Open

Cyber Security & Enterprise Networking Customer Engagements

BYTES

Introduction & Overview

Bytes' Cyber Security Division is a leading provider of comprehensive IT security solutions with over 25 years of experience. We focus on delivering end-to-end and integrated cyber security methodology to our customers including consultancy, solutions, services and insights. Our approach is consultancy-led, ensuring we understand each clients' specific challenges and business goals, to provide innovative and relevant security solutions.

This playbook showcases our customer engagements available to you. Each engagement is led by our expert team of specialists, who will guide you through each step of your journey and provide valuable insights and advice along the way.

Our team of over 70+ specialists encompasses various roles, including solutions, technical, delivery, consultancy, support, and vendor management. Over the years, we have grown significantly, now delivering £400M worth of projects annually. As a result, our customers can trust that they are in capable hands for all their cyber security needs.

> "Over our 25-year journey in the Cyber Security industry, our primary goal has been to support our customers in reducing their cyber risk, protecting their brand and safe guarding their data. This commitment remains as strong today and will continue for the next 25 years. We take pride in forging deep relationships with our customers by becoming an extension to their own teams, allowing us to fully understand their needs."

Luke Kiernan,
Head of Cyber Security, Bytes

Watch the Bytes Cyber Security video

Workshops & Services ›

Cyber Security Customer Engagements

Bytes Workshops & Services

BYTES

Network & Cloud Security

- Cloud & Application Market Review
- Check Point Firewall Health check
- Check Point Free Ticket
- Check Point User License Review
- Data Security Workshop
- Inside The Network Market Review
- The New Edge Workshop

Endpoint & User Security

- Email Resilience Market Review
- Endpoint Security Market Review
- Identity Market Review
- Phishing Assessment Service

Cyber Strategy, Services & Management

- Application Testing Services
- Attack Surface Mapping Services
- Breach Assessment Services
- CAF Gap Analysis
- Cloud Configuration Review Services
- Cloud Security Audit Service
- Cloud Testing Services
- CIS Gap Analysis
- Digital Forensic and Incident Response Management
- Hackers Health Check
- Infrastructure Penetration Testing & Vulnerability Assessment Services
- Posture Control Testing Services
- Red Team Services
- Zero Trust Market Review

Enterprise Networking

- Cisco Lifecycle Review
- Network Maturity Assessment

Microsoft

- Microsoft Cloud Security Review
- Microsoft Copilot for Security
- Microsoft Data Security Workshop
- Microsoft Secure Infrastructure Review
- Microsoft Sentinel Activation Workshop
- Microsoft Sentinel Workshop
- Microsoft Threat Protection Workshop

Glossary of Terms

FOC
Engagement

Back to contents

The Future Is in The Cloud – Are You Ready?

Cloud & Application Market Review

BYTES

As organisations increasingly migrate their operations and applications to the cloud, they encounter a host of new challenges. Simply lifting and shifting on-premises solutions won't suffice to address cloud-centric security considerations. Fortunately, many innovative technologies have emerged to tackle these very issues.

- ✓ **Application Security Testing (SAST, SCA)** spreads DevSecOps methodologies from looking at code in development, all the way into the management and maintenance of the cloud platforms themselves.
- ✓ **Cloud Native Application Protection Platforms (CNAPP)** look directly at security posture, configuration, and vulnerabilities across multi-cloud environments.
- ✓ **Cloud Service Network Security (CSNS)** solutions protect the external facing elements, helping to maintain operational ability and data security.

Across all these elements is the need to maintain least privilege access for developers and administrators.

Bytes are able to help by simplifying an incredibly complex market, saving you time and providing greater clarity regarding the technology landscape.

Our Methodology

Our security specialists work with you to identify your key business challenges and requirements, then walk you through the various options that you have to strengthen your security posture.

The result – clear and simple guidance to further the security of your cloud and applications.

Tech Areas: SAST, SCA, WAAP, CNAPP, CNAP, WAF, NGFW, DAST

Key Features & Benefits

- ✓ A Rounded Understanding Of Your Environment
- ✓ Simplified View Of The Market
- ✓ Bespoke
- ✓ Zero Cost
- ✓ Independent Advice

Key Steps

Understand:

Overview of your dev processes and cloud platforms
Your security road map & requirements

Overview:

Where you are on the journey of development to deploy to customer interaction
How can security tools transform the way you work
Which vendors & vendor comparison

Evaluate:

Pairing client requirements to technology landscape
Narrowing down potential vendors

What To Expect

During this engagement **Bytes** security experts will guide you through the cloud & app security challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

- ✓ **1:1 Interactive Session**
- ✓ **Expert Advice and Guidance**
- ✓ **Can support multiple stakeholders**
- ✓ **Sessions run remotely or in person**
- ✓ **Experience across entire Application and Cloud Security spectrum**

Back to contents

When was the last time you checked your Firewall Estate?

Check Point Firewall Health Check

CHECK POINT BYTES

Our fully accredited Check Point engineers capture and analyse your firewall raw data to find predictive indicators of common firewall failures.

We check all important data points relating to core Check Point functionality including management, access control, firewall, and clustering.

We then walk you through a detailed report of your results including remediation recommendations, so you fully understand the next steps.

Unnoticed over time, many issues can develop that hamper your network performance. If left unchecked these can lead to business impacting events.

Find out more about how Bytes can help you with our **Check Point Firewall Health Check** by contacting us today.

The Bytes Check Point health check is a fast, non-disruptive process that goes right under the hood of your firewall systems, giving them a full MOT. It highlights any lurking issues and ensures that everything is running as it should, giving you complete confidence in your firewall capacity.

Clear, Tangible Results

Individual elements are classed as ‘pass’, ‘fail’ or ‘advisory

✓

Pass
Peace of mind that this area of firewall performance is optimal

✗

Fail
A configuration that is unsupported and could lead to a business impacting event

!

Advisory
A configuration that is unsupported and could lead to a business impacting event

What we Check

- ✓ Core OS Configuration
- ✓ CPU and Memory Utilisation
- ✓ Interface Health
- ✓ Packet Handling
- ✓ Routing
- ✓ Process Status
- ✓ Secure XL and CoreXL
- ✓ Cluster Operation
- ✓ Backup Operation
- ✓ Software Patching

FOC
Engagement

Back to contents

Try out Check Point Direct-to-Engineer Telephone Support Free of Charge

Check Point Free Ticket

CHECK POINT BYTES

Do you have a nagging Check Point ticket that just isn't getting sorted?

Our fully accredited Check Point engineers capture and analyse your firewall raw data to find predictive indicators of common firewall failures.

We check all important data points relating to core Check Point functionality including management, access control, firewall, and clustering.

We then walk you through a detailed report of your results including remediation recommendations, so you fully understand the next steps.

Unnoticed over time, many issues can develop that hamper your network performance. If left unchecked these can lead to business impacting events.

The **Bytes** Check Point health check is a fast, non-disruptive process that goes right under the hood of your firewall systems, giving them a full MOT.

It highlights any lurking issues and ensures that everything is running as it should, giving you complete confidence in your firewall capacity.

What is SPARC (Security Partnerships Active Response Centre)

15+
SPARC has been in operation for 15+ years

80%
80% of support tickets resolved inhouse

24%
24% of issues solved on first call (industry standard is 7-10%)

Direct to 3rd line Support Desk

Drastically less customer downtime

5
Every engineer has a minimum of 5 years' experience

What makes SPARC different ?

We don't believe in first line support. All SPARC engineers are escalation level and you speak to them direct on every call. This means you access the right level of expertise first time. SPARC clients receive a level of support that reduces both 'time-to-fix' and their level of involvement in the ticket resolution process. This means support analysts spend a greater amount of time supporting their business and leave our experts to give them the updates.

SPARC Features

- ✓ Fully accredited engineers in-house
- ✓ Remote access trouble-shooting
- ✓ Escalation level engineers on every call
- ✓ Technical advice
- ✓ Proven issue processes
- ✓ Detailed support SLAs
- ✓ Reduced support overhead
- ✓ Every second counts attitude
- ✓ Remote technical assistance

Check Point ELITE PARTNER ★★★★

Check Point User License Review (ULR)

CHECK POINT™ BYTES

The Bytes and Check Point partnership spans over two decades.

As one of the first partners to be promoted to Elite partner status, Bytes' commercial acumen and technical capability go hand in hand to deliver the most effective and secure solutions for our customers, underpinned by our trusted and second-to-none SPARC support team.

We know over time licensing can become disjointed, out of sync and sometimes difficult to determine the value you are receiving. **Bytes welcome the opportunity to perform a Check Point User Center License Review with you to address these challenges.**

A ULR allows us to quickly determine a number of factors within your estate that customers often come up against;

- ✓ Understanding licensing and subscription package contents
- ✓ Highlighting End of Engineering / End of Life timeframes
- ✓ Legacy or superseded product types
- ✓ Opportunities for consolidation and reducing unnecessary expenditure
- ✓ Misaligned renewal dates causing complexity
- ✓ Support levels and whether they align to business needs
- ✓ And general best practices to address administrative headaches

By partnering with Bytes, we jointly determine clarity on your current estate, cost-optimisation through maximising what you have and renewing only what you are using, and consensus on your strategy moving forward.

