



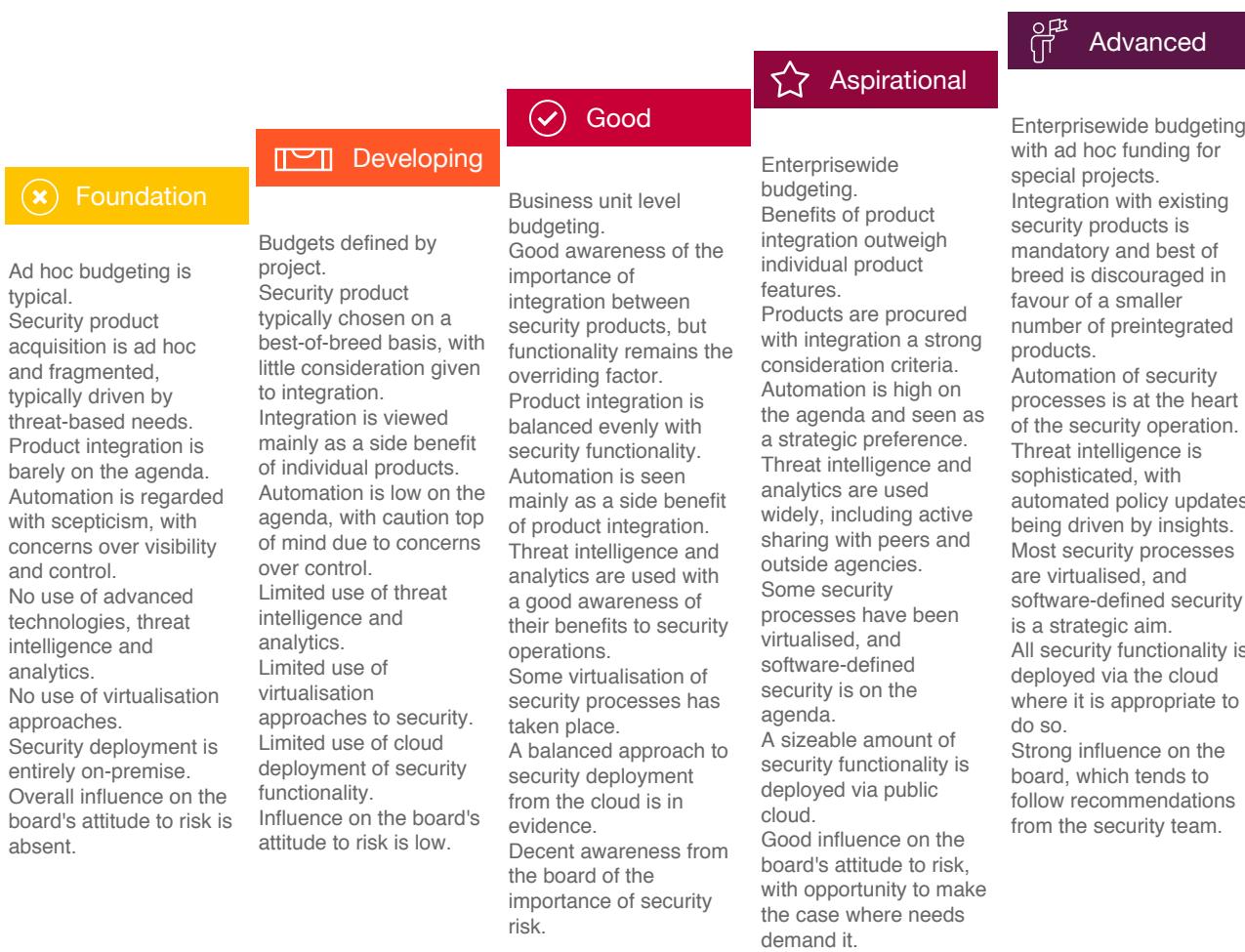
## MANAGING SECURITY OPERATIONS: TOWARDS INTEGRATION AND AUTOMATION

Sponsored by BT and McAfee

### Executive Summary

Thank you for completing the IDC Security Assessment, sponsored by BT and McAfee. This assessment has been developed to provide companies with comparative information regarding the operational maturity of their security functions, backed up by independent research developed and carried out by IDC. The survey collected responses from security influencers or budget holders across 450 organisations globally to understand the differences between companies when it comes to security technologies, integration and manageability, and steps towards automation.

IDC scored individual responses and created a comparison framework, built on grouping organisations into five different levels of operational readiness based on their approach to security strategy as well as management and process automation, as seen in Figure 1. Organisations don't have to be at the top of the scale to start seeing benefits. Any improvement can bring about tangible benefits to IT and the business by increasing agility, resilience and innovation through better confidence to adjust strategy to meet changing market conditions.



