Cyber Security

BACKGROUND

IT security is a top business priority; however, the way that organisations need to approach security has radically changed in recent years due to the evolution of the threat landscape. Traditional perimeter-based security methods are no longer effective as the widespread adoption of cloud services and mobile working has redefined the security perimeter. To overcome this challenge, organisations are embracing Zero Trust Networking, which adapts to the complexity of modern working and helps to protect people, devices and data wherever they are.

SECURITY MATURITY

Every organisation will be at a different level of security maturity, which can be influenced by existing technologies, security requirements and priorities. Achieving Zero Trust is not an overnight exercise and should be part of your wider digital transformation and cloud strategy. Most organisations will adopt a phased approach, tackling the most critical steps with the highest return first so that each phase reduces risk and elevates overall security strength.

OUR CYBER SECURITY SERVICES

Our cyber security services leverage Microsoft technologies to help organisations at any stage of their security journey assess, implement and manage an advanced cyber security strategy. We believe in giving practical expertise and support to ensure that our clients maximise the value from their technologies, reduce organisational risk and stay ahead of the rapidly-evolving threat landscape.

Our three phase approach:

21% of companies have already adopted Zero Trust

63% plan to adopt Zero Trust in the next 12 months

Source: IDG Explorer Survey, May 2019

ZERO TRUST OVERVIEW

Rather than the assumption that anything behind your security perimeter is safe, Zero Trust adopts the approach of "never trust, always verify". Any access request is challenged and verified before granting access, checking against four key criteria:

- **Identity** – who is attempting access and are they allowed?
- **Device** – what device is being used and what is its state?
- **Data** – what is being accessed?
- **Location** – where are they trying to access it from?

ASSESS

Threat Check Workshop or Zero Trust Security Assessment

- ✓ Identify active threats and vulnerabilities
- ✓ Outline risks, severity and impact
- ✓ Prioritise recommendations to mitigate risk and improve security posture

PROTECT

Security Technology Implementation

- ✓ Define and plan a phased security roadmap
- ✓ Implementation of security technologies to achieve zero trust
- ✓ Advise on an evolving security strategy and approach

MANAGE

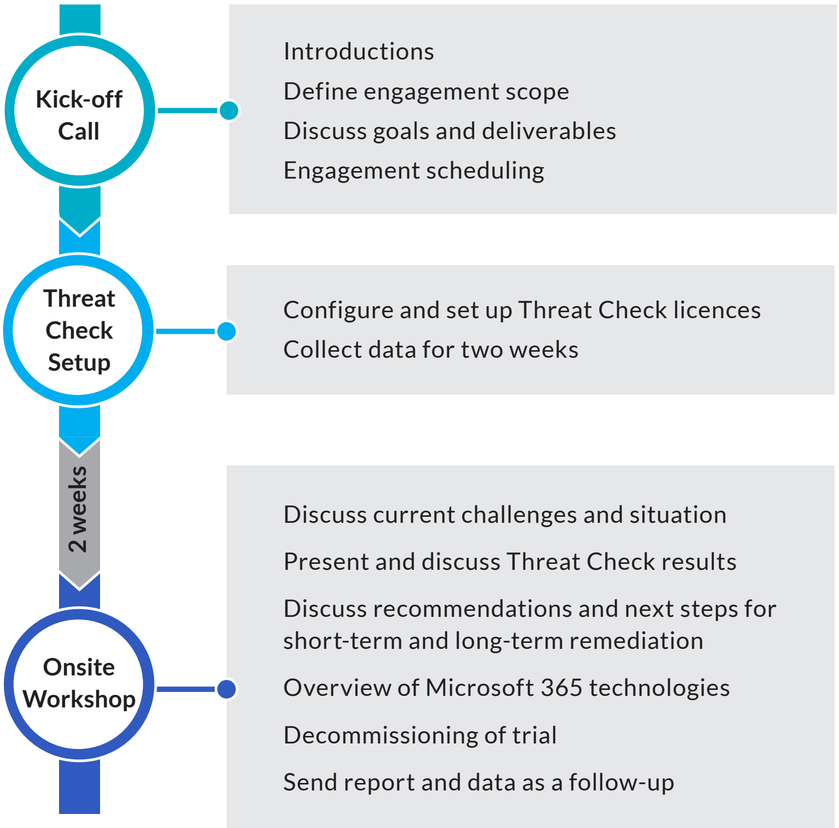
Managed SOC Service

- ✓ Active monitoring and detection of security events
- ✓ Forensic analysis into identified threats and remediation activities
- ✓ Service reports, recommendations and strategic guidance