All we require is any relevant Usercenter numbers and permission from you to begin the process. The ULR is complimentary - we would welcome the opportunity to demonstrate any potential recommendations based on our findings.

Check Point
ELITE
PARTNER
★★★★

Partner Awards

2020
- Cloud Partner of the Year for EMEA
- Best Strategic Partner Contribution of the Year

2021
- Cloud Security Partner of the Year
- Infinity Partner of the Year

2022
- Cloud Partner of the Year
- Top Cloud Partner EMEA
- Harmony Partner of the Year

Secured by Check Point, Powered by Bytes

CHECK POINT™

- ✓ Dedicated Check Point SPARC Support Service since 2005
- ✓ 10+ CCSM Elite Engineers
- ✓ All tickets Direct to 3rd-line engineer
- ✓ 85%+ Support tickets resolved in-house
- ✓ 24×7 P1 service
- ✓ 'Free SPARC ticket' service available

BYTES

- ✓ Check Point Partner since 1999
- ✓ Check Point Elite tier, by invite-only
- ✓ Longest-standing Infinity Partner
- ✓ 2020 - £100m+ revenue cyber security division
- ✓ 2022 Cloud Partner of the Year

FOC
Engagement

Back to contents

Don't let your data walk away.

Data Security Workshop

BYTES

As digital landscapes expand and evolve, managing data is an increasingly complex challenge for organisations. Governance and compliance require strict regulations to be adhered to, whilst adopting hybrid and multi-cloud infrastructures has led to data sprawl. In addition, ransomware attacks are on the rise, reinforcing the need for robust data security.

There is no single technology that enables organisations to have a complete data security platform, meaning designing a data roadmap is crucial to success and choosing the right combination of technologies is the key to a robust data security program.

Discovery | **Key Management** | **Data Encryption**

Back Up | **Classification** | **DLP**

Bytes are able to help by simplifying an incredibly complex market, saving you time, and providing greater clarity regarding the technology landscape.

Our Methodology:

Our security specialists work with you to discuss your existing landscape, identify your current challenges, and run through a step-by-step process of optimal data management and security, designed to strengthen your data posture and resilience.

The Result:

A clear roadmap of your data security journey from discovery to prevention.

Key Features & Benefits

- ✓ A Rounded Understanding Of Your Environment
- ✓ Simplified View Of The Market
- ✓ Bespoke
- ✓ Zero Cost
- ✓ Independent Advice

Key Steps

Understand:

- Overview of your current data landscape
- Discuss where the client is on their data journey

Overview:

- What does an optimal data roadmap look like?
- How can efficient data management and security benefit your organisation
- Solution highlights

Evaluate:

- Discuss leading technology vendors and market trends
- Align with client requirements

What To Expect

During this engagement Bytes security experts will guide you through typical data challenges & solutions with a vendor agnostic approach, ensuring the best fit for your organisation.

- ✓ **1:1 Interactive Session**
- ✓ **Expert Advice and Guidance**
- ✓ **Can support multiple stakeholders**
- ✓ **Sessions run remotely or in person**
- ✓ **Experience across the complete data management and security lifecycle**

Back to
contents

Demystify the digital landscape

Inside The Network Review

BYTES

With networks becoming more complex with the number of devices that have internet access, it's difficult to understand what's on your network and which areas these devices can access. There are now lots of technologies to help deal with these issues and to keep your network secure.

Network Detection and Response:

NDR identifies and stops evasive network threats that cannot be easily blocked using known patterns and signatures.

Network Access Control:

NAC restricts unauthorised users and devices from gaining access to your corporate or private network.

IOT/OT Security:

IOT security focuses on non-IT assets and

their data. Whereas OT security safeguards control systems for physical industrial and medical processes.

Micro Segmentation:

Micro segmentation divides data centres into distinct security segments down to the individual workload level to ensure security controls can be defined. This creates secure zones across cloud and data centre environments, isolating application workloads from one to another and securing them individually.

Find out more about how Bytes can help you with your Network Security strategy by booking in a workshop today.

Our Methodology

Our security specialists work with you to identify your key network security business challenges and requirements, then walk you through the various options to help strengthen your security posture.

The Result

Clear and simple guidance to further the security inside your network.

Key Features & Benefits

- ✓ A Rounded Understanding Of Your Environment
- ✓ Simplified View Of The Market
- ✓ Bespoke
- ✓ Zero Cost
- ✓ Independent Advice

Key Steps

Understand:

Overview of your internal network

Discuss where your |security road map & requirements

Overview:

Where you are on your organisations journey of securing your network

How security tools can transform the way you work

Which vendors & vendor comparison

Evaluate:

Pairing your requirements to your technology landscape

Narrowing down potential vendors

What To Expect

During this engagement **Bytes** security experts will guide you through core identity challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

- ✓ **1:1 Interactive Session**
- ✓ **Expert Advice and Guidance**
- ✓ **Can support multiple stakeholders**
- ✓ **Sessions run remotely or in-person**
- ✓ **Experience across entire Identity Spectrum**

Back to contents

Creating Tomorrow's Solutions Today

The New Edge Workshop

BYTES

As working practices change and businesses evolve to meet the demands of their workforces, clients and competition, traditional networking and infrastructure have fallen by the wayside. With the emergence of cloud, SaaS & hybrid working there is an ever increasing need for progressive technology that can keep up with the new and developing security challenges.

This is where the **New Edge** comes in; a security approach that ensures all areas of your organisation are secure and not just those located behind the firewall. Securing the new edge involves a combination of technologies coming together including:

- **Zero Trust Network Access**
- **CASB**
- **Secure Web Gateway**
- **SD-WAN**
- **Firewalling**
- **DLP**

Bytes are able to help by simplifying an incredibly complex market, saving you time and providing greater clarity regarding the technology landscape.

The New Edge Video

Our Methodology

Our security specialists work with you to identify your key network security business challenges and requirements, then walk you through the various options to help strengthen your security posture.

The Result

a clear map of your journey to a simple, secure new edge

Key Features & Benefits

- ✓ A Rounded Understanding Of Your Environment
- ✓ Simplified View Of The Market
- ✓ Bespoke
- ✓ Zero Cost
- ✓ Independent Advice

Key Steps

Understand:

Overview of your internal network

Discuss where your security road map & requirements

Overview:

Where you are on your organisations journey of securing your network

How security tools can transform the way you work

Which vendors & vendor comparison

Evaluate:

Pairing your requirements to your technology landscape

Narrowing down potential vendors

What To Expect

During this engagement **Bytes** security experts will guide you through core identity challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

- ✓ **1:1 Interactive Session**
- ✓ **Expert Advice and Guidance**
- ✓ **Can support multiple stakeholders**
- ✓ **Sessions run remotely or in-person**
- ✓ **Experience across entire New Edge Spectrum**

Back to contents

Keeping Every Person Secure

Email Resilience Market Review

BYTES

Bytes are here to help combat the challenges that surround email. Our **free Email Resilience Market Review** is designed to help map out an email strategy for your business which gets the balance between security and convenience right.

Email remains the most used and critical application within most businesses and therefore becomes the number one attack vector for cybercriminals. The simple fact remains that securing email is one of the most important steps any organization can take to safeguard against business disruption, data loss and financial damage.

Our Methodology

Our security specialists work with you to identify your key email related business challenges and requirements, then walk you through the various options that you have to strengthen your security posture.

The result – a clear map of your journey to a simple, secure email gateway.

We offer guidance on a variety of the key pillars of email resilience including:

- **Email Security**
- **Backup & Data Recovery**
- **Archiving**
- **API**
- **DMARC**
- **Machine Learning & AI**
- **Awareness Training**

Key Features & Benefits

✓ Simplicity
✓ Bespoke
✓ Detailed
✓ Zero Cost
✓ Independent Advice

Key Steps

Assess:

- Evaluate current requirements
- Explore the Security roadmap
- Understand customer challenges

Discover:

- Deliver workshop and knowledge transfer
- Analyse and discover gaps
- Consider vendors and offerings

Recommend:

- Align appropriate technologies to create solutions
- Provide a bespoke solution recommendation report to assist with business cases

What To Expect

During this engagement Bytes security experts will guide you through core email resilience challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

✓ **1:1 Interactive**
✓ **Insight into Market Leading Technology**
✓ **Recommendations on Current & Future Investments**
✓ **Report detailing Recommendations & Next Steps**

FOC Engagement

Back to contents

Keeping Every Endpoint Secure

Endpoint Security Market Review

BYTES

70% of all breaches originate at the Endpoint according to the IDC. It has always been important for organisations to understand how to secure endpoints and as attackers become bolder this has never been more important.

