Essential Guidance

Security is a continually evolving set of processes and technologies. The challenge is to keep your security operations up to date with changes in the threat landscape as well as the demands from business to support digital transformation programmes and compliance obligations. The demands on security operations are unlikely to ease any time soon. More will be expected of you, but budget and resource increases are unlikely to rise in line.

As you seek to continually improve your security operations there are a number of important considerations to keep in mind:

- Security is now a strategic priority for businesses. It therefore must be aligned to business strategy, and the executive must be adequately and appropriately informed of risks as they emerge and change. Security should be positioned as a business enabler, so work hard at communicating the risks and benefits in terms members will understand.
- An ad hoc and fragmented approach to security technology acquisition is not appropriate for the demands of a modern security operations team. Solutions exist today that enable an integrated and ballistic security architecture that provides both the visibility across the entire estate and the control and management tools to assess security posture. Automation follows integration, and this is essential if security operations are to deliver better efficiency and effectiveness within the prevailing resource constraints.
- Innovation in the security world has for too long largely been in the domain of the attacker. This balance is now being restored, and a plethora of new technologies have emerged over the past five years that offer capabilities that drive security to new heights. Many of these new technologies can be deployed in the cloud, and even more through managed security services, helping organisations to maintain a security operation that is state of the art.

INDUSTRY-LEADING PROTECTION AGAINST NEW AND DYNAMIC THREATS

A Security Incident and Event Management System (SIEM) can help you understand what is happening real time on your networks, detect and highlight malicious activity, threats and attempted hacks before they become an issue. A SIEM, configured and integrated with your network and IT infrastructure, can be used not just to improve situational awareness, but also as a platform to orchestrate and automate responses and to stop attacks well before they become serious breaches.

BT and McAfee have joined forces to gather, analyse and share the latest intelligence, so that protective controls can be updated in real-time. This allows organisations to close the gap between detection and protection. Our partnership means you get access to the latest technology and security intelligence at competitive prices. Together we offer intelligent SOC and SIEM capabilities as a managed service across Europe, able to support customers worldwide. Our joint solutions contain McAfee's dynamic endpoint, Data Loss Prevention, SIEM and associated technologies.

We offer the combined benefits of McAfee's visibility and management of endpoints, currently protecting over 188 million endpoints, alongside BT's heritage in customers' managed security operations and unique carrier-level insight. With BT's 2500+ security specialists on hand, you benefit from expertise in the latest technologies and 24x7x365 cover.

From our 14 global Security Operations Centres we provide a centralised monitoring of your SIEM, giving you the information you need to respond proactively and our highly scalable service can meet the needs of all sizes of organisation – from those organisations with a few sites and hundreds of devices though to global organisations with many thousands of devices that need monitoring.

Get in touch with a BT/McAfee Expert

Book a showcase visit

Download the datasheet