Assess: Microsoft Threat Check Workshop

Our Microsoft Threat Check workshop provides a high-level overview of your security posture, using a Microsoft 365 E5 trial to scan your digital estate to identify active threats and vulnerabilities across email, identity and data. Results are gathered, analysed and presented via a report and on-site workshop to identify key threats and outline prioritised remediation steps.

ENGAGEMENT OVERVIEW



Kick-off Call:

Introductions

Define engagement scope

Discuss goals and deliverables

Engagement scheduling

Threat Check Setup:

Configure and set up Threat Check licences

Collect data for two weeks

Onsite Workshop:

Discuss current challenges and situation

Present and discuss Threat Check results

Discuss recommendations and next steps for short-term and long-term remediation

Overview of Microsoft 365 technologies

Decommissioning of trial

Send report and data as a follow-up

REVIEW YOUR WIDER SECURITY POSTURE

Our Zero Trust cyber security assessment includes the Threat Check assessment as well as a more in-depth review of you wider security situation - please see the next page for more details.

MICROSOFT 365 E5 TRIAL

The Threat Check assessment uses a Microsoft 365 E5 trial to scan and monitor your digital estate, detecting and highlighting active and potential threats.

This uses three key technologies within Microsoft 365:

Azure Active Directory – Detects user identity threats, such as compromised credentials and attempted sign-ins.

Microsoft Defender for Office 365 – Detects threats to email and data, such as malware and phishing attempts.

Microsoft Cloud App Security – Raises alerts on user or file behaviour anomalies in cloud apps leveraging their API connectors.

OPTIONAL INCLUSIONS

In addition, the following areas can be added to the Threat Check but would be discussed during the kick-off call as they require additional configuration or may impact end users:

Microsoft Defender for Identity – Provides visibility into on-premise alerts and detects vulnerabilities, such as plain text credentials.

Attack Simulator – Enables a controlled phishing attack simulator to be carried out to assess end user awareness and risk.

Shadow IT Discovery– Generates a cloud app discovery report, which reveals approved and unapproved cloud applications being used to store company data.

Assess: Zero Trust Security Assessment

Our cyber security assessment reviews your current cyber security posture against a Zero Trust model, reviewing your IT security maturity, identifying risks and vulnerabilities and providing prioritised risk mitigation recommendations to help you adopt an advanced, Zero Trust security model.

Through a combination of consultative reviews and our technical Threat Check assessment, we analyse your security posture, covering six foundational security areas: Identity, Devices, Applications, Infrastructure, Networks and Data.

SECURITY AREAS

Area	Description
Identities	Zero Trust begins with strong identity and access management. We assess how identities are managed, secured and authenticated.
Devices	Devices create a massive attack surface area; we will review how your endpoints are managed, monitored and secured – whether company-owned or personal devices (BYOD).
Applications	We focus on discovering shadow IT and reviewing application access, permissions, usage and monitoring – whether on-premise, hybrid or SaaS.
Network	Zero Trust moves away from a network perimeter focus towards intelligent access controls; however, network security must still not be overlooked. We review network controls to evaluate your network security in a Zero Trust model.
Infrastructure	Your infrastructure is a critical attack vector used to exploit vulnerabilities. We assess how your infrastructure is managed and secured, and measures for anomaly detection.
Data	Data should remain secure even if it leaves company apps, networks, infrastructure or devices. We evaluate your data security (such as labelling, encryption and classifications) to review your data protection measures.

