BYTES | Smarter together

Bytes Managed Security Services

Powered by SecurityHQ

Take swift action where it counts, protecting you business & your customers from genuine risks in the most effective way.

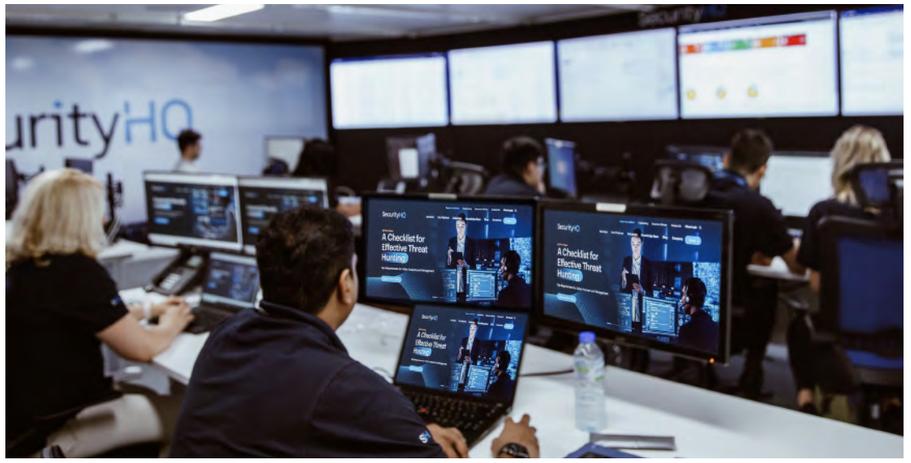
BYTES | Smarter together

Take the right actions in the event of security issues, fast, with support from Bytes and SecurityHQ

Contents:

About Bytes' Managed Security Services
Powered by SecurityHQ

The right combination of tools, skills, people and processes are essential to proactively and effectively manage, detect and defend your environment from all malicious activity, both external and internal.



Which is why Bytes & SecurityHQ understand security inside out. We have more than 20 years of experience working with leading enterprises and countless user environments, across all sectors.

Insight: We know where gaps exist and how to fix them. Our consultants have worked for or in key vendors, service providers, value added resellers, system integrators, major consulting houses and law enforcement – so we have it covered.

Action Based: We know that what you need is a solution to the problem. We don't just conduct audits, assurance testing and expert analysis. We provide practical and flexible real-world solutions, virtual services and support, to help keep you secure.

Lets work in stages, aligned to your business requirements.

Achieving your goals doesn't have to be cumbersome. The key is to adopt an approach based on business need and maturity. Taking the right step at the right time.

We can help you decide the best approach. Here are examples of four areas you may wish to prioritise, depending on your scenario.

People
- Help with identification of assets
- Take ownership for protection
- Follow and apply protection processes

Process
- Alignment of security with business process
- Automation and repeatability
- Threat and risk assessment
- Communication

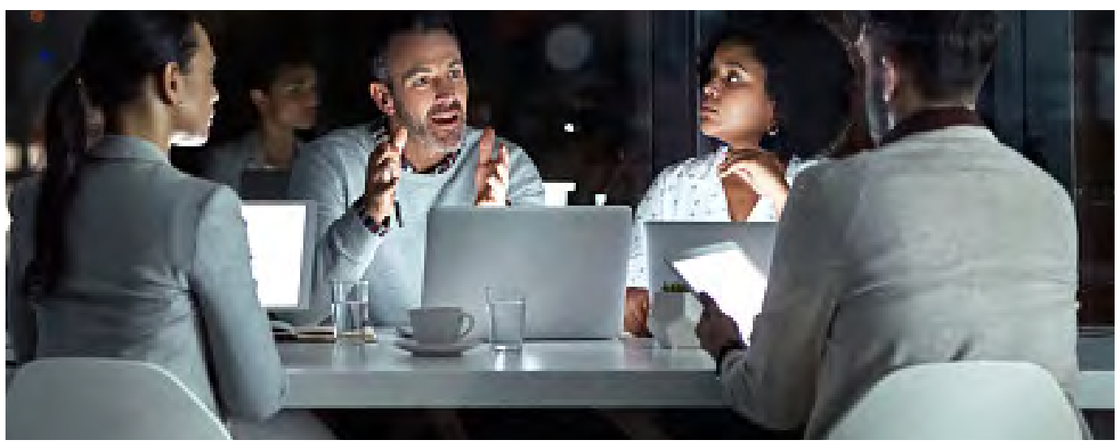
Information
- Identification of the 'crown jewels'
- Tiered security based on risk and value of the information
- Information classification, handling, labelling and watermarking

