-certified SOC-as-a-Service, together with planning, configuration, management, troubleshooting, ticketing, remediation and a customer portal. It is available to any site in Europe.

Our analysts work as an extension of your in-house IT team to understand your environment and proactively respond to threats as they occur.

Once up and running, our SOC experts monitor your IT assets via the EventTracker console on a 24/7/365 basis and provide daily or weekly summaries called Critical Observations Reports, escalating incidents per procedure.

They are also available to answer questions and provide support for incident review and forensics and audit assistance and conduct regular assessments and planning sessions of the service deliverables with your own managers through executive dashboard reviews.

The Hughes Europe Security Operations Centre (SOC) has been audited and formally certified as compliant with ISO/IEC 27001:2013.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

An extension to SOC, Security Information and Event Management (SIEM) uncovers the cyber threat intelligence hidden in your log data, helping you to identify actual threats and risks to your data and assets. By collecting and analysing log sources within your network, SIEM enables you to take preventive action against cyber threats.

SIEM enables you to gain actionable security intelligence with greater visibility and aggregation of events to secure your entire network and enable you to improve operational efficiency.

SIEM and log management capabilities provide the core of our threat protection platform, EventTracker, and empower threat detection with support for thousands of devices and applications.

Real Time Analysis for Proactive Security Alerts

SIEM platforms are tasked with monitoring an ever-increasing attack surface that encompasses physical servers, workstations, endpoints, and cloud infrastructure. To ensure your environment is safe, log and event data is logged and indexed for quick search, analysis, and alerts.

With in-depth analysis, proactive security alerts ensure your organisation quickly responds to any alarming anomalies or threats. To enable this, Hughes Europe security analysts build, maintain, and respond to rule-based alerts that are backed by dashboards, alert scores, contextualisation, and automated response capabilities.

Full Security Standards Compliance

Keeping up with changes in regulations and additions of new mandates can be time consuming, tedious, and if not done well, a dangerous liability for your organisation. SIEM can help you to reduce risk and improve operational efficiency by automating the steps required by various industry regulations and mandates.

With our combined SIEM, log management and SOC capabilities, organisations can secure the environment, establish the baseline, track user activity, alert on potential violations, and generate audit-ready reports to help with PCI DSS, HIPAA, ISO 27001, NIST 800-171, DoD, RMF, GDPR, and other compliance requirements.

PCI DSS Compliance

Managing PCI DSS (Payment Card Industry Data Security Standard) compliance for retail and hospitality chains can be a headache. Each location with point-of-sale systems and cardholder data needs both vigilant security and business agility. Managing network connectivity, cybersecurity, and compliance are all interrelated. Hughes helps you simplify compliance management and improve your brand's security posture while letting you get back to business.

Easier PCI DSS compliance management, in conjunction with firewall management and compliant network design, is available from Hughes Europe as a separate module. Get a comprehensive set of tools and expertise to simplify compliance across the enterprise, including franchise systems. With Hughes, you get a centralised portal for vulnerability scan management, network auditing, SAQ submission, robust file integrity monitoring, audit-ready reporting, and compliance support from experts.

ADDITIONAL CYBER SECURITY OPTIONS

For maximum protection, Hughes offers the following extensions to SOC and SIEM.

Endpoint Protection

Endpoint protection uses artificial intelligence to identify and block advanced threats. By blending endpoint protection and threat detection and response within a SOC-as-a-Service solution, we enable stronger yet simpler cybersecurity against so-called zero-day threats (ones that have not been previously identified), advanced persistent threats (APTs), ransomware, and file-less attacks – all with unmatched accuracy and speed.

Vulnerability Assessment Service (VAS)

With VAS the SOC works with you to identify and group assets, schedule scanning, and detect vulnerabilities on a monthly or quarterly basis. Reports and remediation recommendations are integrated into the dashboard for review. The Hughes SOC provides trend reports showing new, remediated, or unchanged vulnerabilities.
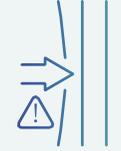
Intrusion Detection System (IDS)

As an additional layer of protection to any intrusion detection system (IDS) configurations already implemented in your firewall, the SOC installs EventTracker IDS to configure, tune, and maintain available rules to monitor your network. Alerts are integrated into the EventTracker console, which can launch notifications or implement auto-remediation actions.

