Close the security gap with a unified approach

Detect, block and remediate risks faster with end-to-end visibility of the security cycle
Events are not correlated. Tools are not integrated. Teams are not connected. Knowledge is not shared. The IT security gap is getting bigger. And more and more organisations – and sensitive data - are falling through the cracks. Nine out of ten large organisations experienced a security breach last year.1

From denial of service attacks and virus infections to device theft and fraud, the origins of these breaches are steadily increasing. And so too is the financial fallout. It’s estimated that the global losses from cyber crime have now topped $300 billion per year.2

‘Are you secure?’ has truly become a billion-dollar question - a question that very few organisations can answer with a categorical yes.

Welcome to the new normal

With a relentless stream of new threats emerging – mobile malware alone grew by 614 per cent in the space of a single year – an organisation’s security position is in a constant state of flux. A website that was secure on the Sunday might be compromised on the Monday – as demonstrated by the first Heartbleed incidents in April 2014.

It’s not just security threats that are evolving; cloud, virtualisation, software-defined and mobility initiatives mean that organisations’ infrastructures are continually shifting too, creating new chinks in the IT security armour.

With hackers and malware architects now using automated toolkits and taking a ‘profit-driven’ approach to their activities, these chinks will be discovered – and rapidly exploited. In 2012, the median number of security breaches suffered by a large organisation was 71; in 2013 it was 113.3

With threats increasing in volume, variety and velocity on a daily basis, organisations don’t just risk falling through a security gap, they risk falling into a security black hole.

Making the right investments

Simply throwing more money at the problem is not the answer. It might buy more peace of mind, but it won’t necessarily buy more protection.

Security budgets went up by around 51 per cent in 2013 compared with the previous year.4 Yet security incidents still increased by 25 per cent5 – and this only accounts for those incidents that were actually detected. Many more happen in the IT shadows.

With 49 per cent of organisations planning to increase their security spend in the next 12 months, IT departments need to ensure they are investing in the right mix of solutions, skills and strategies to bolster their defences.

Faced with a myriad of options from a myriad of vendors, many IT professionals struggle to decide which security solutions need to be retired, refreshed or retained.

“The sheer number of threat actors and different levels of capability mean that large organisations potentially have too much to track and assess. Without the help of others - in terms of threat intelligence and assessment, as well as supply chain security – cyber defence becomes difficult,” observes Gartner.6

Redefining the perimeter

Many organisations have under-estimated just how much the security landscape has changed. Despite the rising tide of threats and breaches, 74 per cent of organisations believe their security activities are effective.4

But security strategies can only be effective if organisations understand the full breadth and depth of the challenge. To gain this understanding, they must first close the gap in knowledge, tools and teams.

Security can no longer be viewed in relation solely to a network port or a server. It must be viewed in relation to the business. As Gartner states: “Security and risk are fundamentally intertwined with everything an organisation does, forming a matrix of interconnected risks and rewards.”5

Every application, every device, every web-based service is now a potential entry point – and therefore a potential risk. The traditional perimeter no longer exists.

This is the new normal – and it demands a radically different approach to security. As Gartner confirms: “Traditional defences, such as signature-based anti-malware tools and stateful inspection firewall technology, are less and less effective against new threats.”6

Organisations don’t just need new tools and technologies to survive the new normal, they also need to tighten up their security processes and sharpen up their strategies. And do it on a continual basis.

As Gartner advises, “Security practitioners must shape and reshape security architecture and programmes to keep a balance between business enablement and risk management in 2014 and beyond.”7
Finding the gaps

To ensure improvement efforts are focused on the right areas, organisations must first understand where they are and where they want to be with their security position. They need to assess. They need to audit. And they need to act.

With security no longer constrained by any perimeter, these activities must encompass a wide range of risks across a wide range of end points. Given such complexity, it’s not surprising that a quarter of organisations have never carried out any form of security risk assessment.

Working with an external partner will not only simplify but also accelerate the assessment process - and the closing of any gaps. Security assessments should span each stage of the attack cycle - before, during and after – and pinpoint areas for improvement.

Detecting and defending are often the main focus of an organisation’s security strategy and any assessments. Yet to improve both these capabilities, IT departments must also assess what they do after an attack and how they adapt their processes.

As Gartner states: “Security processes, unlike appliances, software and services, cannot be acquired in exchange for cash. They can only be established by an organisation and then mature to an appropriate level.”

Gaining the visibility advantage

An integrated approach is key to reaching a higher level of maturity – and achieving better outcomes. By unifying people, process and tools at every stage of the security cycle, organisations will be able to identify, block and remediate a threat as it travels from the client device to the network to the datacenter.

For example, there’s no point in the end user services team detecting an abnormal log in on a smartphone before an attack, if this information is not available to the security operations team during a subsequent virus outbreak.

Greater automation across the security cycle will not only simplify the sharing of such event information, but also accelerate the response. When an attack strikes the importance of ‘relevant’ pre-attack insight cannot be underestimated. Locating that ‘insight’ in a timely, digestible manner, however, remains a challenge.

Automating the correlation of events across the IT infrastructure is fundamental to providing organisations with a single view of the attack status and its potential source.
Adapt to the new normal: 10 steps for strengthening security

1. Unify management across wired and wireless environments with consolidated security tools and technologies.

2. Regularly conduct security assessments to identify gaps in tools, policies and defences.

3. Correlate information about security events across datacenter, workplace and networking devices.

4. Review and reinforce basic controls such as patch management and anti-malware measures.

5. Undertake a profiling exercise that maps access rights and security controls to different workstyles.

6. Maintain a threat assessment framework to identify the origins of different risks and to prioritise how to respond.

7. Enhance staff education programmes and publish regular updates on risks and regulations.

8. Monitor internal usage of applications and databases and establish context-aware capabilities.

9. Implement policies for data usage in the cloud and on employee-owned mobile devices.

10. Increase the level of forensic visibility – you can’t respond to things that you can’t see.

Computacenter’s security credentials:

- Our skills and solutions span the entire IT stack – from the workplace to the network and the datacenter.
- We have developed a range of assessments that help organisations define and deliver a multi-layered information security framework.
- We manage thousands of devices and events every month for our customers, which gives us a unique insight into emerging and evolving security risks.
- Computacenter has been working with Cisco for more than three decades and has been a Gold Partner since 1998.
- We hold Cisco Advanced Technology Provider specialisations in eight disciplines, including Telepresence, Security, Networking and Unified Communications and Collaboration.
- We don’t ‘add’ or ‘do’ security: it’s automatically part of every solution that we deliver.
Computacenter is Europe’s leading independent provider of IT infrastructure services, enabling users and their business. We advise customers on their IT strategy, implement the most appropriate technology from a wide range of leading vendors and manage their technology infrastructures on their behalf. At every stage we make our customers’ businesses sharper by removing cost, complexity and barriers to change across their IT infrastructures.

Computacenter operates in the UK, Germany, France and the Benelux countries, as well as providing transnational services across the globe.