Technology
- Robust IT and technical security standards
- Basic security controls (hardening, patching, AV etc.)
- Advanced security controls including IAM, DRM, DLP, IPS, WAF, memory analysis etc.
- Monitoring & alerting

Back to Contents

Top 4 Customer Challenges

	The Problem	The Solution
1 **Incident Response Capability**	Security incidents do, and will, occur. Post detection, a rapid response is critical to contain and investigate rogue activity 24/7.	Bytes provides Incident Response playbooks, supported with our IBM Resilient SOAR platform & Certified Incident Handlers to contain threats.
2 **Defend Unlimited Threats with a Limited Budget**	Security Operations Centre detection tools, and the analysts used to drive them, are costly. Building a defensive SOC capability inhouse is beyond the budget of most organisations.	Our SOC services provide world-class tools and skills, at a fraction of the price it would cost to build a Security Operations Centre inhouse.
3 **Risk Reporting & Business Security Intelligence**	36% of breaches are the result of errors and/or misuse of systems. Risky assets, users and behaviour needs to be presented graphically and within a business context.	By visualising risky behaviour and misconfigurations, we target the threat at its source. Our customers receive detailed weekly reports with granular statistical analysis to illuminate risky behaviour, security posture issues and security incident metrics.
4 **Complex & Evasive Threat Detection**	Organisations struggle with the rapid identification of malicious behaviour. This identification requires a matured SIEM, with advanced correlation, anomaly and user behaviour analysis, together with continuous monitoring.	Bytes applies advanced correlation & machine learning to expose patterns of illicit behaviour. SOC immediately investigates the extent of an event, and its context, to derive a complete analysis with mitigation and risk quantification.



Key Differentiators

Extension of a Customers Team

Integrity & Transparency

Our code of ethics is fundamental, not only to our business success, but to the growth of all that we value. We place the power of our SOC team into the client's hands, providing complete visibility of their digital footprint, systems and processes, specific threats, and security posture.

Innovation

Cyber threats are increasing, both in terms of volume and sophistication. Which means that traditional approaches need to be re-evaluated. Bytes & SecurityHQ combine best-in-business technology, processes, and expert minds to provide advanced solutions to your security needs.

Incident Management Platform

Collaboration is critical for effective security operations. Our Incident Management & Analytics Platform provides a single pane of glass for incident workflows, SLA management, data visualisation and document repository.

Bespoke & Engineered

Every client is different. Your risks, industries, geolocations, regulatory requirements, and processes demand a bespoke response. We provide tailored services based on client's specific needs. Built from the foundation up, Bytes' team of expert engineers know exactly what is required for each and every event.

Company Credentials

Bytes' Credentials

Cyber Essentials Certified

QMS ISO 27001 : 2013 Registered — Certificate No:337802020

ISO 9001 Certified · ISO 14001 Certified

Trusted Partner

IASME Consortium — Gold Certified Company

SecurityHQs' Credentials

Crown Commercial Service Supplier

SecurityHQ Top Cyber Security Consulting/Services Companies in Middle East 2020

Information Security Management System — DNV·GL — ISO/IEC 27001 — UKAS Management Systems 0013

ISO 9001:2015 Registered Company

Cyber Essentials Certified

IBM Gold Business Partner

Beacon Award Winner 2021

Back to Contents

Managed Detection & Response (MDR) & Managed SOC

Powered by SecurityHQ

Powered by real-time log analytics, with security orchestration automation & response tooling, Bytes' MDR and Managed SOC service rapidly identifies & limits the impact of security threats.

Threat detection
24/7 monitoring & identification of threats, anomalies & policy violation with analyst driven investigations.