APPROACH

We use non-intrusive security technology to scan your digital estate over two weeks, picking up active and potential threats and vulnerabilities to identify security weaknesses.

Alongside this, our security consultants will complete a comprehensive audit to review your cyber security.

BENEFITS

Holistic security view – Our assessment service provides a view of your security posture so that you gain a clear picture across your digital estate.

Detect live threats – The security toolset report will highlight any active security threats that could need to be immediately remediated.

Reduce risk – We help identify potential security vulnerabilities so that you can quickly mitigate these risks before an issue arises.

Clear security priorities – We identify clearly prioritised recommendations to aid security decision making and help you define your security roadmap to implement the most effective remediations first.

Speak to an expert – Rather than simply sending a report, one of our security consultants will come to your offices to present the findings and allow time for discussions and questions you may have.

ASSESSMENT SCOPE

Our cyber security assessment includes the following elements;

IDENTITY

- ✓ MFA
- ✓ Conditional Access
- ✓ Single-sign on (SSO)
- ✓ Password hygiene
- ✓ Legacy Authentication
- ✓ Identity Security Posture
- ✓ Phishing Attempts
- ✗ DMARC/DKIM/SPF

DEVICES

- ✓ Endpoint protection
- ✓ MDM, MAM & BYOD
- ✓ Web filtering
- ✓ Vulnerability management
- ✓ Patch management
- ✓ Endpoint encryption
- ✓ Endpoint detection & response (EDR)
- ✗ Hardware

APPLICATIONS

- ✓ Shadow IT discovery
- ✓ Abnormal behaviour monitoring
- ✓ OAuth app consent
- ✗ APIs
- ✗ Custom applications

NETWORK

- ✓ IDS/IPS
- ✓ Network traffic monitoring
- ✓ SIEM (log analytics)
- ✗ Firewall configuration and management
- ✗ Network segmentation

INFRASTRUCTURE

- ✓ Privileged Identity Management (PIM)
- ✓ Just in Time (JIT)
- ✓ Domain controllers
- ✓ Server encryption
- ✓ Infrastructure monitoring
- ✓ Event log monitoring
- ✓ Server patching
- ✓ Email security
- ✗ Server configuration

DATA

- ✓ Data classification
- ✓ Labelling policies
- ✓ Data encryption
- ✓ Data Loss Prevention (DLP) policies
- ✓ Ransomware protection
- ✗ File and folder permissions

ASSESSMENT DELIVERABLES

On completion of the audit and scanning, our security consultants will review the findings and present them within your report. This includes:

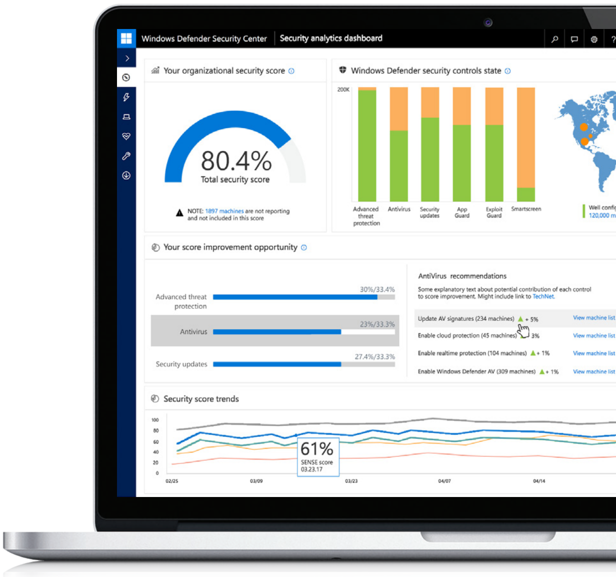
Overview: An overall view of your security posture and security maturity.

Risks and Threats: Receive a detailed breakdown of active and potential risks and vulnerabilities found across your digital estate. This will outline the threat, its severity and potential impact.

Dashboards: We will share the technical findings via dashboards, charts and reports to give you the detail into any weaknesses and risks.

Mitigations and Recommendations: We will outline the recommended mitigations and clearly prioritise the most effective remediations to make to aid your strategy and decision making.