Working out what you need from an endpoint solution and where you are from a Security Strategy point of view can be a daunting task but is needed before you can ensure security for all of your endpoints. task but is needed before you can ensure security for all of your endpoints.

Bytes are here to help. Our **free Endpoint Market Review** is designed to help you map out an Endpoint strategy for your business which gets the balance between security and convenience right.

Our Methodology

Our security specialists work with you to identify your key endpoint challenges and requirements, then walk you through the various options that you have to strengthen your security posture.

The result – a clear map of your journey to simple, secure endpoints.

We Offer Guidance on All Types of Endpoints & Cover All Main Topics

- Desktop/ Laptop/Server
- VDI
- Mobile
- XDR/MDR
- Managed Services
- Threat Intelligence
- AI & Automation
- Identity Threat Detection

Key Steps

Assess:

- Evaluate current requirements
- Explore the Security roadmap
- Understand customer challenges

Discover:

- Deliver workshop and knowledge transfer
- Analyse and discover gaps
- Consider vendors and offerings

Recommend:

- Align appropriate technologies to create solutions
- Provide a bespoke solution recommendation report to assist with business cases

What To Expect

During this engagement Bytes security experts will guide you through core email resilience challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

- ✓ **1:1 Interactive**
- ✓ **Insight into Market Leading Technology**
- ✓ **Recommendations on Current & Future Investments**
- ✓ **Report detailing Recommendations & Next Steps**

FOC Engagement

Back to contents

Balance Risk and Convenience, Keeping Everyone Secure

Identity Market Review

BYTES

Bytes are here to help. Our **free Identity & Access Workshop** is designed to help you map out an Access & Identity strategy for your business which gets the balance between security and convenience right.

80% of Security Breaches are caused by compromised or weak credentials. Now more than ever, it's important for businesses to understand how to secure user access, balancing the need for 'right now' access to critical resources with business risk and compliance.

Working out the correct approach can be complex but is business critical in order to provide your staff, customers and third parties with just the right access to the right resources in the right place at the right time.

Our Methodology

Our expert engineers work with you to identify your key access challenges and requirements, then walk you through the various options that you have to strengthen your security posture whilst ensuring smooth, simple user access.

The result – a clear map of your journey to simple, secure user access at every point of your business – from new staff onboarding to privilege management.

Guidance on 6 different areas of Identity & Access Management

- ✓ Multi-Factor Authentication & Single Sign On
- ✓ Identity Lifecycle Management
- ✓ Identity Access Management
- ✓ Privilege Access Management
- ✓ Identity Threat Detection
- ✓ Identity Governance & Administration

Key Steps

Assess:

- Evaluate current requirements
- Explore Security roadmap
- Demonstrate Multi Factor Authentication & Single Sign On

Discover:

- Deliver workshop and knowledge transfer
- Analyse and discover gaps
- Consider vendors and offerings

Recommend:

- Align appropriate technologies to create solutions
- Provide a bespoke solution recommendation report to assist with business cases

What To Expect

During this engagement **Bytes** security experts will guide you through core identity challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

1:1 Interactive Session

Expert Advice and Guidance

Can support multiple stakeholders

Sessions run remotely or in-person

Experience across entire Identity Spectrum

Chargable Engagement

Back to contents

Strengthen Your Cyber Defences

Phishing Assessment Service

BYTES

At **Bytes**, we offer proactive Phishing Assessment Services designed to safeguard your business against increasingly sophisticated cyber threats. Our tailored assessments ensure a resilient and secure business environment.

Are You Protected?

In today's dynamic cyber threat landscape, undetected vulnerabilities pose significant risks to your business's security. Our Phishing Assessment Service is proactive, identifying and mitigating these risks through meticulous evaluations. We uncover potential entry points for phishing attacks, empowering you to fortify your defences and stay ahead of evolving threats.

Is This Service for You?

Recognise the need for a phishing assessment by identifying key indicators such as increased phishing attempts, successful attacks, or compliance obligations. Evolving business landscapes and similar businesses experiencing attacks also emphasise the importance of evaluating your security posture.

Protect your business proactively against potential threats with Bytes **Comprehensive Phishing Assessment Services**.

Why You Need This

Security Awareness: Educate and raise awareness among your employees about phishing tactics, making them more vigilant against potential threats.

Risk Identification: Discover vulnerabilities in your systems and practices, addressing weaknesses before real threats exploit them.

Prevention and Mitigation: Implement targeted measures to prevent and mitigate phishing attacks by refining protocols, enhancing employee training, and employing robust security technologies.

Compliance Requirements: Meet regulatory standards and protect sensitive data while avoiding penalties through regular phishing assessments.

Asset Protection: Strengthen defences to safeguard sensitive information and assets from potential compromise, averting data breaches and financial losses.

Continual Improvement: Regular assessments provide insights into evolving threats, enabling you to adapt and enhance defences accordingly.

What's Included?

Our Phishing Assessments involve essential stages:

Planning & Preparation: Define assessment scope and objectives, targeting vulnerabilities, employee awareness, and security measures.

Reconnaissance & Intelligence Gathering: Craft lifelike phishing scenarios by collecting relevant information.

Execution of Phishing Campaigns: Simulate attacks, monitor responses, and evaluate campaign effectiveness.

Analysis & Reporting: Analyse results, identify weaknesses, and provide a detailed report with recommendations.

Training & Remediation: Educate employees and implement enhanced security controls.

Follow-up & Continuous Improvement: Monitor security and schedule periodic assessments for ongoing protection.

Chargable
Engagement

Back to contents

Assure quality, secure functionality

Application Testing Services

BYTES

Given the prevalence of cyber-attacks, regular application testing is essential. Bytes cyber services detect hidden vulnerabilities, ensure compliance with industry standards, and maintain customer trust. We assess current security measures to guide future cybersecurity investments, enhancing your overall security posture and resilience against threats.

Bytes' Application Testing Services target security vulnerabilities in web, API, mobile, and desktop applications. **CREST-certified** testers conduct thorough assessments, offering expert analysis and tailored insights.

By simulating real-world attacks, we pinpoint weaknesses and provide comprehensive reports with risk levels and remediation steps, ensuring robust protection for your applications.

With extensive experience in penetration testing and vulnerability assessments, **Bytes** delivers detailed, actionable recommendations. Our proven success across various industries makes us a reliable partner in safeguarding your applications and business operations against potential threats.

Find out more about how Bytes can help you with our **Application Testing Services** by contacting us today.

Key Benefits

✓ **Comprehensive Security Assessment:** Our penetration testing covers all application types, from web, API, mobile and desktop.

✓ **Expert Analysis:** CRESTcertified testers deliver detailed insights and recommendations.

✓ **Customised Testing:** Tailored to meet your specific needs, whether for a full-scale assessment or targeted testing.

✓ **Vulnerability Identification:** Discover hidden weaknesses before attackers do.

✓ **Compliance:** Ensure adherence to industry standards and regulations.

✓ **Security Assessment:** Evaluate the effectiveness of current security measures.

✓ **Proactive Defence:** Stay ahead of emerging threats with regular testing.

Why Choose Bytes?

✓ **Certified Expertise:** Our team of CREST-certified testers brings extensive experience and proven success across various industries.

✓ **Thorough Coverage:** We ensure all aspects of your infrastructure are thoroughly examined, leaving no vulnerabilities overlooked.

✓ **Proven Track Record:** We ensure all of our engagements are successful across various industries.

✓ **Actionable Insights:** We provide detailed reports with clear, prioritised recommendations to effectively address security issues.

Chargable Engagement

Back to contents

Defining Potential Attack Vectors

Attack Surface Mapping Services

BYTES

At Bytes, we offer advanced Attack Surface Mapping Services, employing OSINT (Open- source Intelligence), dark web monitoring, and active scanning techniques to map potential attack vectors. Our assessments provide a comprehensive view of your organisation's digital footprint, ensuring a proactive approach to bolstering your cybersecurity defences.

Why Attack Surface Mapping Matters:

Attack Surface Mapping involves a thorough examination of your digital footprint, identifying potential entry points for cyber threats. Utilising OSINT, dark web monitoring, and active scanning, we comprehensively map out potential attack vectors to strengthen your security posture.

Is Attack Surface Mapping Right for You?

Consider an Attack Surface Mapping assessment if proactively identifying potential attack vectors and fortifying your cybersecurity defences is essential for your organization.

Secure your organization against cyber threats with Bytes Comprehensive **Attack Surface Mapping Services.**

Why Choose Our Attack Surface Mapping Services.

- ✓ **Proactive Security Approach:** Identify and address potential vulnerabilities before they're exploited by threat actors.
- ✓ **Comprehensive Threat Discovery:** Gain insights into your organisation's digital footprint, ensuring a proactive defence strategy.
- ✓ **Risk Mitigation:** Address identified vulnerabilities to reduce the risk of cyber threats and attacks.
- ✓ **Protection of Sensitive Data:** Safeguard sensitive information from exposure by identifying potential leaks or breaches.
- ✓ **Continual Improvement:** Leverage insights to continuously refine security strategies and fortify defences.