Incident management & analytics platform
for dashboarding, SLA management, ticketing & customer ITSM integration.

SIEM technology
analytics powered by IBM QRadar, the world's most powerful SIEM, with customer user access.

SLA management
15-minute response for critical incidents, with real-time SLA dashboards.

How it Works

Cybercrime is evolving, which means issues with solutions, including people, processes & technology, are prominent. Bytes provides round-the-clock monitoring to detect, investigate, notify & respond to incidents & potential threats.

Market leading technology. We use IBM QRadar to power our Threat Analytics & Correlation Engine. The scale & sophistication of QRadar is second to none.

24/7 threat monitoring. We support incident response using playbooks driven by advanced orchestration & automation systems (IBM Resilient). This process rapidly contextualises incidents with enriched data, orchestrates response workflows, & automates threat containment.

Benefits

- 24/7 detection of threats powered by real-time analytics & IBM QRadar.
- 24/7 incident response supported by GIAC certified incident handlers (GCIH).
- Advanced correlation & ML to detect complex threats.
- Incident containment & triage. Contain threats via incident playbooks & SOAR platform.
- Automate containment response to block threats.Cloud Native: Azure, AWS, Office365, Oracle Cloud & more.

Service Overview

01. Data Collection
- Syslog
- Cloud API
- Agentless Windows
- Apps & Database

02. Data Processing
- QRadar SIEM analyses & correlates data
- Identifies risky user behaviour (UBA)
- Contextualise Intelligence

03. Advanced Analytics
- User behaviour analytics
- Business service risk profiling
- Anomaly + behavior algorithms

04. Analyse Detect & Respond
- 280 + SOC analysts detect, investigate & respond to anomalous activity
- 24/7 detection & response
- Eliminates false positives

05. Business Intelligence & Reporting
- Data driven documents created using BI tooling
- Rich analytical reports to identify risk and enhance posture

06. Incident Management & Analytics Platform
- Efficient incident management platform
- Orchestrate incident response, service request and SLA monitoring
- Improve quality and context for incident response

07. Threat Containment
- Mitigating risk with automatic containment
- Block malicious IPs
- Suspend rogue users
- Isolate infected machines

08. Log Management & Compliance
- Secure log storage (1 yr)
- ISO 27001, PCI DSS, GDPR, NIST Compliance reporting

Managed Extended Detection & Response (XDR)

Powered by SecurityHQ

With XDR, receive everything you get with MDR, plus the feature additions that work best for you.

Bring your own license
Use our own turnkey solution or bring your own license and merge the package you want.

Weekly security meetings
Led by Senior Analysts, to illuminate risks, incidents, and security posture enhancements.

24/7 threat detection
24/7 monitoring and identification of threats, anomalies, and policy violations with analyst-driven investigations.

24/7 threat response
Threat Containment and Triage with Incident Management and Orchestration.

How it Works

Businesses now require different combinations of detection and response capabilities. We offer XDR with multiple feature options, to ensure an enhanced security posture specific to your needs.

User Behaviour Analytics: Identify patterns of usage that indicate malicious or anomalous user behaviour. From launched apps, file access, to network activity, monitor who touched what, when and where an element was accessed, how it was made, and how often.

Network Flow Analytics: View and gain a comprehensive view of your entire network infrastructure, by examining sources, target ports, IP addresses and more.

Endpoint Detection & Response: Continually monitor endpoints, gain full visibility of your whole IT environment, detect incidents, mediate alerts, stop breaches, and receive instant advice.

Benefits

- Essential cyber-solutions and improved SIEM experience, combined for multi-layer protection.
- Advanced threat prevention & detection with comprehensive view of risks via real-time monitoring and alerting.
- Compliance standards supported.
- Rapid onboarding with industry experts.
- 24/7 incident response supported by GCIH certified incident handlers.
- Cost Saving - No need to build internal SOC capabilities or maintain the required tools.

System X Threat Containment: IR Security Orchestration Automation and Response (SOAR) for accelerated enrichment, playbooks, and threat containment.

Dark Web Monitoring: Monitor the dark, deep, and visible web to detect risks and alert, investigate and take down off¬ensive content.