Network Traffic Analysis (NTA)

EventTracker Network Traffic Analysis provides unparalleled visibility into your network threats and any security blind spots. It augments security analytics to provide an in-depth picture of cyber criminals and low-and-slow attacks that wait days or even months to launch. It provides customised and intuitive reports that quantify how your network is being used, by whom, and if suspicious traffic exists. Network Traffic Analysis also optimises your network, user, and application performance with rich context around attacks.

BUSINESS CONTINUITY

Do you store data in the cloud, for example in Microsoft 365 and Google Workspace? It's a good business decision to do so, but the popularity of these solutions also makes them a popular target for cyber criminals. The **Hughes Business Continuity** service provides a cost-effective way to minimise any disruption caused by a security breach.

Software-as-a-Service (SaaS) apps have fundamentally changed the way companies do business, enabling them to take advantage of economies of scale and reduce IT infrastructure costs. While these apps offer many advantages, one thing they can't do is completely protect your business data from external threats.

Large companies put in place disaster recovery facilities, typically servers in physically protected data centres that ensure business continuity in the event of security breaches and other seriously disruptive events. But this is prohibitively expensive for most companies.

Again, Hughes Network Services Europe has the answer, with Hughes SaaS Protection. This provides simple, automated and secure backup. With this solution and our expert help, you can avoid downtime and keep business data more secure – and avoid a data disaster.

Hughes SaaS Protection is a cloud-to-cloud backup solution that is used to protect thousands of businesses every day. It offers comprehensive backup and recovery for critical cloud data that lives in Microsoft 365 and Google Workspace applications. This includes OneDrive, SharePoint, Teams, Gmail, Google Drive, and more.

Flexible restore options allow you to recover lost data quickly, while retaining file and folder structures in Microsoft 365 and Google Workspace (formerly G Suite).

With automated, continuous backups, you can protect Microsoft 365 and Google Workspace applications against accidental or malicious deletion, ransomware attacks, and other cloud data loss with automatic backups performed three times daily.

FIREWALL MANAGEMENT

As part of the service design Hughes will work closely with you to configure an environment based on the zero-trust model to ensure that your firewalls provide the highest security whilst allowing for optimal network connectivity to achieve your business goals. If your network carries card payment data, rest assured that Hughes by default designs PCI DSS compliance as an integral part of the network security concept.

The managed firewall service focuses on three core components of the overall security implementation: segmentation, configuration and patch management.

In order to ensure security hygiene, the implementation is conducted according to a hierarchical access and configuration methodology, which limits access by authenticating and authorising at the required level. All access and configuration changes are tracked and logged, providing detailed historical accounting for troubleshooting purposes, forensics, auditing and compliance.

Segmentation is key to robust firewall management. It limits the damage that could be caused by viruses and malware, preventing the failure from spreading to other parts of the network. Also, if a segment is compromised it is easier and faster to discover and respond to a threat that is already isolated by the nature of the design.

The second essential component of firewall management is the configuration of secure connectivity from the branch site to central resources or other branch locations by tunnelling the traffic and securing the data transmission using encryption.

The third component is the implementation of platform patches in a timely manner as soon as they are released by the OEM. Patches or updates could be security updates, bug fixes, software improvements, or critical vulnerability mitigation.

We also track all applicable licences and renew on time so that services such as updates and unified threat prevention (UTP) services are not discontinued.

A NAME YOU CAN TRUST

Our flexible networking solutions combined with our multi-vendor approach means we take modern technology capabilities and identify the right solution to meet our customers' commercial needs. Our long-standing relationships with our customers, which span many years, are testament to our collaborative and quality-focused approach. We deliver our services throughout Europe with offices in the UK, Germany and Italy and offer a single point of contact with a single, aggregated service level agreement for all sites irrespective of size or location. As the European business unit for Hughes, we work in collaboration with our sister business units in North America, South America, India and International to deliver fully integrated solutions on a global scale.

For further details about our products and services contact us today.

HUGHES WORLDWIDE CAPABILITIES

$1.85 BILLION Dollars in revenue

Supporting **425,000** business and government sites worldwide

2,100 employees globally

7+ million terminals of all types delivered in **more than 100 countries**

Deployed **35,000** SD-WAN sites to date

Customers on **6 continents**

5 decades of networking expertise

WANT TO KNOW MORE? GET IN TOUCH

TELEPHONE
UK: +44 (0) 1908 425 300

HughesON™