What's included?

Our Attack Surface Mapping involves essential stages:

OSINT and Dark Web Monitoring: Extensive examination of publicly available information and dark web sources to identify sensitive data exposure or potential threats.

Comprehensive Reporting: Detailed reports outlining discovered attack surfaces, potential vulnerabilities, and recommendations for mitigation.

Mapping Potential Attack Vectors: Identify and document potential avenues for cyber-attacks within your organisation's digital landscape.

Active Scanning Techniques: Vulnerability scanning of networks and systems to discover weaknesses and potential entry points.

Chargable Engagement

Back to contents

Strengthening Your Security Posture

Breach Assessment Services

At **Bytes**, we offer proactive Breach Assessment Services tailored to fortify your organization's security against potential breaches. Our comprehensive assessments ensure a resilient and secure business environment.

Why Breach Assessment Matters:

Breach assessments are crucial to simulating an attacker's actions after gaining access to your environment. Equipped with standard user credentials, our expert testers execute a simulated breach scenario to identify vulnerabilities and evaluate your security defences.

Is Breach Assessment Right for You?

Identify the need for a breach assessment if proactive security measures, compliance obligations, or concerns about potential breaches are critical for your organization.

Protect your organization from potential breaches with Bytes Comprehensive Breach Assessment Services.

Why Choose Our Breach Assessment Services?

✓ **Proactive Security:** Identify weaknesses before malicious actors exploit them.

✓ **Enhanced Defence Strategies:** Implement targeted measures to bolster your defences against potential breaches.

✓ **Risk Mitigation:** Mitigate the impact of security breaches by addressing vulnerabilities proactively.

✓ **Compliance and Protection:** Comply with industry standards and protect sensitive data from breaches and associated damages.

✓ **Continuous Improvement:** Leverage insights from assessments to continually enhance your security posture.

What's Included?

Our Breach Assessment involve essential stages:

Simulation of Intrusion: Testers simulate an attacker's actions upon gaining access using standard user credentials.

Analysis and Reporting: Detailed reports outlining findings, vulnerabilities, and actionable recommendations to fortify defences.

Evaluation of Security Measures: Comprehensive assessment of existing security protocols and defences.

Identification of Vulnerabilities: Pinpoint weaknesses and potential entry points an attacker might exploit.

Back to contents

Providing Expert Analysis of Your Security Solutions, Processes & Procedures:

CAF Gap Analysis

BYTES

Bytes

CAF Gap Analysis provides organisations with a security focused gap analysis based on the National Cyber Security Centre Cyber Assessment Framework (NCSC CAF).

The NCSC CAF outlines 14 cyber security & resilience principles, which are recognised to have a material impact on your ability to prevent cyber attacks and to reduce the overall risk associated to your IT infrastructure.

The **Bytes CAF Gap Analysis** provides expert analysis of your security solutions, processes, and procedures to provide tangible recommendations on how best to improve your organisation's security posture.

Why Bytes Offer This

The CAF Gap Analysis session allows Bytes to deliver value to the customer by assisting in the alignment of their security infrastructure to industry recognised frameworks.

- Collate information on your current security solutions, their functionality & utilisation.
- Deliver a session outlining the results, identifying key focus areas & outlining improvement recommendations.
- Provide a detailed report with RAG Matrix, tangible next steps, improvement areas & impact of gap analysis.
- Compare your current security provision across multiple areas to the 14 cyber security & resilience principles.

Key Features & Benefits

✓ **Simplicity:** No tools or scripts

✓ **Bespoke:** Tailored to each individual company

✓ **Detailed:** Encompasses all areas of security best practice

✓ **Industry Recognised:** Internationally approved, continually updated framework

✓ **Zero Cost:** Our expert-led service is completely free

✓ **Independent advice:** Vendor agnostic approach focused on best practices

What To Expect?

The CAF Gap Analysis is delivered through the following stages:

Discovery: We collect and collate information on your current security solutions, processes and procedures.

Analysis: We reference your answers against the 14 principles of the NCSC CAF.

Consultation: We host a session to discuss and clarify the information collected and to gather any additional information needed to create your report.

Outcome: A bespoke and detailed report is produced and will include a high-level score against each of the 14 principles, as well as detailed explanations to justify the score and recommendations for next steps to improve the overall result.

Chargable Engagement

Back to contents

Ensuring Compliance and Security

Cloud Configuration Review Services

BYTES

At Bytes, we provide meticulous Configuration Review Services for cloud environments including Azure, Microsoft 365, Amazon Web Services (AWS) or Google, tailored to guarantee compliance and bolster security measures. Our assessments align your configurations with industry benchmarks for a secure and compliant cloud environment.

Why Configuration Review Matters:

Evaluating configurations against industry benchmarks such as CIS Benchmark (Level 1 or Level 2) is crucial for ensuring compliance and fortifying security. Our expert assessments ensure your cloud environments adhere to these standards, minimising vulnerabilities and ensuring robust security.

Is Configuration Review Right for You?

Consider a configuration review if maintaining compliance, fortifying security measures, or ensuring adherence to industry standards is vital for your cloud environment.

Secure your cloud environment and ensure compliance with **Bytes Comprehensive Configuration Review Services.**

Why Choose Our Configuration Review Services?

- ✓ **Compliance Assurance:** Ensure adherence to industry benchmarks, meeting regulatory standards and avoiding penalties.
- ✓ **Enhanced Security Measures:** Implement recommended changes to fortify configurations against potential vulnerabilities.
- ✓ **Risk Mitigation:** Proactively address configuration weaknesses to minimize security risks.
- ✓ **Protect Critical Assets:** Safeguard sensitive data and critical assets within your cloud environments.
- ✓ **Continual Compliance:** Maintain ongoing compliance through periodic assessments and updates.

What's included?

Our Configuration Review involve essential stages:

Evaluation Against Industry Benchmarks: Thorough assessment of configurations against CIS Benchmark (Level 1 or Level 2)standards.

Identification of Compliance Gaps: Pinpoint deviations from industry benchmarks, highlighting potential security risks.

Analysis of Configurations: Detailed examination of your cloud settings to identify vulnerabilities.

Comprehensive Reporting: Detailed reports outlining assessment findings, compliance gaps, and actionable recommendations for security enhancement.

Chargable Engagement

Back to contents

A single viewpoint from which to secure your cloud

Cloud Security Audit Service

CHECK POINT

BYTES

This service offers you Check Point's award-winning Cloud Guard Posture Management cloud compliance solution for 30 days, at no cost, so you can detect and plug your cloud security and compliance gaps.

Bytes set up your trial Cloud Security Posture Management account. Within 15 minutes, your cloud platforms are connected.

You start to see results within an hour. Gain a clear, detailed and complete map of your overall public cloud health.

Continuous audit and assessment is vital to avoid cloud misconfigurations, compromises and breaches.

Trial lasts 30 days at no cost or obligation.

Bytes free Cloud Security Snapshot provides complete visibility of your public cloud assets and their compliance across Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, or, all three combined.

A clear, detailed, and complete security map of your cloud architecture – with results within an hour – at no cost.

The Result

A true picture of your cloud assets & compliance across multiple public clouds.

✓ **Cloud Assets Configuration**
Identify which applications and workloads you have running on the cloud.

✓ **Public Exposure Levels**
Understand the applications & workloads that are public-facing & more vulnerable to threats.

✓ **Network Topology**
Review your network layout & understand areas prone to threat exposure.

✓ **Security Groups**
Discover and classify your security groups by varying exposure levels.

✓ **Traffic & User Activity**
Review how applications and workloads interact & the traffic associated.

Service Benefits

Onboarding of multiple cloud platform accounts.

An overview of any security issues that are identified by the platform.

The ability to run a continuous compliance rule set on each account.

Remediation steps against best practice.

Find out more about how Bytes can help you with our **Cloud Security Audit Service** by contacting us today.

Chargable Engagement

Back to contents

Ensuring excellence in the cloud, one test at a time

Cloud Testing Services

Bytes' Cloud Testing Services identify and mitigate security vulnerabilities in cloud environments. Our comprehensive approach, conducted by **CRESTcertified** testers, includes security reviews, breach assessments, audits, and CIS Benchmark assessments, ensuring your cloud infrastructure is secure against threats. Each tailored assessment provides expert analysis and actionable insights for effective vulnerability remediation.

In the digital age, cloud environments are prime targets for cyber-attacks, making assessments essential. Our services ensure compliance with industry standards and help uncover misconfigurations and evaluate the effectiveness of your security measures. This proactive approach reduces the risk of security breaches, enhances cloud resilience, and continuously improves defences against emerging threats.

Choosing **Bytes** allows you to leverage the expertise of experienced testers for thorough cloud environment assessments. Our detailed reports provide clear, actionable recommendations to help prioritise and address security issues effectively.