Onsite workshop: We also come onsite where one of our security consultants will deliver the results and discuss the findings and recommendations with you.


Windows Defender Security Center
Security analytics dashboard
Your organizational security score
80.4%
Total security score
Windows Defender security controls state
200K
Advanced threat protection
Antivirus
Security updates
App Guard
Exploit Guard
Smartscreen
Your score improvement opportunity
Advanced threat protection
30%/33.4%
Antivirus
23%/33.3%
Security updates
27.4%/33.3%
AntiVirus recommendations
View machine list
Security score trends
100
80
60
40
20
0
02/25
03/09
03/23
04/07
04/14
61%
SENSE score
03.23.17

NOTE: 1897 machines are not reporting and not included in this score

Some explanatory text about potential contribution of each control to score improvement. Might include link to TechNet.

Update AV signatures (234 machines) + 5%

Enable cloud protection (45 machines) 3%

Enable realtime protection (104 machines) + 1%

Enable Windows Defender AV (309 machines) + 1%

Protect: Cyber Security Implementation

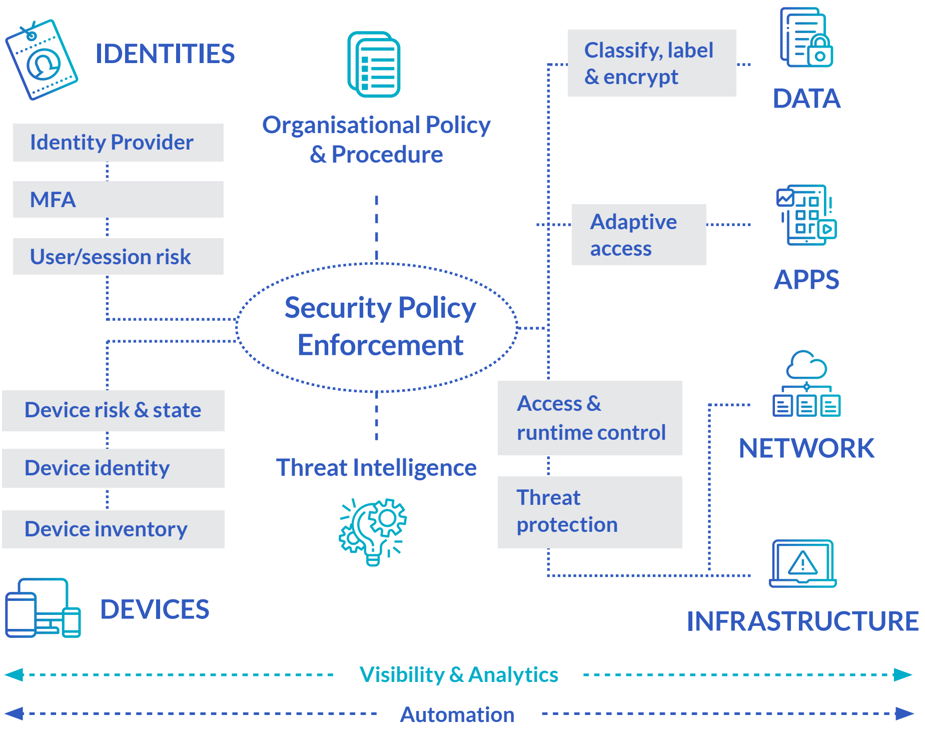
Our security implementation services help you implement a Zero Trust model that is underpinned by leading Microsoft security technologies. Following an assessment of your organisation's situation, risks and goals, we will follow our project methodology with clear communication and milestones to implement the technologies to secure and protect your data, people and organisation.

PHASED SECURITY APPROACH

While a Zero Trust model is most effective when implemented and integrated across your entire digital estate, most organisations will need to adopt a phased approach. As Zero Trust is designed for a cloud-first mobile-first environment, organisations may be held back by legacy systems.

