ideal
Defining customer experience

CISCO

MANAGED SIEM

Enterprise-grade peace of mind

Navigating the security landscape

> Personal data and intellectual property are at the heart of digital businesses, and the penalties for failing to secure them are legal, reputational and financial.

Security doesn't stand still. As technology becomes more pervasive - and more fundamental to doing business - there's an ever growing number of people interested in your organisation for quite the wrong reasons. Their tools, and the techniques they use have come a long way: hackers are organised and motivated by financial gain or political ideals, malware is distributed and developed in communities and by organised criminals, and exploits are targeted and carefully researched.

The landscape continues to change, and attacks on the enterprise are more serious and sophisticated than before. In its Mid-year Cyber Security Report for 2017, Cisco explains that while revenue generation is still the primary objective of most attackers, some have the ability and inclination to lock systems and simply destroy data as they go. Cisco predicts that this may be a precursor to a new type of 'destruction of service' attack, where adversaries seek to eliminate the safety net on which organisations rely to restore their systems and data following cyber incidents.

Against this, personal data and intellectual property are at the heart of digital businesses, and the penalties for failing to secure them are legal, reputational and financial. In the first half of 2017 alone, the UK saw two breaches in which 200,000 or more customer records were stolen, and the Information Commissioner's Office (ICO) issued four fines of £100,000 or more to companies failing to protect data sufficiently. The WannaCry and Petya ransomware attacks affected more than 100,000 organisations across 150 countries, between them causing chaos in the NHS, temporarily shutting down major manufacturing facilities, and disrupting the world's biggest shipping company for five days.