With a proven track record across industries, Bytes is a trusted partner for robust cloud infrastructure security and regulatory compliance.

Find out more about how Bytes can help you with our **Cloud Testing Services** by contacting us today.

Service Benefits

Comprehensive Security Assessment:
Our service examines your cloud environment, conducting security reviews, breach assessments, security audits, and CIS Benchmark assessments, using industry-standard tools to identify vulnerabilities.

Expert Analysis and Insights:
CREST-certified testers with extensive experience deliver detailed, actionable recommendations tailored to your specific needs.

Proactive Defence:
We identify hidden vulnerabilities and misconfigurations before they can be exploited. Regular assessments ensure compliance with industry standards and regulations.

Enhanced Security Posture:
Our evaluations of current security measures help you make informed decisions about future cybersecurity investments.

What These Services Cover

✓ **Initial Consultation:**
We start by understanding your cloud environment, security concerns, and testing goals.

✓ **In-depth Assessment:**
Our team identifies potential weaknesses and misconfigurations within your cloud infrastructure.

✓ **Comprehensive Reporting:**
We provide detailed findings, including risk levels, affected components, and actionable remediation steps, with prioritised recommendations to address the most critical issues first.

✓ **Continuous Improvement:**
We highlight effective security measures and identify gaps to ensure compliance with regulatory requirements and internal security policies.

✓ **Holistic Coverage:**
We thoroughly examine cloud security policies, configurations, and controls, performing security audits to verify compliance and adherence to best practices.

Chargable Engagement

Back to contents

A Leading Approach to Strategy Optimisation

CIS Gap Analysis

BYTES

The Center for Internet Security (CIS) Top 18 Critical Security Controls is a prioritised set of best practices created to stop the most pervasive and dangerous threats of today. Developed by leading security experts from around the world, the set is refined and validated every year.

While there is no silver bullet for security, organisations can significantly reduce their risk of compromise by implementing the CIS top 18 critical security controls, as they move from a compliance-driven approach to a risk management one.

Bytes are here to help you along that journey, starting with **a free-of-charge analysis** of how your current security provision aligns to the CIS Top 18 Controls.

Bytes CIS Gap Analysis Session gives businesses a Security Posture Gap Analysis based on the CIS Top 18 Controls. Those 18 security best practices are most likely to have a material impact on your business' ability in preventing breaches and reducing risk.

An expert analysis of security solution details by our engineers will provide tangible recommendations on improving/refining your security provision to maximise risk-reduction and compliance while keeping expenditure under control.

We have created this engagement to better work with our customers in **building a first-class cyber security strategy** which complies to established best practices.

Key Features & Benefits

✓ **Simplicity:**
No tools or scripts

✓ **Bespoke:**
Tailored to each individual company

✓ **Detailed:**
Encompasses all areas of security best practice

✓ **Industry Recognised:**
Internationally approved, continually updated framework

✓ **Zero Cost:**
Our expert-led service is completely free

✓ **Independent advice:**
Vendor agnostic approach focused on best practices

What To Expect?

The CIS Gap Analysis is delivered through the following stages:

✓ **Discovery:**
We collect and collate information on your current security solutions, processes and procedures.

✓ **Analysis:**
We compare your current security provision across multiple areas to the top 18 CIS Controls.

✓ **Consultation:**
We deliver a session outlining the results, identifying key focus areas & outlining improvement recommendations.

✓ **Reporting:**
We provide a detailed report with RAG Matrix, tangible next steps, improvement areas & impact of gap analysis.

Chargable Engagement

Back to contents

Empowering Swift and Secure Digital Investigations

Digital Forensic & Incident Response Management

Bytes offers comprehensive Digital Forensic and Incident Response Management services to protect and remediate your organisation against cyber threats. Our services encompass both proactive and reactive measures to ensure your security posture is resilient and prepared for any incident.

Bytes' Digital Forensic and Incident Response Management services provide a holistic approach to cyber security, combining proactive preparedness with reactive expertise. Our services help you stay ahead of threats, respond effectively to incidents, and strengthen your overall security posture.

By partnering with **Bytes**, you gain access to a team of experienced professionals dedicated to safeguarding your organisation from cyber threats. Our tailored solutions and continuous support ensure your business remains resilient and secure in an ever-evolving threat landscape.

Find out more about how Bytes can help you with our **Digital Forensic & Incident Response Management** by contacting us today.

Proactive Services

Our proactive services are designed to prepare your organisation for potential cyber incidents, ensuring swift and effective responses when needed.

These services include:

✓ **Incident Response Planning & Reviewing:**
Develop and refine your incident response plans to ensure they are robust and effective. We work with you to create detailed, actionable plans tailored to your organisation's unique environment and risk profile.

✓ **Incident Response Retainer Services:**
Establish a partnership with Bytes for prioritised, rapid response support in the event of a cyber incident. Our retainer services ensure you have immediate access to our experts when time is critical.

✓ **Readiness Assessments:**
Simulate real-world incident scenarios to test and improve your incident response capabilities. These exercises help your team understand their roles, identify gaps, and enhance coordination during an actual incident.

Reactive Services

Our reactive services provide immediate support and remediation to minimise the impact of security breaches and restore normal operations as quickly as possible.

These services include:

✓ **24/7 Incident Response:**
Our team of experts are available around the clock to respond to cyber incidents, providing rapid containment, eradication, and recovery efforts to minimise damage and downtime.

✓ **Compromise Assessments:**
Conduct thorough investigations to determine if your systems have been compromised. Our assessments identify indicators of compromise, assess the extent of the breach, and provide detailed remediation steps to eliminate threats and prevent future incidents.

Chargable Engagement

Back to contents

Your proactive shield against cyber threats

Hacker’s Health Check

BYTES

Bytes Hacker’s Health Check service offers a tailored engagement to enhance a company’s cybersecurity posture by simulating an external hacker’s perspective.

This service conducts external reconnaissance to pinpoint vulnerabilities and exposures that could make your organisation an attractive target for cyber threats. Without performing active testing, we assess publicly accessible information and analyse security measures from an outsider’s viewpoint.

By adopting the mindset of a hacker, we identify weak spots that could be exploited, facilitating targeted remediation efforts. This evaluation employs a professional scoring system, providing you with a Hacker’s Health Check score, indicating your risk level and specific rating.

Our service thoroughly examines your digital footprint, external assets, and dark web exposure, providing actionable insights from **CREST-certified** experts.

This comprehensive assessment ensures your systems are robust against potential attacks, safeguarding your operations and enhancing your security posture.

We uncover hidden vulnerabilities, ensure compliance with industry standards and regulations, and evaluate current security measures to guide future cybersecurity investments. Choosing **Bytes** means leveraging experienced professionals in cybersecurity assessments.

Our detailed reports highlight effective security measures, identify gaps, and provide prioritised recommendations to address the most critical issues. With a proven track record across various industries, **Bytes** is your trusted partner in fortifying your cybersecurity defences and ensuring robust protection for your organisation.

Find out more about how Bytes can help you with our **Hacker’s Health Check** by contacting us today.

Key Objectives

- ✓ Conduct external reconnaissance to gather information about your digital footprint.
- ✓ Identify vulnerabilities and exposures in your external-facing assets.
- ✓ Pinpoint potential entry points into your systems and data.
- ✓ Analyse potential threats and prioritise vulnerabilities based on impact and likelihood of exploitation.
- ✓ Deliver a report outlining the threat landscape and hacker’s quick wins.
- ✓ Provide actionable insights and guidance to strengthen cybersecurity defences.

Service Benefits

Proactive Detection: Identify security gaps and vulnerabilities before exploitation.

Enhanced Security Posture: Strengthen defences and resilience against threats.

Cost Savings: Avoid financial losses from security breaches.

Reputation Protection: Safeguard your organisation’s reputation against cyber incidents.

Peace of Mind: Gain confidence in your ability to withstand cyber threats and attacks.

Chargable Engagement

Back to contents

Infrastructure Penetration Testing & Vulnerability Assessment Services

BYTES

In today's rapidly evolving threat landscape, your IT infrastructure is constantly at risk from cyber-attacks.

Bytes' services are meticulously designed to identify and mitigate security vulnerabilities across your entire IT environment. By adopting a comprehensive approach, we ensure your systems are robust against potential attacks, providing peace of mind and a secure operational environment.

Our holistic security evaluations cover both external networks and internal systems. **CREST-certified** testers use industrystandard tools and techniques to conduct thorough vulnerability assessments and simulate real-world attacks, identifying potential weaknesses and entry points.

Each assessment is tailored to meet your specific requirements, from comprehensive evaluation to targeted testing on critical systems.

Regular infrastructure penetration testing, and vulnerability assessments are essential for staying ahead of emerging threats.

Find out more about how Bytes can help you with our **Infrastructure Penetration Testing & Vulnerability Assessment Services** by contacting us today.

Our Proactive Approach

✓ **Uncovers:** Hidden vulnerabilities, ensures compliance with industry standards, and maintains customer trust.

