INSIGHT'S CYBERSECURITY CAPABILITIES OVERVIEW

Insight

Introduction

Cybersecurity is more crucial than ever for businesses of all sizes as the frequency and sophistication of cyber threats increases. Cybersecurity breaches can result in devastating consequences, including financial losses, legal liabilities, damage to brand and loss of customer trust.

Protecting your business from cyber threats is not just a matter of compliance or good practice; it is essential for safeguarding your operations and ensuring business continuity.

Investing in robust cybersecurity measures is an investment in the future resilience and success of your business. By implementing effective cybersecurity strategies, you can mitigate risks, detect and respond to threats in a timely manner, and build a strong defence against cyber-attacks.

Cybersecurity is not just a necessity; it is a strategic imperative for businesses looking to thrive in a secure and resilient environment.

At Insight, we understand the need for a comprehensive approach to security.

Insight's approach to cybersecurity

Cybersecurity is complicated — demanding an all-hands-on-deck approach from your end users, security teams and tools. That is why we take a holistic approach to cybersecurity across both technology and integration domains delivered through repeatable methods and proven processes that yield successful results. Our experts will guide you from end-to-end, leading to improved efficiency, effectiveness, and strategic alignment.

Insight's holistic security model

Insight's approach to Cybersecurity

We have comprehensive technical skills in the five technology domain areas:

- Endpoints
- Applications
- Cloud
- Network, Datacentre and IOT
- Data centric

but as a leading solution integrator, we understand that technical excellence in these domains is not enough. Security needs to be addressed holistically, ensuring all areas of security are integrated and coordinated. We do this through the application of:

- Governance, Risk and Compliance
- Identity and Access
- Threat Detection and Response
- Human Factors

The gaps where the technology domains intersect are where extra value can be gained by helping enhance your overall security posture in a cost-efficient way.

We can help you:

- Improve Cybersecurity posture.
- Identify and mitigate risks.
- Reduce complexity through the minimising of overlapping technologies.
- Optimise security operations.
- Ensure security controls add value and improve return on spend.

The Technology Pillars

Endpoints

Gone are the days of a single device per user in a business, it's more than likely your employees are using multiple devices. Endpoints play a critical role in cybersecurity for organisations, serving as entry points for cyber threats and vulnerabilities. The challenges in securing endpoints have grown due to the proliferation of devices, remote work environments, and the increasing sophistication of cyber-attacks targeting endpoints. Typical common challenges include endpoint visibility, vulnerability management, data protection, and application control.

These devices need to be managed, their security posture monitored and updated, and active defences for blocking malware and exploits need to be deployed and maintained. Our endpoint security solutions focus on the process of securing endpoints such as laptops, desktops, servers, and mobile devices that are used to access company networks and data.

We can help you:

- Gain visibility into your endpoint estate, at a device and application level.
- Detect and respond to cyber threats in real-time.
- Protect sensitive data on devices from unauthorised access.
- Prevent malware infections and cyber-attacks on endpoints.
- Gain visibility into endpoint activities for effective monitoring.
- Secure devices for remote work environments.

Applications

Cyber threats are constantly evolving and as a result, organisations are faced with significant challenges. This is further compounded by the fact that the complexity of modern applications is becoming increasingly more intricate, with numerous interconnected components and third-party integrations, resulting in a wider attack surface. Hackers and malicious actors continuously develop new techniques to exploit vulnerabilities in applications.

All organisations use applications which need to be kept patched to keep on top of vulnerabilities – on both user endpoints and server infrastructure. Many organisations will also create their own applications either via low/no code or via traditional development or DevOps. Embedding security and privacy by design into the software development life cycle is critical for these organisations.

Our team of experienced security consultants can help you reduce the risks in your application infrastructure. We'll help you stay up to date with vulnerability and patch management for your off-the shelf applications as well as provide automated code reviews and runtime protection for any in-house built web applications.

