Managed Security Services

While the security landscape is becoming more complex and threats more pervasive, a sophisticated ability to not only counteract but also pre-empt attacks, is available.
How exposed are you to attacks?

Security has become a much deeper executive discussion because of the modern diversity of channels through which businesses can be attacked. Mobility, bring your own device, virtualisation, the cloud, and social media have all opened new doors into the organisation. At the same time, most businesses need to manage a range of technologies provided by a variety of vendors, all of whose security approaches, as built into their technologies, are different. And, of course, the regulatory environment calls for an increasing number of types and levels of proven compliance.

Adding pressure to organisations is the fact that technologies, business models, regulatory environments, and the threat landscape are evolving continuously.

So, security has become a broad discipline that affects the entire organisation and calls for a range of highly specialised and dynamic skills and technologies that most businesses don’t currently have. The boardroom question is: how cost-effectively can these be acquired or accessed?

Dimension Data has learned that the answer lies in understanding how profoundly security has changed in recent years. Most organisations have firewalls, antivirus, and network intrusion prevention systems in place. Research shows, though, that they simply don’t have the manpower or technology to maintain them efficiently. Systems are not patched regularly. As a consequence, organisations don’t know whether or not they’ve been attacked and aren’t taking proactive steps.

Much more importantly, these very limited systems cannot predict attacks. Recent highly publicised security breaches at multinationals have proved just how disastrous reputational damage can be. They’ve also demonstrated how critical it is to be able to correlate threats pre-emptively and respond to them immediately.

However, achieving this necessitates a fundamental change in security focus as well as significant investment. You need industrial-strength levels of documentation, processes, and procedures. You need enough highly qualified engineers and security specialists to man your security systems 24/7, analyse the information from them continuously, and be able to respond immediately. You need to continuously update your technology – and the cumulative experience, insight, and knowledge of thousands of independent security experts globally working towards the same goal of pre-empting attacks.

The best way to achieve this successfully and affordably is through managed security services.

It’s critical to be able to correlate threats pre-emptively and respond to them immediately.
You need to continuously **update** your technology – and the cumulative **experience**, **insight**, and **knowledge** of thousands of independent **security experts** globally working towards the same goal of **pre-empting** attacks.
Our subject matter experts use information from the incident response team to find the most expedient means of containing and mitigating a threat. They also implement countermeasures to attacks.

Value now and in the future
Organisations are often required to do more with less and often it’s difficult to justify the cost of a managed security service because its value is based on future performance.

What are the alternatives?
A security monitoring service, on its own, is inexpensive. It monitors and analyses network environments in real time, providing information, context, external audit, and operational guidance for onsite security management. It’s no substitute for local management and control, however.

Packaged software monitoring options are also inexpensive, but usually simply compare one security device log to another. They can’t evaluate network security in the context of the global threat environment, the vulnerabilities apparent from an external scan, or even the network’s own history. And no software can provide the staff development programmes and opportunities, global operations, and advanced analytical tools of a properly managed security monitoring service provider.

The security monitoring that comes packaged with other IT outsourcing services offers the convenience of a single provider for a range of services, but it fails to separate responsibilities for maintaining and evaluating security. It can also subordinate security monitoring functions to larger, generic operational activities thereby diluting the security specific value.

By contrast, independent, full-service security monitoring specialists can lower your costs by reducing your risk on the basis of:
• the range, depth, sophistication, and scalability of their technologies
• the quality of the human intelligence networks they maintain and deploy
• the metrics and certifications they use to measure and audit their performance in predicting and immediately responding to your threats

A holistic approach focused on business value
Dimension Data’s Managed Security Services are designed to manage and operate your infrastructure in a way that ensures that all your policy, compliance, performance, availability, and capacity needs are met. We cover people, processes, technology, and threat insight and support outsourced, cloud-based, and hybrid security infrastructures across multiple vendors and technologies.

Our holistic approach to security is also flexible. We help you determine which aspects of your security estate are best managed in-house with internal resources and monitoring tools, and which are best outsourced to us.

We not only give you access to the world’s most sophisticated security management platform and most advanced threat correlation technology, we also have the resources to allocate dedicated level 3 engineers to your particular organisation.

Our incident response team, which monitors your environment and analyses threats, has more than 10 years’ experience and in-depth knowledge of the motives and methods of attackers.

Our subject matter experts use information from the incident response team to find the most expedient means of containing and mitigating a threat. They also implement countermeasures to attacks.

Our forensics team, which has 16 years of industry experience, understands how to express a chain of evidence and collection of data as legal evidence. It performs root cause analysis and business impact assessments should an attack result in any loss or damage prior to being contained.

Our client security portal presents service-specific data, such as virtual machine scan results, current open incidents, user access failures to a specific asset, performance monitoring data for specific assets, etc. We also combine vulnerability, severity, and asset criticality information to quickly identify, rank, and address violations and vulnerabilities on networked systems and devices.

A choice of two portfolios

Managed Services for Security
These include:
Managed Firewall: protects your key information assets across networks, hosts, applications, and databases
Managed Intrusion Detection and Prevention: provides a fully managed, 24/7 service that uses network-based intrusion detection and prevention systems to protect networks from attack and misuse
Managed Email Gateway: ensures that your email gateway technologies are monitored and managed effectively, to provide continued protection from information leakage and from viruses, trojans, spyware, and malicious code distributed via email
Managed Web Gateway: ensures that your Web gateway technologies are monitored and managed effectively, to provide continued protection from information leakage and from viruses, trojans, spyware and malicious code distributed via the Web
Managed Web Application Firewall (WAF): protects your key information assets across Web-based applications
Your organisation can **embrace** cloud and social media technologies to **deliver** and **exchange** information while **protecting** it from accidental data loss, malicious attacks, and emerging threats.

**All our Managed Services for Security include:**

- 24/7 technical phone support
- around-the-clock security monitoring and maintenance
- access to the client security portal
- comprehensive reporting

**Cloud Services for Security**

These include:

**Email Security-as-a-Service:** ensures a consistent, ‘always on’ email experience for your users while guarding against email threats – including viruses, phishing, spam, spyware, data theft, and blended threats

**Real-time Threat Management-as-a-Service:** enables effective, real-time monitoring, detection, analysis, and response for the security data your network produces

**Why Dimension Data?**

- broad expertise across a variety of technology focus areas
- strategic partnerships with leading security technology vendors
- as part of NTT Group, Dimension Data was recognised as a Challenger in Gartner’s 2014 Magic Quadrant for Global MSSPs
- our founding and membership of the Threat Intelligence Alliance gives us access to 122 intelligence feeds and, therefore, a unique threat correlation ability
- our participation in the compilation of the NTT Global Threat Intelligence Report, alongside Solutionary, NTT Com Security, and the NTT Innovation Institute, Inc. (i3), enables us to use combined client data, security research, and real-world experience to protect your organisation
- real-time threat management platform: an enterprise-wide risk management solution enabling our security operations centre (SOC) analysts to centrally manage attacks, threats, and exposures
- global footprint, local delivery: with over 25,000 employees and operations in 58 countries, across five continents
- proven track record: over 6,000 security clients across all industry sectors

---

**About the Magic Quadrant**

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

---

1 Gartner, Magic Quadrant for Managed Security Services, Worldwide, Kelly M. Kavanagh, 30 December 2014