✓ **Detailed Analysis:** Performed by CREST-certified professionals, identify critical and low-level vulnerabilities and provide clear, actionable recommendations.

✓ **Evaluate:** Current security measures and highlighting areas for improvement, to help you make informed cyber security investments, significantly reducing the risk of security incidents and strengthening your infrastructure's security posture.

Why Choose Bytes?

✓ **Certified Expertise:** Our team of CREST-certified testers brings extensive experience and proven success across various industries.

✓ **Thorough Coverage:** We ensure all aspects of your infrastructure are thoroughly examined, leaving no vulnerabilities overlooked.

✓ **Trusted Partner:** With a track record of successful engagements, Bytes is a reliable partner in enhancing your cybersecurity defences.

✓ **Actionable Insights:** We provide detailed reports with clear, prioritised recommendations to effectively address security issues.

Chargable Engagement

Identify & Mitigate Security Vulnerabilities

Posture Control Testing Services

BYTES

In today's interconnected world, network infrastructure is a primary target for cyber-attacks, making posture control testing crucial.

Our services identify hidden vulnerabilities before attackers can exploit them, ensures compliance with industry standards, and maintains customer trust. Regular testing reduces the risk of costly security breaches and enhances your network's resilience against emerging threats.

Bytes' Posture Control Testing Services identify and mitigate security vulnerabilities in your network infrastructure, ensuring firewalls, Wi-Fi, servers, workstations, segmentation, and IoT devices are secure against potential threats.

Our **CREST-certified** testers provide expert analysis and actionable insights, customising our testing to meet your specific requirements, from detailed firewall assessments to comprehensive segmentation testing.

We optimise settings, implement advanced security measures, and ensure data integrity and confidentiality.

Our tailored engagement can isolate critical assets, limit breach impact, and ensure devices are securely configured, enhancing overall IT security and compliance with industry standards.

Core Testing Areas

Firewall Configuration Review:
Thorough examination of your firewall configurations, rules, and policies to ensure they meet industry best practices and effectively protect your network.

Server and Workstation Configuration Reviews:
Assess security configurations of systems and applications, ensuring they are hardened against potential attacks.

Wi-Fi Testing:
Evaluate the security of your wireless networks, including encryption, authentication, and access controls.

Segmentation Testing:
Assess the effectiveness of your network segmentation and VLAN configurations to prevent unauthorised access and lateral movement.

IoT Testing:
Examine the security of your connected devices, identifying vulnerabilities in their configurations, communications, and data handling.

Our Services include Configuration Review for

- ✓ Firewalls
- ✓ WiFi
- ✓ Servers
- ✓ Workstation Security
- ✓ Network Segmentation
- ✓ IoT Device Management

Find out more about how Bytes can help you with our **Posture Control Testing Services** by contacting us today.

Back to contents

Proactive Protection, Professional Precision

Red Team Services

BYTES

Bytes' Red Team Services simulate real-world attacks to test your organisation's defences against Advanced Persistent Threats (APTs).

Our approach ensures robust security, providing strategic insights to fortify defences. **CREST-certified experts** deliver cutting-edge analysis and actionable insights, customising engagements to meet specific needs, from insider threats to physical security assessments.

In today's **complex threat landscape**, Red Team services are essential for uncovering weaknesses traditional assessments might miss, ensuring preparedness for sophisticated attacks.

Bytes are here to help maintain compliance with industry standards, customer trust, and legal requirements, while **reducing the risk of costly breaches** and **improving resilience and incident response effectiveness.**

Find out more about how Bytes can help you with our **Red Team Services** by contacting us today.

Key Steps

Overview

Start with a consultation to understand your security concerns and objectives.

Evaluate

- Develop a tailored attack plan using advanced techniques such as social engineering, physical security assessments, and technical exploitation.
- To identify vulnerabilities and test your detection and response capabilities.

Follow Up

Post-engagement we provide a detailed report with findings, risk levels, and remediation steps, along with continuous support to enhance your security posture.

What These Services Cover

✓ **Insider Threat Assessments:**

- Evaluaties the risks posed by malicious or compromised insiders, including scenariobased testing of insider threats.
- Simulates scenarios where attackers gain access to stolen laptops, smartphones, or other devices to assess data and corporate resources.

✓ **Hackers Health Check:**

- Provides a realistic evaluation of your security posture by simulating an external hacker's perspective.
- This proactive approach helps you identify and address weaknesses before they can be exploited, reducing the risk of costly security breaches.

✓ **Phishing and Vishing:** Conducts targeted phishing (email) and vishing (voice) campaigns to evaluate employee awareness and response to social engineering attacks.

✓ **Physical Security Assessments:** Assessing physical security controls through attempted unauthorised access to facilities and sensitive areas.

✓ **Open-Source Intelligence (OSINT):** Gathering publicly available information to identify potential vulnerabilities and exploitation opportunities.

✓ **Advanced Persistent Threat (APT) Simulations:** Emulating the tactics of sophisticated threat actors to test your defences against long-term, targeted attacks.

FOC
Engagement

Back to contents

Reimagine Your Cyber Security & Embrace Zero Trust

Zero Trust Market Overview

BYTES

Introducing **Zero Trust**, a security model that pro – actively adapts to the complexity of the modern working world by embracing the mobile workforce, and protecting people, devices, apps, and data wherever they're located.

Zero Trust is not a product, but a methodology of integrating multiple security tools and sources of information to enhance the efficiency and efficacy of your security investments. The result of this will be that your security infrastructure effectively becomes more than the sum of its parts. Through automation, integration, visibility, and remediation you will be able to free up valuable time for your security team to focus on priority tasks.

In addition, by following the three core principles of **Zero Trust**, you will be able to better strategise and utilise your available resource in such a way that maximises your ability to mitigate risk.

Bytes are here to help you navigate a complex range of technologies, frameworks, and best practices to ensure you optimise your security posture, making use of existing investments, as well as advising on new areas to consider exploring.

Receive Guidance on Zero Trust Foundations:

Never Trust, Always Verify

Assume a Breach

Apply Least Privileged Access

What To Expect

During this engagement **Bytes** security experts will guide you through core zero trust challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

- ✓ **1:1 Interactive Session**
- ✓ **Expert Advice and Guidance**
- ✓ **Can support multiple stakeholders**
- ✓ **Sessions run remotely or in person**
- ✓ **Experience across entire Zero Trust Spectrum**

Useful Zero Trust Resources

- ✓ Zero Trust Content Hub
- ✓ Zero Trust 3 Minute Explainer Video
- ✓ Meet the Zero Trust Team
- ✓ Bytes CTO on Zero Trust

Key Steps

1

Overview:

- ✓ What is Zero Trust
- ✓ Core Principles
- ✓ Core Technologies

2

Evaluate:

- ✓ Knowledge transfer
- ✓ Analyse and discover gaps
- ✓ Consider vendors and offerings

3

Integrate:

- ✓ Enhance your Zero Trust
- ✓ Complementing technologies
- ✓ True integrations

Make Sustainable Decisions At The Right Time

Cisco Lifecycle Review

BYTES

The assessment will consist of a full review of previous **Cisco** spend followed by a presentation covering all feedback, recommendations, and findings.

This session can also cover the latest network trends and threats, suggestions for improvements on energy consumption, and the ultimate delivery of your business objectives.

This process will allow you to have a plan in place to deal with managing your network over the long term and will give you visibility of the age, support status and refresh cycle of your network.

Our Methodology

By working with **Bytes** to carry out this assessment, our team will get to know your current estate and what it is you are trying to achieve and will then highlight any security vulnerabilities, analyse potential energy savings, including PoE and then also provide feedback on the lifecycle status of your current network components.

The Assessment Will Deal With All Networking Matters Across Your Business & Will Cover The Following:

- ✓ Cisco Letter of Authority
- ✓ Install Base Report
- ✓ Analysis of Potential PoE Energy Savings
- ✓ End of Life/End of Sale Items
- ✓ End of Support/Co-termination
- ✓ Security Vulnerabilities
- ✓ Upgrade and Trade in Recommendations
- ✓ Architectural Recommendations
- ✓ Sustainable Recycling Options

The Assessment is Delivered in 5 Phases:

1. Discover:

- Gather as much information as possible
- Conduct both a technical and business review

2. Analysis:

- Analyse against lifecycle milestones and associated support contracts

3. Review:

- Analysis of the data carried out
- Architecture mapping exercise
- Create a set of prioritised recommendations

4. Outcome:

- Roadmap against architectural objectives

5. Report:

- Provided based on risk, cost, and strategy
- Detailed recommendations against compliance, energy, environmental, and security policies

FOC
Engagement

Back to contents

Mapping Network Excellence

Network Maturity Assessment

BYTES

Bytes can provide you with our complimentary Network Maturity Assessment for your organisation to profile capabilities in unlocking your network's potential, to identify business requirements whilst mitigating associated risks.