XDR Process

Hunt for Threats

Investigate Security Breaches

Collect and Organise Data

Improve Visibility

Speed up Detection and Repsonse Times

Not Sure What You Need? Discuss Feature Options with our Security Analysts.

Back to Contents

Managed Firewalls

Powered by SecurityHQ

Bytes' Managed Firewalls, powered by SecurityHQ, provides businesses with the vital skills and knowledge to fully manage and maximise their existing technology, whilst keeping up with the sophistication of rising cyber threats.

Next generation
Bytes' managed multi-layered stateful FW including application control, DDoS protection, sandboxing, VPN remote access and more.

Specialist skills
Your team is already overstretched. We monitor 10,000+ network sensors & process 50,000+ events per second.

24/7 management
Infrastructure monitored, managed and maintained around the clock, 24/7, every day of the year.

Round the clock support
24/7/365 support from SecurityHQ's award-winning global SOC, operated by expert engineers. ISO 27001, Cyber Essentials and Crown Commercial Service Supplier accredited. ISO 9000/27001 and ITIL certified processes.

The Challenge

Modern firewall management is resource-intensive and requires a high-level of expertise. Traffic must be monitored continuously to detect & respond to threats. Devices must be provisioned, deployed, upgraded, and patched to defend against the latest threats. Policies and configurations must be updated to ensure controls work in multiple environments. If not continually and correctly monitored, networks and data are left vulnerable to attack.

The Solution

Our certified, skilled, and experienced engineers will free IT from the burden of implementing, monitoring, and maintaining their firewall & intrusion prevention system and ensure the optimal performance of your network infrastructure, with 24/7 firewall administration, rule base management, firewall maintenance, backup, and recovery.

Benefits

- Reduce complexity and streamline processes with complete resource management.
- Enhance reputation by minimising breaches, & safeguarding data.
- Address internal skill shortages & staff costs.
- Optimise security policies.
- Reduce attack surface for mitigation of cyber threats.

Our certified, skilled and experienced engineers provide the following services:

- Compliance Reporting
- Backup & Recovery
- Firewall Architecture Planning
- Policy & Rule-set Management
- Patch Management
- Performance & Availability Management
- Device Migration & Deployment

Managed Endpoint Protection (EPP/EDR)

Powered by SecurityHQ

The demand for advanced endpoint security solutions, coupled with skilled analysts to proactively detect and respond to those risks has grown. Bytes Managed Endpoint Protection (EPP) and Endpoint Detection & Response (EDR) service leverages the power of SecurityHQs' 24/7 SOC, together with your choice of enterprise EPP/EDR tooling.

Easily integrated
Our services are simple to deploy & easy to integrate within your systems.

Incident management & analytics platform
For dashboarding, SLA management, ticketing & customer ITSM integration.

Rapid response & smart automation
Central support for automation of IR activities & repetitive processes.

Precise, action-oriented & flexible reporting
Risk based & patch prioritised time, with weekly & monthly reports.

The Challenge

Endpoint security has evolved from traditional antivirus, to comprehensive protection, which includes behavioural detection and attack surface reduction tooling, providing protection from sophisticated malware and evolving zero-day threats. To maximise protection, expert analyst skills are required to ensure that the endpoint attack surface is secured, and that threats are monitored, detected, and mitigated.

Many organisations lack the skills, resources or time to operate, maintain and monitor their EPP/EDR solution, which is why we provide a service wrapper to support our customers' endpoint security, 24/7.

The Solution

We provide the proactive management, to reduce vulnerabilities and the attack surface, and apply security policies with 24/7 monitoring to detect and respond to threats.

Benefits

- Gain control. Endpoints and users are the new perimeter. Take control of the risk.
- Proactive management, reduce vulnerabilities, minimise attack surface and mitigate endpoint risk.
- 24/7 detection & response. Cyber wars need a cyber army.
- Powered by your enterprise, market leading endpoint security tools.
- Reduce costs. Managed Service results in less resource requirements and overhead.