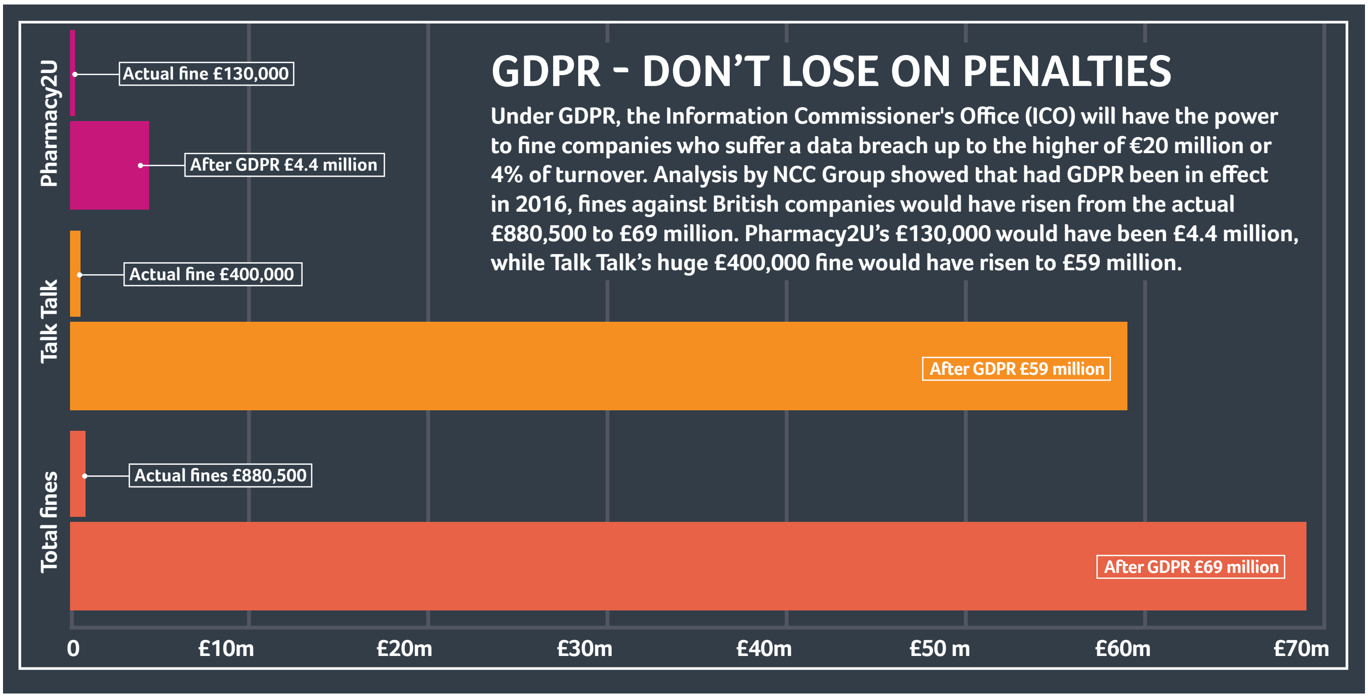
Your challenge

The security and integrity of your data is paramount to protecting your brand and customers, and achieving business goals. With multiple IT systems generating multiple independent and interrelated security alerts, the best practice approach to managing and protecting against cyber threat is to maintain a 24/7 in-house security operations centre (SOC), but there are considerable challenges:

- **Skills availability** - cyber security expertise is in great demand, and recruiting and retaining high-calibre staff is expensive and time-consuming
- **Management expertise** - the organisation needs management skilled in understanding, prioritising and acting on security issues
- **Cost** - establishing and maintaining a 24/7 SOC requires considerable investment in staff, training, threat intelligence awareness, equipment and facilities

> Lack of visibility into dynamic IT environments, the risks presented by "shadow IT", the constant barrage of security alerts, and the complexity of the IT security environment are just some reasons resource-strapped security teams struggle to stay on top of today's evasive and increasingly potent cyber threats.
>
> **Cisco Mid-year Cyber Security Report,** 2017

The very largest businesses may be able to afford the necessary investment - increasingly they can't afford not to - but where does that leave medium-sized organisations? You're handling the same kind of data, are held to the same standards and are big enough to attract the wrong kind of attention, but the numbers for an in-house SOC are prohibitive. The risk is that you are left exposed - and with the EU General Data Protection Regulation (GDPR) on the horizon, the penalties are about to get even more severe.



GDPR - DON'T LOSE ON PENALTIES

Under GDPR, the Information Commissioner's Office (ICO) will have the power to fine companies who suffer a data breach up to the higher of €20 million or 4% of turnover. Analysis by NCC Group showed that had GDPR been in effect in 2016, fines against British companies would have risen from the actual £880,500 to £69 million. Pharmacy2U's £130,000 would have been £4.4 million, while Talk Talk's huge £400,000 fine would have risen to £59 million.

Managed SIEM

Enterprise-grade peace of mind

To meet these challenges Ideal has launched a managed SIEM (security information and event management) service, providing always-on, proactive and expert monitoring and maintenance of security across the organisation. Operated from Ideal's UK-based 24/7 SOC, Ideal's managed SIEM service integrates with your entire IT environment, enabling Ideal to analyse multiple data sources on your behalf, correlating observed activity into business and security events.

Ideal's managed SIEM service covers firewalls, networks and network devices, servers and applications. It starts with us installing an AlienVault USM Appliance into your virtualised or physical compute environment. We build integrations with databases, logs, remote logs, WMI and network devices, to deliver asset discovery, threat intelligence, behavioural monitoring, event and intelligence correlation, log collection and incident response.

> Hackers and scammers are more organised, cyber threats are more sophisticated, and the regulatory landscape is more robust. Securing the enterprise is more important than ever, but access to people, skills and resources is challenging. Our managed security service provides an affordable and effective solution.
>
> **Adrian Clarke**
> Senior cyber security consultant, Ideal

Ideal prides itself on its proactive approach to managed services. Our aim is to discover and diagnose security threats and incidents before you detect an issue. For each alert, Ideal will proactively filter and analyse the threat, and provide guidance and recommendations on the required remediating actions. Where the alert relates to equipment and services managed by us, we will carry out the required actions. In addition, Ideal's SOC analysts will produce reports to default compliance templates including PCI DSS, ISO 27001 and the National Cyber Security Centre's 20 Critical Security Controls.