At the end of this assessment, we will provide you a summary of measures/countermeasures, as well as our recommendations.

Discover the transformative potential of Bytes Networking solutions for your organisation with our quick and accurate self-assessment framework.

Participating in this comprehensive evaluation not only confirms your strengths but also surfaces and qualifies any gaps or weaknesses, providing you with tailored recommendations to effectively address these challenges.

Optimise your network's efficiency and security by engaging with our self-assessment today and unlock the full potential of Bytes Networking solutions tailored to meet your unique needs.

The Result - Insight into Your Networks:

✓ **Security & Compliance:** Threat Protection, Data Protection, Secure Access & Compliance Management

✓ **Integration & Automation:** APIs & Interoperability, Workflow Automation, Customisation, Reporting & Analytic

✓ **Performance & Scalability:** High Availability, Scalability, Load Balancing & Bandwidth Management

✓ **Cloud Management:** Centralised Management, Visibility & Monitoring, Configuration & Deployment, Software Updates & Maintenance

✓ **Network Infrastructure:** Robust Connectivity, Wireless Solutions, Switching & Routing, Network Optimisation

Key Steps

Questions:

- Answer the questions on the survey provided by your Account Manager.

Overview:

- Allow Bytes 2 working days to review the content
- Your measures/ countermeasures will be drawn up as well as suggestions.

Follow Up:

- Attend a 45-minute workshop meeting
- Review the report with one of our Networking Specialists
- Provide you with feedback

What to Expect

During this assessment Bytes networking experts will guide you through the networking challenges & how best to solve them with a vendor agnostic approach, ensuring the best fit for your organisation.

- **1:1 Interactive Session**
- **Expert Advice and Guidance**
- **Can support multiple stakeholders**
- **Sessions run remotely or in person**
- **Experience across entire**
- **Networking spectrum**

Network Maturity Assessment Survery

Funded Engagement

Back to contents

Elevating Cloud Protection

Microsoft Cloud Security Review

Microsoft BYTES

The Cloud Security Assessment gives you an analysis of your organisation's security posture, evaluating vulnerabilities, identity, and compliance risks with remediation recommendations.

Best for when you need to...

- Increase your knowledge around vulnerabilities to cyber attack & potential business risks
- Align data compliance policies to industry standards
- Integrate identity management requirements into standard business processes

Global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015[1]

Migrate confidently with expert help along the way

Our experts will guide you through our detailed four-phased approach, from identifying your business goals to implementing specific action items.

The Four Phases

Planning: Identify business goals and objectives

Data Collection: Provide a clear picture of the current data estate

Analysis: Optimise investments with data and infrastructure analysis

Action: Implement a strategic plan tailored to each cloud journey

Outcomes for Your Business

Empower your organisation to make decisions backed by data and guided by experts

- ✓ An understanding of your organisation's threat landscape to improve threat surface management
- ✓ A roadmap with clear visibility to progressive improvements for compliance adherence
- ✓ Best practices to integrate identity management requirements into standard business processes

Find out more about how Bytes can help you with Microsoft's **Cloud Security Assessment** by contacting us today.

Funded
Engagement

Back to contents

Defend at Machine Speed and Scale

Microsoft Copilot for Security

Microsoft BYTES

Security teams fight an asymmetric battle against **well – resourced, organised, and sophisticated attackers**. To protect their organisations, security practitioners must respond to threats that are often hidden among noise. Compounding this challenge is a global shortage of skilled security professionals.

Copilot for Security is the first security product to enable security analysts to move at the speed and scale of AI. It deploys **skills, threat intelligence, and unparalleled contextual awareness** to help security teams navigate security operations with speed and confidence. For the first time in the history of security operations, organisations do not require decades of experience, advanced knowledge of query languages, and skills like malware reverse engineering to perform their most critical SOC use cases.

The Copilot for Security Advantage

Copilot for Security combines the most advanced large language model (LLM) with a security-specific model from Microsoft. This security-specific model in turn incorporates a growing set of security skills and is informed by Microsoft's unique global threat intelligence and more than 65 trillion daily signals.

Copilot for Security also delivers an enterprise-grade security and privacy-compliant experience as it runs on Azure's hyperscale infrastructure.

Turn Questions Into Action

✓ **Security Operations:** Manage vulnerabilities and emerging cyberthreats, start a guided investigation, and speed your work with script analysis and query assistance.

✓ **Device Management:** Generate policies and simulate outcomes, gather device information for forensics, and configure devices with best practices from similar deployments.

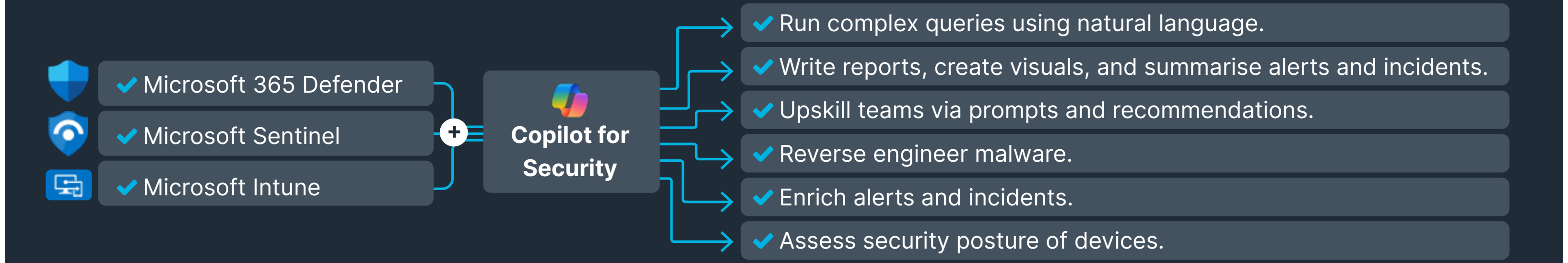
✓ **Identity Management:** Discover overprivileged access, create access reviews for incidents, generate and describe access policies, and evaluate licensing across solutions.

✓ **Data Protection & Compliance:** Identify data impacted by incidents, create a summary of data and user risks, analyze documents, and surface risks of collusion, fraud, and sabotage.

✓ **Cloud Security:** Discover cyberattack paths impacting workloads and summarize common cloud vulnerabilities and exposures.

Copilot for Security takes Microsoft Security to the Next Level

Today, Copilot for Security integrates with Defender, Sentinel, and Intune products. It does not replace any of these products, but enhances them with a unique set of use cases and capabilities that make security tasks drastically more accessible. As a result, analysts can perform tasks that were previously reserved only for the most experienced team members.



✓ Microsoft 365 Defender
✓ Microsoft Sentinel
✓ Microsoft Intune

Copilot for Security

✓ Run complex queries using natural language.
✓ Write reports, create visuals, and summarise alerts and incidents.
✓ Upskill teams via prompts and recommendations.
✓ Reverse engineer malware.
✓ Enrich alerts and incidents.
✓ Assess security posture of devices.

Funded Engagement

Back to contents

Identify Data Security Risks In Your Organisational Data

Microsoft Data Security Workshop

Microsoft BYTES

Bytes provide world class expertise. From security, storage and virtualisation to licensing, digital transformation and managed services. Our breadth of insight & experience has helped hundreds of the worlds best known brands and will do the same for your business. The added value from our passionate, customer focused, service driven people will help you achieve more.

The **Data Security Check** leverages Microsoft Purview tools and services in an automated process to:

- ✓ **Discover** data that is stored in the Microsoft 365 Cloud and analyse it for the presence of artifacts that may impose data security risks to the organisation.
- ✓ **Analyse** user behaviour for events that impose a risk to the customers organisation. These vulnerabilities range from the loss of intellectual property to workplace harassment and more.

The Data Security Check is structured around typical Microsoft 365 services and their associated data repositories that organisations use. At its core, the Data Security Check analyses user behaviour and scans data repositories related to email, collaboration, and document storage.

What To Expect

- ✓ A Security Check report that includes findings and insights from the automated discovery process.
- ✓ A list of recommendations and actionable next steps that will help mitigate the identified risks.
- ✓ Clear look into Microsoft's approach to data security and mitigating and controlling insider risks.
- ✓ Optional Compliance Manager Tenant Assessment report with suggestions and top key improvement actions.
- ✓ Set of long term recommendations on your compliance strategy, with key initiatives and tactical next steps.

What's Included?

By participating in this engagement, our experts will work with you to:

Pre-Engagement Meeting:
Document your objectives and strategy around data security, privacy and compliance.

Data Security Check:
Show how to detect, investigate and take action on Data security and privacy risks.

Microsoft Purview Portfolio Overview:
Demonstrate ways to accelerate your compliance journey with the latest Microsoft technologies.

Recommendations & Next Steps:
Provide actionable next steps based on your needs and objectives.

Optional modules can be added to extend the Data Security Check to include on premises data repositories, Windows 10/11 endpoints and more. All activities share a common framework that will allow you to understand the risks that exist in your organisation and develop a roadmap to mitigate and protect your company's information.