Our Managed EPP/EDR provides a service wrapper to market leading endpoint tools which deliver:

Management: Proactive Security Controls

- Web Content Filtering
- Proactive Vulnerability Management
- Attack Surface Reduction
- Application Control
- Control Folder Access
- Host Firewall Control

24/7 Monitoring Detection & Response

- 24/7 Anti-Virus Detection Response
- Endpoint Detection & Response
- Containment & Response Automation
- Threat Hunting
- SIEM Correlation, Logging & Analytics
- Weekly Meetings & Analytical Reporting

Back to Contents

Managed Microsoft Sentinel

Powered by SecurityHQ

Empower your Microsoft Sentinel with SecurityHQs' 24/7 Security Operations Centre (SOC). Microsoft Sentinel SIEM tool, together with SecurityHQ skills, analytics, and security orchestration, delivers the highest degree of threat detection and incident response.

Azure platform as a service monitoring
Monitor malicious activity from Azure PaaS systems (IIS, SQL, Defender ATP & Azure WAF platforms).

Azure infrastructure as a service monitoring
Correlate suspicious host activity for server & application hosts in Azure IaaS.

User risk monitoring
Detect malicious activity & risky user behaviour that is derived from the log analysis.

Precise, action-oriented & flexible reporting
Risk based & patch prioritised time, with weekly & monthly reports.

How it Works

From users, to apps and devices, to servers on any cloud, see and stop threats before the damage is done. Be it data theft, ransomware, fraud or information governance issues, all organisations have their own security risks. Managed Microsoft Sentinel is the industry-leading solution for businesses to protect against all forms of cyber threats and attacks. Bytes work as an addition to your team, by running Microsoft Sentinel as a service. Our security engineers are experts in advanced analytics and threat hunting, detection, and response, and operate out of Security Operations Centres (SOCs) located around the world, every minute of every day, to ensure maximum security.

Benefits

- 24/7 detection & response. Collect data at cloud scale.
- Identify previously undiscovered threats. Use analytics to minimise false positives.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks.
- Identify anomalous and malicious patterns with automated recovery systems.

Service Overview

Digital Risk & Threat Monitoring

Powered by SecurityHQ

Bytes' Digital Risk & Threat Monitoring identifies attacks, breached corporate material, credentials, intellectual property and brand infringement by harvesting data available on the surface, deep & dark web.

Fast-track investigations
Based on indexing customer URLs, domains, VIPs, IPs & assets.

Direct threat monitoring
Focus on threats that are specific to your industry & business.

Incident management & analytics platform
For dashboarding, SLA management, ticketing & customer ITSM integration analysis.

Instant visibility
Achieve immediate transparency of all your systems & processes.

How it Works

View, monitor, prioritise and analyse all digital elements of your organisation, including Internet, applications, systems, cloud, and hardware. Harvest information from the Dark Web, Deep Web, and public domain for complete visibility.

Our **Digital Risk Complete Service** is suitable for large organizations with multiple brands, domains, and complete coverage of Digital Risks supporting both Threat Intelligence and Brand Monitoring use-cases.

Our **Digital Risk Lite Service** is focused on covering Cyber Threat Intelligence across the surface, dark, and deep web, for mid & small size organizations with a single domain and brand.

Benefits

- 24/7 monitoring of your digital footprint.
- Identify threats: Credentials, breach indicators and IOC detection to neutralise the threat.
- Protect your brand by pursuing direct attacks to specific sectors and utilise campaign tracking.
- VIP Targeting: Your VIPs' will be targeted. Monitor exploits against them.
- Actionable intelligence: Measure and track your company's digital risk and attack surface at any time.

Monitor Surface, Deep & Dark Web

01.
Configure
Identify Key Assets
- Online Infrastructure
- Intellectual Property
- Company Domains

02.
Collect
Monitor for Exposure

03.
Contexualise
Threat Intelligence

04.
Mitigate
Take Action & Protect
- SearchLight Portal
- Automation & Orchestration
- Ticketing Platform or SIEM
- Threat Intelligence Platform
- GRC Platform

Back to Contents

Vulnerability Management Service

Powered by SecurityHQ

Bytes' fully managed Vulnerability Management Service helps businesses protect the integrity of their applications and data by proactively identifying potential attack vectors in their environment by providing visibility into potential exposure areas within a distributed network.