For a successful transition, it is worth implementing a Zero Trust model as part of your wider digital transformation – adopting new technologies as legacy systems and existing environments are migrated to the cloud. By phasing the adoption, the transition can focus on prioritising the most effective and least challenging changes for maximum benefit to your security posture, whilst ensuring a smooth transition for your staff.

ZERO TRUST ARCHITECTURE



MICROSOFT 365

Microsoft is a leader in security technology and we recommend implementing Microsoft 365 to achieve Zero Trust.

Microsoft 365 includes a comprehensive and advanced suite of integrated security products, such as Microsoft Cloud App Security, Intune, Azure Information Protection and the Microsoft 365 Defender solutions. Using these products allow organisations to secure and protect their staff, devices and data with a modern Zero Trust approach.

WHY MICROSOFT 365?

- The biggest strength of Microsoft 365 is the **unparalleled scale** of its underlying platform: the Intelligent Security Graph. This uses machine learning and advanced AI to continually improve and learn from the trillions of signals that Microsoft receive daily.
- Microsoft's products work perfectly together, integrating and feeding data across all solutions. With **one integrated toolset**, you benefit from simplicity and reduced complexity for quicker detection.
- Using Microsoft 365 potentially removes many additional **third party costs**.
- Microsoft 365 not only provides the security tools, but offers **centralised management capabilities** so that changes in security and compliance can be quickly updated and immediately enforced.
- Ensures a **smooth user experience** for your staff so they are protected but productivity is not impacted.

SECURITY MATURITY ROADMAP

Every organisation's cyber security roadmap will be unique, but a 'typical' strategy with common milestones and products could look like:

TRADITIONAL

Traditional perimeter-based security model securing the internal network. Difficulty securing and managing devices and a lack of visibility over cloud services and data once it leaves the network.

Methods:

Network perimeter security model

Firewalls and IDS

Anti-virus/malware protection

Single factor authentication

MODERN

Moving towards dynamic security with a focus on data and identity protection (Multi-Factor Authentication, Conditional Access) to gate access and increased analytics into threats.

Products:

Azure Active Directory

Microsoft Defender for Identity

Microsoft Defender for Office 365

ADVANCED

Mobile devices are secured to enable BYOD and centralise management, cloud threat protection is in place and usage monitored. Analytics are being used to assess user behaviour and identify threats.

Products:

Intune - MDM & MAM

Microsoft Cloud App Security

Microsoft Defender for Endpoint

Web Filtering

OPTIMAL

Strong use of machine learning and automation with real-time threat detection and response. Data is self-protecting and there is zero trust across the entire network.

Products:

Azure Information Protection

Azure Sentinel

Threat Hunting

BUILDING THE RIGHT STRATEGY

All organisations will be at different stages of their security journey and have different priorities and challenges that will shape their strategy. We work closely with our clients to build the right strategy, forming the most appropriate phasing to meet your unique requirements.

The phasing of your roadmap would be determined by:

- Focusing on critical security changes to ensure **key baseline protection**
- Determining complexity of changes against your digital estate so low complexity and highest value changes are delivered first to **deliver value quickly**
- Reviewing any **business priorities** or requirements with timescales (such as compliance certifications)
- Assessing **current technologies** and any legacy infrastructure to determine any potential challenges
- Ensuring the **best use of licensing** by implementing technologies that you may already be paying for first
- Reviewing your **cloud migration strategy** and wider IT roadmap to ensure your security strategy aligns

GET CERTIFIED

We can also help you gain cyber security accreditations for compliance, such as:

- **Cyber Essentials**
- **Cyber Essentials Plus**
- **ISO27001**

Manage: Security Operations Centre

Security threats are becoming more advanced and sophisticated, and as a result companies are struggling to keep up with the rapid pace of change and complexity in cyber security. Our Security Operations Centre (SOC) combines best use of technology, mature ITIL-aligned processes and highly skilled security teams to give organisations access to a dedicated security team that would be uneconomical to maintain internally.

Our managed security service provides active monitoring and handling of security events identified using Microsoft 365 Defender and Microsoft Azure Sentinel. This enables us to rapidly detect and respond to threats, reducing your overall security risk and giving you greater peace of mind. We work in partnership to provide ongoing practical recommendations and monthly service reports to help your organisation stay ahead of evolving threats.