Funded Engagement

Back to contents

Supporting Resiliency:

Microsoft Secure Infrastructure Review

BYTES

Customers have had to move quickly to respond to new demands and new pressures over the past two months.

Customers are pivoting to remote work and putting the safety of their employees, customers, and communities first.

Implementing technology and revised ways of working whilst moving at pace is tough. Combine this with maintaining security and it's easy to see how vigilance could slip.

The Secure Infrastructure Assessment will provide practical quick wins to help ensure you maintain control.

Microsoft

How It Works

✓ The Secure Infrastructure Assessment utilises the **Cyber Security Assessment Tool (CSAT)** for collecting and analysing data.

✓ Office 365, SharePoint and Fileshares are included in the scope. All endpoints, fileservers, configurations, security rights and roles are scanned and analysed.

✓ CSAT collects information about accounts, firewall settings, installed applications, the OS/Service Pack and Fileshares. CSAT also exports users and groups from Active Directory and Azure AD.

✓ Based on these scans the Secure Infrastructure Assessment surfaces potential cyber threats and vulnerabilities.

✓ The resulting reports and workbook will provide practical recommendations and quick wins plus a high-level roadmap to help you regain vigilance and control.

Deliverables

✓ **Action Plan to improve Cyber Security**

✓ **Urgent priority actions & quick wins**

✓ **Technical Data and Analysis**

- Endpoint details & risks
- Inventory & version data
- Suspicious applications
- Admin privileges
- Bad password attempts & suspicious logons
- Data protection: Potential PII data
- Externally shared Sharepoint data
- Microsoft Secure Score End of Life products

✓ **Overall CIS (Center for Internet Security) Company Rating**

- Mapped to Basic, Foundational & Organisational controls

Funded Engagement

Back to contents

An accelerated session to support with your planning of Sentinel and to get you up and running!

Microsoft Sentinel Activation Workshop

BYTES

Microsoft Sentinel is a scalable, cloud native Security Information and Event Management (SIEM) platform.

Microsoft Sentinel provides enterprises with the **ability to ingest data at cloud scale and utilise this to detect threats,** this, coupled with the analytics and threat intelligence that Microsoft provides allows for rapid detection and response for the threats that would previously go undetected.

Bytes believe that customers should be maturing their incident response capabilities by utilising Sentinel, especially in Microsoft Cloud Environments where there are several services enabled. This will allow for a single point to view and track and assess any suspicious activity within the Microsoft Cloud stack.

To facilitate this belief, **Bytes** are offering a session that will provide a planning & activation exercise to ensure that core considerations are evaluated and planned accordingly.

Additionally, we can investigate the various options around utilising your M365 licensing for greater visibility and explore areas such as Security Co-Pilot for future AI enhancement. Following this, **Bytes** will support you with a basic implementation of Microsoft Sentinel for your Microsoft Cloud Environment.

Microsoft

This acts as a springboard into using Microsoft Sentinel to begin analysing and detecting threats within your cloud environment. The session is a 1-hour session, **free of charge to Bytes Customers,** with the result being that your Microsoft Sentinel instance is configured to your Microsoft Cloud Services to begin receiving insights and alerts on possible threats.

What to Expect

- ✓ Data Collection
- ✓ Detection of Threats
- ✓ Investigation of Incidents
- ✓ Respond and Contain

The Workshop Focuses on 6 Key Points:

Requirements Gathering: Get an idea of the business and technical requirements and expectations you have of Sentinel.

Sentinel Provisioning: We will work with you to implement an instance of Sentinel into your Azure Subscription.

Planning and Considerations: Get an understanding of your current environment and provide guidance on how best to deploy Sentinel in a structured manner.

Estimate Pricing: Look to get a rough idea of what log sources you will need to ingest into Sentinel, combined with your assets we can provide an estimated price of Sentinel.

Connecting M365 Data Sources: Walk you through the setup and configuration of Sentinel to begin collecting logs and data from your enabled Microsoft Cloud Services.

Next Steps: Assess and recommend next steps, such as exploring options around further professional services and managed services to support you with enhancing your response capability.

Funded Engagement

Back to contents

Gain a bird's eye view across your enterprise with SIEM for a modern world.

Microsoft Sentinel Workshop

BYTES

Bytes provide world class expertise. From security, storage and virtualisation to licensing, digital transformation and managed services. Our breadth of insight & experience has helped hundreds of the worlds best known brands and will do the same for your business. The added value from our passionate, customer focused, service driven people will help you achieve more.

Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Get an overview of Microsoft Sentinel along with insights on active threats to your Microsoft 365 cloud and on premises environments with a Microsoft Sentinel Engagement. Every organisation is different, so this engagement can be customised to fit your environment and goals.

We can provide either of two scenarios:

Remote monitoring:

If your organisation doesn't have its own security operations center (SOC) or if you want to offload some monitoring tasks, we will demonstrate how Bytes can perform remote monitoring and threat hunting for you.

Joint threat exploration:

If your organisation is interested in learning how to integrate Microsoft Sentinel in your existing SOC by replacing or augmenting an existing SIEM, we will work with your SecOps team and provide additional readiness to bring them up to speed.

What We Will Do

*optional component

- ✓ **Analyse** your requirements and priorities for a SIEM deployment.
- ✓ **Define** scope & deploy Microsoft Sentinel in your production environment.
- ✓ **Remote** monitoring* of Microsoft Sentinel incidents and proactive threat hunting to discover attack indicators.
- ✓ **Explore** threats and demonstrate how to automate responses and perform threat hunting.
- ✓ **Recommend** next steps on how to proceed with a production implementation of Microsoft Sentinel.

What's Included?

By participating in this engagement, our experts will work with you to:

Discover threats to your Microsoft 365 cloud and on premises environments across email, identity and data.

Understand how to mitigate threats by showing how Microsoft 365 and Azure security products can help mitigate and protect against threats that are found.

Plan next steps and provide information to build a business case for a production deployment of Microsoft Sentinel including a technical deployment roadmap.

In addition, depending on the selected scenario, you will also:

Experience the benefits of a managed SIEM with a true cloud native SIEM, managed and monitored by our cybersecurity experts. (Remote Monitoring scenario)

Receive hands on experience, learn how to discover and analyse threats using Microsoft Sentinel and how to automate your Security Operations to make it more effective. (Joint Threat Exploration scenario)

Funded Engagement

Back to contents

Learn how to put next generation Microsoft Security tools to work for you.

Microsoft Threat Protection Workshop

Microsoft BYTES

Bytes provide world class expertise. From security, storage and virtualisation to licensing, digital transformation and managed services. Our breadth of insight & experience has helped hundreds of the worlds best known brands and will do the same for your business. The added value from our passionate, customer focused, service driven people will help you achieve more.

Do you know how many phishing attacks your organisation has received? If employees are using the right password protocol? Whether personal data is being exposed? In short, is your organization's cloud environment as secure as you think it is?

Improve your security posture with a Threat Protection Engagement.

Organisations today are managing a growing volume of data and alerts while dealing with tight budgets and vulnerable legacy systems. Get help achieving your broader security objectives and identify current and real threats by scheduling a Threat Protection Engagement.

We can help you develop a strategic plan customised for your organisation and based on the recommendations of Microsoft experts in security. You'll gain visibility into immediate threats across email, identity, and data, plus clarity and support on how to remediate vulnerabilities and upgrade your security posture for the long term.

Why You Should Attend

- ✓ Identify current, ongoing security threats and discover vulnerabilities in your environment.
- ✓ Walk away with actionable next steps based on your specific needs and objectives.
- ✓ Document your security strategy for the benefit of key stakeholders.
- ✓ Better understand how to accelerate your security journey using the latest Microsoft Security tools.

Who should attend?

The engagement is intended for security decision makers such as:

- **Chief Information Security Officer**
- **Chief Information Officer**
- **Chief Security Officer**
- **IT Security Architects**
- **IT Security Administrators**
- **IT Security Operations (Sec Ops)**

What To Expect?

We'll help you better understand how to prioritise and mitigate potential attacks, with:

Analysis of cybersecurity threats that are found targeting your organisation.

Actionable recommendations to help immediately mitigate the identified threats and discovered vulnerabilities.

Visibility into vulnerabilities to your Microsoft 365 cloud and on premises environments to better understand, prioritise and address vulnerabilities and misconfigurations across your organisation.

Long term recommendations from Microsoft experts about your security strategy, with key initiatives and tactical next steps.

Back to contents

Cyber Security Customer Engagements

Glossary

Market Review:
A market review provides a concise analysis of current market trends, performance and future outlook.

Gap Analysis:
A gap analysis identifies the differences between current performance and desired goals, highlighting areas for improvement.

Workshop:
A technology workshop is an interactive session where participants learn about and engage with new technologies through hands-on activities and discussions.

Service:
A service is an ongoing or one-time offering that fulfils a need or solves a problem for customers.

BYTES