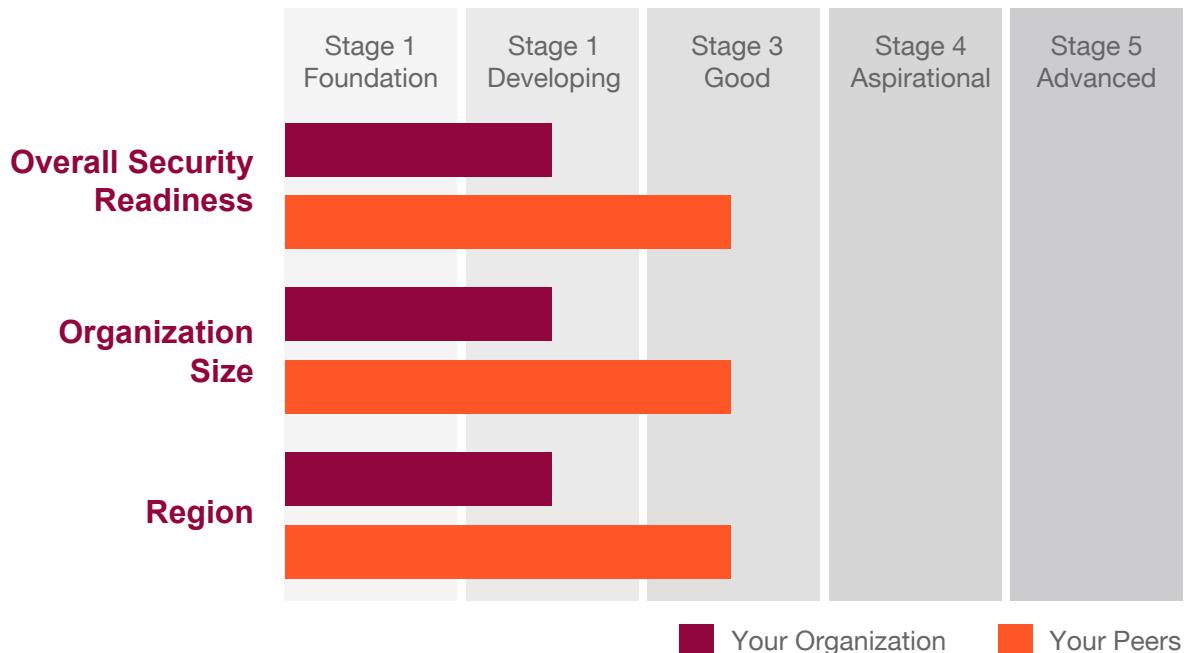
# IDC Security Operational Readiness Assessment



## Overall Results

Based on your responses, you are placed within **30%** of companies overall in the readiness group of **Stage 3: Good**, which is the **3rd** level out of five.

Figure 2: IDC Security Operational Readiness Assessment Results



## Overall summary

Compared to the best in class capabilities, your organization is:

- **2 levels behind the global leaders**
- **1 level behind the leaders in companies of size 500-999**

## Your performance in more detail

This assessment tool was designed to help establish your organisation's IT security operational readiness to cope with the evolving threat landscape that impacts digital businesses, both today and in the future.

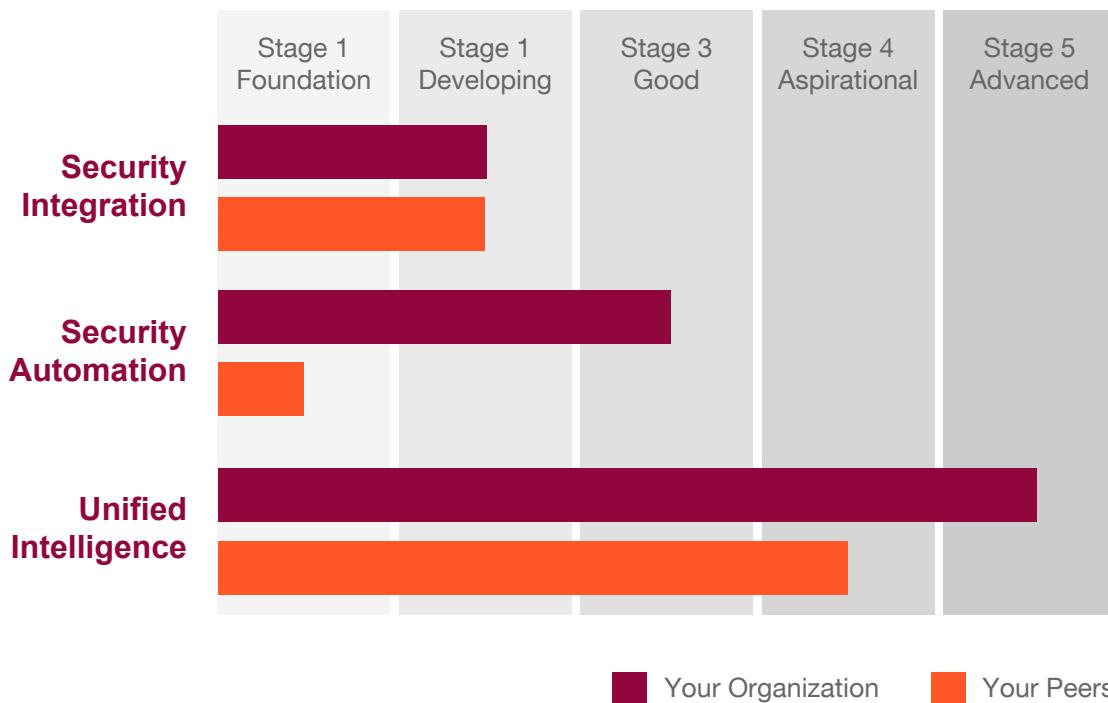
- **Security Strategy**
- **Integration and automation**
- **Use of advanced security capabilities**

Your performance in each area is compared to your peers in Figure 3 on the following page.



