Meet the challenge of compliance with managed network mapping

The snowballing demands of regulation have created a growing need for data privacy and compliance auditing. But mapping and archiving your entire history of network activity and system logs can be a costly and time-consuming burden. We can help remove that burden by managing your security, archiving and compliance requirements for you. We'll fully map your entire downtime and compliance history and make it available for audit reporting on demand.

Demand for data privacy and protection audits is skyrocketing, fuelled by government and industry mandates and regulations that range from Sarbanes Oxley, California SB1386 and the PCI Standard for merchants and banks, to NERC CIP for utilities.

Organisations both large and small face the unprecedented burden of storing all IT system logs: real-time and historical evidence of access; activity and configuration changes for applications, servers and network devices.

Security log retention enables your organisation to meet compliance guidelines while we take over the time-consuming process of mapping network activity to audit reporting. This means you get streamlined and centralised audit reporting of security incidents. We deliver global compliance reporting and access to all current enterprise log data – and you get forensics capability through archived security incidents and archived log data.

Protecting your business

Our log management services combine data collection, analysis and problem solving to meet your threat detection and compliance needs. Our data storage solution will help protect your intellectual property, financial data and business plans.

We'll collect every one of your organisation's logs from all connected data sources, including networking, servers and applications. You can access and audit vital data immediately by preserving all logs in unaltered form, providing a variety of reporting templates and presenting valid statistical comparisons across all platforms and applications.

The benefits of a managed approach

Security

- identify and respond swiftly to potential problems
- fast monitoring and incident response provide immediate alerts
- login monitoring for unauthorised access identification
- incident logs enable easy pattern identification and trend analysis.

Compliance

- satisfy explicit data retention requirements
- data archived and indexed for long term analysis
- high volumes of raw log content summarised for reports and forecasting based on statistical trends
- easy access to data for immediate and detailed response to customer or regulatory inquiries.

Financial

- gain advantages without infrastructure or resource investments
- identify and assess risks for enhanced business planning
- reduced cost of retaining in-house security expertise
- keep existing infrastructure and reduce network downtime and vulnerability
- access a variety of reporting options without a time and resource consuming development cycle.

The quick and easy way to a healthy network

As soon as your data sources have been integrated, we can begin monitoring your network 24/7. We'll alert you immediately to any anomalous behaviour and when an incident occurs, you'll have ongoing assistance until the issue has been resolved.

You can see your network status at any time via a web portal and system logs are available online for six months before being securely archived. You can depend on timely assistance from our SOC analysts around the clock.

We can monitor devices across your networks, from intrusion detection systems, intrusion prevention systems, firewalls and routers, to servers, applications, mainframes and PCs. We combine this monitoring with a database of identified threat situations and a worldwide team of experts to help us protect your infrastructure. We also offer you the option of outsourcing all aspects of the management to us – simplifying the process.

The solution ensures we detect internal and external attacks on your network as they happen and halt these attacks before damage is done. This eliminates the expensive and time- consuming clean-up costs required following network attacks.

Achieve optimal results

When you combine our security log management service with our leading security threat monitoring you also get:

Comprehensive correlation engine

- our proprietary correlation engine, Socrates, matches your unique network information with threats, attack signatures, patterns and known vulnerabilities
- eliminates false readings and identifies real threats faster than any comparable service
- Responds to threats with immediate and precise recommendations.

24/7 compliance monitoring

- 24/7 incident response
- integrity and presentation of data is legally admissible
- user access to programs and data constantly monitored and reviewed
- all logs are collected to BT secure facilities
- a subset of critical devices are monitored.

> "Security and compliance requires specialized expertise, and it makes more sense to outsource that so my staff can stay focused on the core business objectives... BT can survey all the potential threats worldwide. They can provide a much wider, more current view of the threats. That's something we can't do as efficiently, given our current staff levels."
> **John Lambeth, CISSP,CISA VP Information Technology Blackboard, Inc**

Why choose BT?

Key role of human intelligence

Our philosophy is underpinned by a belief in the importance of human intelligence. No matter how advanced a technology, there will always be an attack that will get around it. This is where people enter the equation. No-one has more experienced and qualified security analysts who are able to recognise the bigger picture in the data than BT.

Security Operations Centres (SOCs)

We have a network of 12 SOCs at different locations around the world, where customer devices are managed and monitored, and where our security analysts are on hand to provide real time support and response services to protect your networks.

Breadth and depth of experience

Trust is one of the core values that drives our own business culture, and we believe it is fundamental to the choice of security partner for any organisation. We are one of the world's leading and most trusted security brands, derived from a set of credentials that have been earned over decades of experience in the field:

- we are one of the largest security and business continuity practices in the world, with over 2,500 security professionals globally
- our secure networking experience includes monitoring more than 30,000 customer devices from our SOCs around the world
- we have global analyst recognition for our achievement in delivering outstanding managed security services globally to customers.

What could Security Log Retention do for you?

Visit bt.com/globalservices

Offices worldwide.

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

Issued: July 2018