WHAT’S INCLUDED?

- **Alert monitoring and investigation** - Our security team will review network security alerts and triage, classify, prioritise and investigate the threat to determine whether further action is required
- **Forensic analysis** - Analysis of identified security incidents and report generation and distribution to outline key information, implications and guidance around discovered threats
- **Remediation and recovery** - We perform the necessary remediation activities for infrastructure support clients to remove the threat and carry out any mitigation actions
- **24/7 support** - 24/7 proactive monitoring
- **Monthly service reports** - Allowing us to monitor trends and insights as part of our ITIL problem management framework, which enables continuous service improvement
- **Security road-mapping** - We provide you with practical advice into security quick wins and long-term recommendations that can feed into your security strategy and roadmap
- **Monthly threat hunting activities** - Proactively searching for cyber threats to identify threats that evade security controls
- **Phishing simulation training** - Attack simulation using Microsoft Defender for Office 365 to conduct periodic phishing and password attacks in order to identify and train vulnerable employees

BENEFITS OF OUR MANAGED SOC

Cost-effective access to a security team that would be difficult to maintain in-house

Respond quickly and effectively to threats to protect your data, staff and organisation

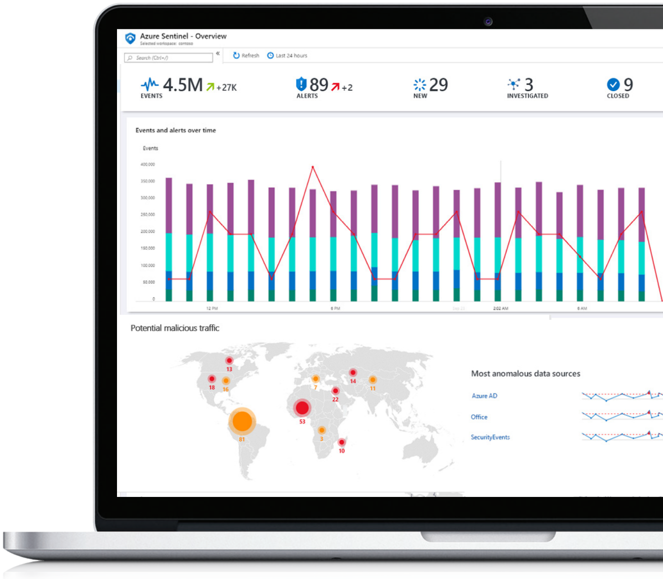
Fosters a **forward-thinking security strategy** through regular reporting and recommendations

Ensures security incidents are **thoroughly investigated** and mitigated for future protection

Established **ITIL-aligned Managed Service Provider** with advanced processes, technologies and industry standards (ISO 9001 & ISO 27001)

Focus on **maximising the value of your Microsoft investments** to ensure best use of technologies and licensing

Proactively reduces risk through threat hunting and training to stay ahead of evolving threats



About us

We are Microsoft cloud and security experts that help organisations adopt and benefit from cutting-edge Microsoft technologies.

Our Services:

- Cyber Security
- Modern Workplace
- Business Applications
- Hybrid IT & Cloud
- Managed Services
- Networking & Comms

Our aim is to help our clients gain the most value from their Microsoft investments through our transparent, honest approach and by utilising our technical expertise.

Microsoft Partner

Microsoft

Gold Cloud Productivity
Gold Collaboration and Content
Gold Cloud Platform
Gold Application Development
Gold Windows and Devices
Gold Enterprise Resource Planning
Gold Data Analytics
Gold ISV
Silver Cloud Customer Relationship Management
Silver Enterprise Mobility Management
Silver Security
Silver Small and Midmarket Cloud Solutions
Silver Datacenter

WHAT NEXT?

If you would like to find out more information about our cyber security services, or have any questions, please get in touch with our team today.

✉ hello@chorus.co ☎ 01275 398 900 www.chorus.co