## IDC Security Operational Maturity by capability

Figure 3: Section Readiness



## How to get ahead

Regardless of your level, there are certain areas that are continuing to evolve and are worth focusing on above all else:

- **Integration** – focusing on security product integration, for enhanced visibility across the security estate
- **Automation** – exchanging threat information between products and updating policy decisions with minimal human supervision
- **Advanced technology** — utilising the latest technologies to improve detection and remediation
- **Advanced deployment approaches** — prioritising cloud deployments and thus benefitting from specialist security resource at scale, regular maintenance and state-of-the-art updates, with minimal downtime



## Improvements to Security Strategy

### Developing

The security you deliver to the business may be perfectly functional, but it is unlikely to be in line with business objectives. For some reason, security operations are unable to influence business decisions, which means that budgets tend to be allocated on an ad hoc, or at least localised, basis with little strategic enterprisewide planning. Aligning security provision with your businesses digital transformation programmes is fundamental, and this places new demands on both the security technology deployed and the efficiency and effectiveness of operations.

## Improvements to Integration and Automation

### Good

You have intuitively followed a path of security product integration and are realising the benefits of this through automation. However, this is unlikely to be consistent across your entire security estate. The adoption of a holistic, open and strategic integration platform will yield benefits not just for your existing portfolio but for future product acquisitions. Furthermore, you will get even greater gains by automating policy updates and remediation across your entire estate, rather than being restricted to preintegrated products from a single vendor.

## Improvements to Security Capabilities

### Good

You are making effective use of global threat intelligence services, and likely doing it in collaboration with peers and outside agencies. If you are not using threat intelligence to drive automated policy updates then this should be on your to-do list. You should also investigate security analytics if you are not already doing so, but make sure you have a process of continuous improvement through quantitative feedback. Managed services may also be appropriate, as they can provide greater context, as well as benefiting from the insight from multiple organisations.

You seem to have a strong set of advanced security technologies at your disposal. You are more likely to be using machine learning today, and looking seriously at cognitive computing for deployment within two years. Beyond this, you should begin looking at the benefits of blockchain and distributed ledger technology, which has a variety of security use cases, plus containerisation and other micro-segmentation approaches that can help to limit the damage suffered from attacks.



## Essential Guidance

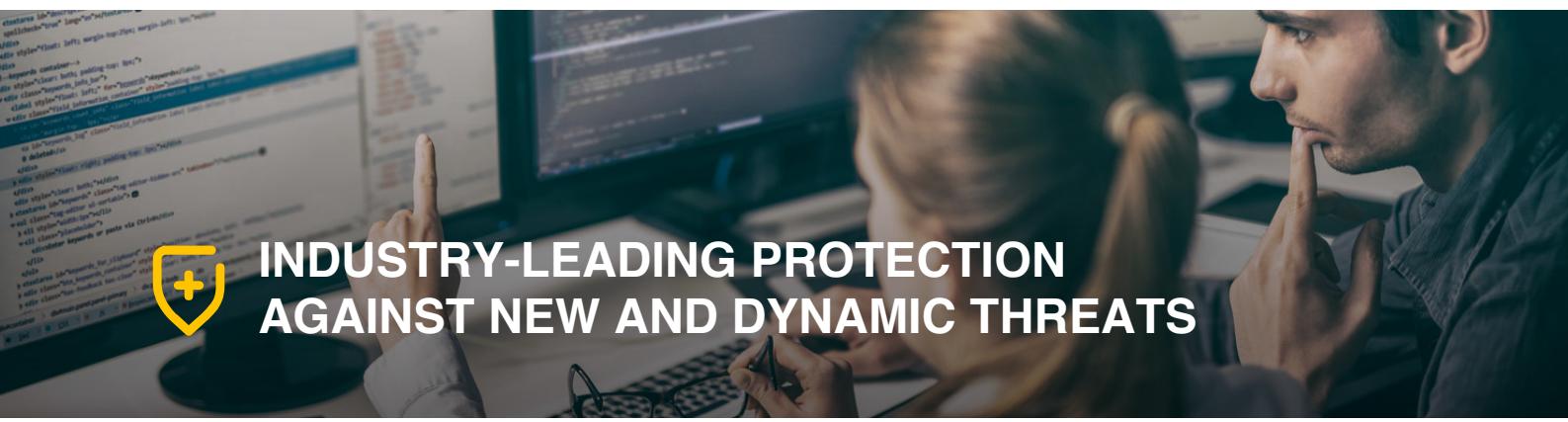
Security is a continually evolving set of processes and technologies. The challenge is to keep your security operations up to date with changes in the threat landscape as well as the demands from business to support digital transformation programmes and compliance obligations. The demands on security 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.



Download the datasheet