Customisable reporting
Focus on the status of vulnerabilities within your enterprise, including measures, activities, & service summaries.

Accredited & assured
We use ISO 9000/20000/27001 certified processes. Our analysts have CISSP, CCNS, CompTIA, ITIL V3 & COBIT 5.0 certifications.

Single pane of glass dashboard
Comprehensive overview of the vulnerabilities within your network, broken down by severity & current scan results.

Prioritisation & assignment
displays the severity of identified vulnerabilities, their impact & relationship to business criticality.

How it Works

The service may be delivered as either an external or internal solution. When both scanning types are combined, clients are able to differentiate between which vulnerabilities are from the outside, the inside or from both locations.

Internal scanning allows the client to assess the state of vulnerabilities within their enterprise. A large percentage of network-based attacks originate unknowingly from inside a protected or private network.

External scanning presents the hacker's eye view of the network perimeter and highlights open risk exposures. External scans identify and assess only devices with routable IP addresses. Scans are scheduled by the SOC and launched from our Secure Data Centre environment. External scans do not require setup, or hardware/ software investment. External scanning is delivered based on the number of IPs and the frequency of scanning.

Benefits

- Complete visibility of known and unknown assets residing on your network.
- Remediate discovered vulnerabilities in your environment.
- Prioritise and assess discovered assets.
- Receive detailed reporting, including recommendations for remediating discovered vulnerabilities.
- Verify and re-scan to confirm remediated vulnerabilities that have been correctly patched.
- Receive round the clock support from experienced and dedicated Security Engineers.

Stay Ahead of Attackers

Accurate Scanning
Non-invasive, intelligence-gathering scanning system emulates techniques used by attackers, as they build upon knowledge from prior exploits.

Information Monitoring
Generate reports, submit & view vulnerability exceptions, perform on-demand scans & quickly gain insight into risks across your environment.

Risk Prioritisation
With automated asset classification & risk prioritisation, assess & manage risks more effectively.

Expert Support
Let our team of security experts respond to & remediate identifiable vulnerabilities.

Network Detection & Response (NDR)

Powered by SecurityHQ

NDR is a highly sophisticated 24/7 monitoring service which utilise unsupervised Machine Learning (ML), taps into the network and analyses real-time network traffic to form a complex understanding of what is "normal' for your environment as it evolves.

ML algorithms
learn on the job, combined with expert analysts, to create bespoke protection.

Data agnostic
Threat detection across entire estate – everything from laptops, desktops, phones, servers, to IoT, BYOD and Industrial/Operational Control Systems.

Smart automation & rapid response
Central support for automation of repetitive processes.

Unparalleled threat visibility
Look for anomalies, in the normal pattern of behaviour for your unique network.

How it Works

Instead of relying on signatures, the platform establishes a 'pattern of life' for the entities in your infrastructure and uses this knowledge to identify anomalous activity. Darktrace is data agnostic. This allows threat detection across your entire estate – everything from laptops, desktops, phones, servers, to IoT, BYOD and Industrial/Operational Control Systems, including cloud, endpoint, virtual, SaaS and email environments.

By monitoring all raw network traffic, this service models every IP address on your network as well as the network, providing 100% network visibility.

Benefits

- AI-driven investigation, threat hunting, triage, and automation at speed and scale.
- Make visible every attempted attack and deviation.
- Instant network visibility into existing blind spots.
- Comprehensive coverage of your entre digital business.

Service Overview

01. Data Collection
- Syslog
- Cloud API
- Agentless Windows
- Apps & Database

02. Data Processing
- Darktrace and QRadar SIEM analyse and correlate data
- Identifies risky Network behaviour
- Contextualise Intelligence

03. Advanced Analytics Dashboards
- Darktrace Award Winning UI
- QRadar Dashboard
- SecurityHQ Incident Management & Analytics Platform Dashboard

04. Analyse Detect & Respond
- 280 + SOC analysts detect, investigate and respond to anomalous activity
- 24/7 detection & response with SOAR Resilient
- Proactive Threat Hunting