WHO NEEDS MANAGED SIEM?

Lack of access to the latest threat intelligence

Increasing regulatory requirements

Increased risk from security threats such as ransomware or DDoS attacks

The need to review, analyse and correlate existing security data

The challenge of resourcing and operating your own 24/7 SOC

Lack of security analytical skills and supporting toolsets

What are the benefits?

Ideal's managed SIEM service provides peace of mind through active monitoring of your security environment. Our security centre is operated from our Brighton-based offices and manned by permanent, vendor-qualified staff with the expertise to manage and advise on security issues as they occur. Your data is not sent to the cloud.

Key benefits:

- All essential resources - security analysts, operational SIEM, global threat intelligence, established incident investigation process - provided 'as one' on a 24/7 basis
- Real-time identification of threats, and management of the necessary notifications or alert levels, minimising response time and reducing the impact of security events
- Continuous monitoring of security events on your infrastructure
- One-stop SOC remediation for any monitored infrastructure that is managed by Ideal
- Robust and reliable security incident response
- Security compliance, demonstrable to management, auditors and regulators
- Access to expertise and threat intelligence to properly categorise and advise on incidents
- Free up your IT staff to focus on your business initiatives and objectives
- Peace of mind for a predictable monthly cost

The Ideal solution

Ideal has been providing managed support and security services for more than seven years, and has built a reputation among customers for proactive support, effective incident management and excellent attention to detail. Our Brighton SOC is staffed 24/7 by a team of experienced, vendor-qualified engineers with networking, server and security certifications from vendors including Cisco, Palo Alto Networks, Red Hat, Microsoft and AlienVault.

Ideal's managed SIEM service leverages AlienVault's threat detection and incident response capabilities. The AlienVault Unified Security Management (USM) platform combines five key security principles:

- Behavioural monitoring
- Intrusion detection
- Asset discovery
- Vulnerability assessment
- SIEM

Also integrating data from the unique Open Threat Exchange (OTX) - the world's first truly open threat intelligence community - the platform helps Ideal provide the very best in threat detection and response with community powered, expert-verified threat intelligence.

What our managed services customers say:

"[Ideal has] been catering for our every network/security/voice need for many years without a hitch. The calibre of their staff is second to none - the support engineers are well trained and have extensive knowledge that your business can rely on. I would highly recommend Ideal."

Matthew Blewett, IT manager, EMEA & Group Infrastructure, Rouse

"We have a faster network, a strong robust system, greater resilience and decreased security risks."

Chris Fullalove, IT director, Caffyns Group

For more detail on the Ideal solution, including SLAs and the full scope of the service, please refer to our Managed SIEM service description.

Cisco and security

Ideal works only with organisations that display the highest standards of integrity. We're a Cisco partner, and for more than seven years we've been providing managed security services to customers operating on Cisco network architectures.

Cisco is committed to maintaining strong protections for its customers, products and company, striving to earn trust by always being trustworthy, transparent and accountable.

Specifically, Cisco:

- Takes active measures to safeguard the security and reliability of the network
- Is committed to securing and protecting its customers and their data
- Adheres to a secure development lifecycle (SDL) in the development of its products and services
- Provides equal and simultaneous access to security vulnerability information for all parties globally
- Makes timely and actionable breach notifications to impacted parties
- Publishes data regarding requests from law enforcement and national security agencies for customer data
- Drives and follows open, global standards

About Ideal

Founded with a focus on excellent customer experience, Ideal designs, provides and manages secure infrastructure for organisations who see IT as a core business enabler. Proudly based next to Brighton station, Ideal supports organisations operating across Britain and globally. From its in-house SOC it provides managed security services to high-profile customers, including Allport Cargo Services, Aspire Defence Services, Beggars Group, Caffyns, East Sussex Healthcare NHS Trust, OneFamily, and Rother District Council.

cisco