05. Containment
- Mitigating risk with automatic containment with Darktrace Antigena
- Autonomous containment without disrupting business operations

06. Reporting And Analytics
- Data driven documents created using BI tooling
- Rich analytical reports to identify risk and enhance posture

07. Incident Management & Analytics Platform
- Efficient incident management platform
- Orchestrate incident response, service request and SLA monitoring
- Improve quality and context for incident response

Routine Activities
- Darktrace Tuning
- Vendor Co-ordination
- Health Check
- New Dashboard Design

Back to Contents

Testimonials

Bytes Managed Security Services in partnership with SecurityHQ

“The customer-focused, technically astute benefit of the Bytes Managed Security Services experience in implementing a large scale, complex 24x7 security operations such as ours is immeasurable. The team just gets it”

- Mary Kotch, Group CIO/CISO, Aspen Insurance

“To handle threats effectively, Incident management platform consolidates threat intelligence, security analysts, analytics, alerts and response”
“I am confident that Bytes Managed Security Services will have the most comprehensive, secure services in the market.”

- Matt Vassallo, Deputy Group CISO, Aspen Insurance

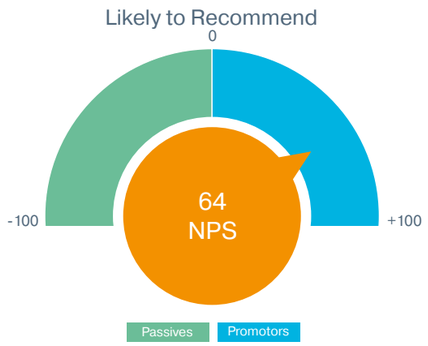
“We are particularly happy with their tailored approach to our security requirements and the way they rapidly adapt to the ever-changing threat landscape.”

– Gurdip Kundi , Operations Director/Infrastructure Manager, Foxtons

Customer Satisfaction Survey

Bytes Managed Security Services in partnership with SecurityHQ

How likely is it that you would recommend Bytes Managed Security Services to a friend or colleague?

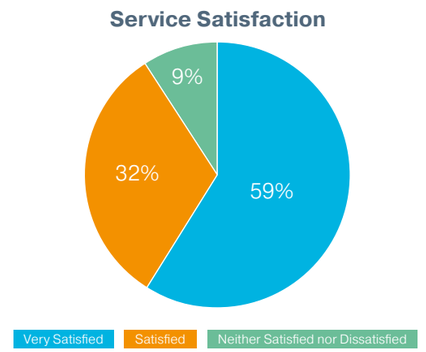


Overall, how satisfied or dissatisfied are you with Bytes Managed Security Services?

Feedback

“Your services are top-notch !!”

- Global CIO, Insurance

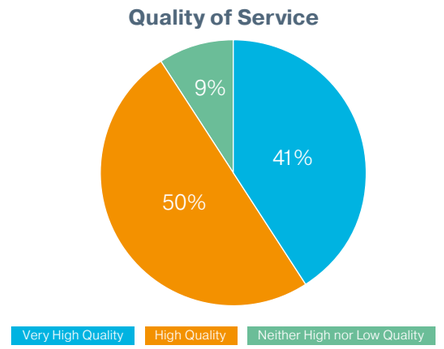


How would you rate the quality of the service?

Feedback

“Great service I am overall happy with your service.”

– CISO, Information Technology

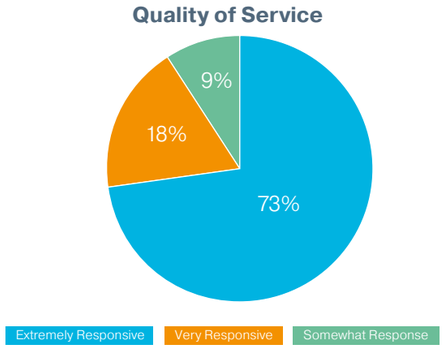


How satisfied are you with your designated Service Manager, their responsiveness and overall relationship management?

Feedback

“Our experience has been great. We have had and continue to have a great working relationship with all staff.”

– Project manager, Computer Software



Why Managed Services?

Luke Kiernan

Head of Security Alliances, Bytes Software Services

“Bytes have been supporting businesses in Cyber Security for 20+ years and our resilient partnership with SecurityHQ takes our managed security service offering to greater strengths. SecurityHQ are a global MSSP that monitors networks 24/7/365, to ensure complete visibility and protection against customers cyber threats. With decades of experience, over 250 ‘eyes on’ security analysts, working across 6+ SOCs, coupled with the precise combination of tools, skills, people and processes to ensure detection and response is met with high standards. Together our goal is to be a powerful extension of a business’s security arsenal, enabling them to meet extensive threats without spiralling resource needs or management complexity. We offer an extensive range of services from Managed SOC, NOC, EDR, Threat Intel, Vulnerability Management and more.”

Steve Marshall

Group CISO and Head of Cyber Consulting, Bytes Software Services

“As technology gets smarter and more automated, we have to rely on multiple solutions to secure it and multiple sources to view the threats to it. This creates pressures on organisations in terms of managing costs and spiralling complexity. Misconfiguration and human error sits at the heart of many successful breaches, and from the work we do with our customers, it is evident that most companies suffer a breach due to the failure of a single security control; a missing patch, a compromised set of credentials, AV not picking up some malware.

Attackers only ever get better and can and do use businesses own tools and solutions against them. The internal overlay required to provide vigilance is only growing and even now is out of the reach of many organisations. Gone are the days of the 'if' or the 'when' of a security incident, we now live in an age of ‘how bad’, and ‘how can I manage the optics of the situation’. Therefore, the key differentiator today is visibility and the time to respond. This requires insight and expertise, 24/7/365, delivered by specialists. Which is why Bytes’ diverse range of managed security services are so vital in today's environment.”

Feras Tappuni

CEO, SecurityHQ

“Both companies, SecurityHQ and Bytes, have taken the time to get a deep understanding of the Managed Security Services offerings for their clients. This is not a new relationship; this is a relationship that has been developed over time and with hundreds of hours of time invested. The growing client list is testament to the work that our teams put in, even more so, the renewal rate shows you the satisfaction level of the clients”.

Chris Cheyne

SOC Director and CTO, SecurityHQ

“Bytes team have a deep understanding of their customers security demands and the best practices required to resolve their challenges. It’s why their customers trust them, and it’s also why our Managed Security Services are a perfect fit for Bytes’ service portfolio.”

Bytes Managed Security Services

Bytes is a leading provider of world-class IT solutions. Our portfolio of services includes cloud, security, end-user computing, datacentre, data management, licensing, asset management, storage, virtualisation, training, deployment and managed services.

We work with SME’s, corporates and public sector organisations to modernise and digitally transform their IT infrastructures. Established in 1982, Bytes has grown rapidly and now employs over 450 people across 5 locations in the UK and Ireland. Our turnover in FY 2019 was in excess of £520M. Thanks to our passionate people and close vendor partnerships, we've helped hundreds of top brands transform, grow and adapt to the changing technology landscape.

Reasons to partner with Bytes:

- Microsoft’s No.1 UK Partner
- Top 3 supplier to the NHS and approved for 30+ Public Sector buying frameworks
- 20+ years experience within our Specialist Security Division
- Top accreditations with 100+ technology partners
- 1,000+ vendor solutions sold per year
- 3,500+ customers - 93% rate service good/excellent & 96% would recommend us
- Sunday Times 100 Best Companies to Work For 2020

Learn how we can help you, visit **www.bytes.co.uk**

Discover More!

Get in touch on:

+44 1372 418500

or **Tellmemore@bytes.co.uk**

Alternatively find us at **https://www.bytes.co.uk/security/managed-security-services**

SecurityHQ

SecurityHQ is a Global MSSP, that detects, and responds to threats, instantly. As your security partner, we alert and act on threats for you. Gain access to an army of analysts that work with you, as an extension of your team, 24/7, 365 days a year. Receive tailored advice and full visibility to ensure peace of mind, with our Global Security Operation Centres, and utilize our award-winning security solutions, knowledge, people, and process capabilities, to accelerate business and reduce risk and overall security costs.

BYTES | Smarter together