Trust Insight to tackle your application security challenges head-on, providing you with robust protection and peace of mind.

We can help you:

- Manage your application estate to keep on top of the vulnerability & patching cycle.
- Integrate security controls into your DevOps processes without compromising development velocity.
- Shift-left the detection and remediation of threats, reducing cost of remediation.

Cloud

Cloud computing offers unmatched scalability and efficiency, but it also presents significant security challenges. Organisations need to protect their sensitive data from unauthorised access, breaches and vulnerabilities whilst staying compliant with regulations and safeguarding the business's reputation.

It's important to take a proactive, risk-based approach, collaborating with your cloud providers to establish a robust security framework.

Insight's cloud and security experts have years of experience building, securing, and running multi-cloud environments for organisations of all sizes and complexities. We'll help you create a comprehensive security framework with proactive monitoring so you can focus on growth, scalability and innovations.

We can help you:

- Achieve visibility across your multi-cloud environment.
- Secure workloads wherever they are created.
- Monitor and maintain compliance against security frameworks.

Datacentre, Network and IoT

In the modern interconnected world, there is a rapid expansion of the digital landscape, creating a complex web of technology which has opened the door to increased cyber threats, data breaches and unauthorised access.

It takes a multi-layered approach to build the security defences and resiliency required in businesses today. A combination of firewalls, encryption, access controls and regular security audits is just the beginning. You must continuously stay ahead of the threats with advanced threat detection systems and expert analysis to be proactive in identifying and mitigating potential risks.

We take a consultative approach to solving your datacentre, networking and IoT security challenges. With a deep understanding of business, technology, and security, we create the right solution for your business — from strategy and planning with design, to implementation and managed services. Our security experts can help you navigate the complexity of technology required to build and manage effective cybersecurity defences, minimising overlaps and delivering cost-effective cybersecurity defence.

Helping you with:

- Visibility into complex hybrid architectures
- Improved operational continuity.
- Security controls will work across both your on-premises and cloud networks.
- Keeping your data secure from source to destination.

Data-Centric

While security professionals spend a lot of time on securing applications and infrastructure for many organisations the critical asset they need to protect is data. Whether it's employee information, client orders, production figures or intellectual property, it's the data moving around your business that is likely adding most value for your end customers and business – and presenting the most risk if its compromised.

A good place to start when thinking about your holistic security strategy is with data, and a data-centric approach should begin by engaging your business stakeholders, not with technology.

Our approach focuses on safeguarding the data itself, rather than just securing the systems or networks that store and transmit it. We help you stay ahead of the curve and effectively protect your organisation's most valuable asset.

Helping you with:

- Discovery of the sensitive and stale data across your estate.
- Help to classify data to ensure the right amount of control is applied.
- Compliance with data protection regulations.
- Auditability of data use

Integration Domains

Governance, Risk and Compliance (GRC)

Governance, risk, and compliance are essential components of cybersecurity for businesses, encompassing the policies, procedures, and mechanisms to manage cybersecurity risks and ensure compliance with regulatory requirements such as GDPR and NIS2. Organisations face challenges in establishing effective governance structures, identifying and assessing cybersecurity risks, and implementing robust controls to mitigate threats.

Effective GRC practices establishes clear roles, streamlines processes, and mitigates cyber risks. A robust approach will increase your cybersecurity maturity, reduce legal and financial liabilities, improve your customer trust and adherence to regulatory compliance.
Insight helps make sure security is supporting the needs of your business, not constraining it. Using security risk assessments to calculate the cost of that risk and determine where controls should be placed for best effect, whilst ensuring the controls you have selected are doing their job effectively.

We help you with:

- Assessing risks
- Defining the most effective controls
- Developing policies and processes
- Embedded experts at all levels of the organisation up to CISO level

- NIS / NIS2
- DORA
- EU AI act
- ISO27001
- Cyber Essentials/+
- CIS18
- NIST CSF
- PCI-DSS

Identity & Access

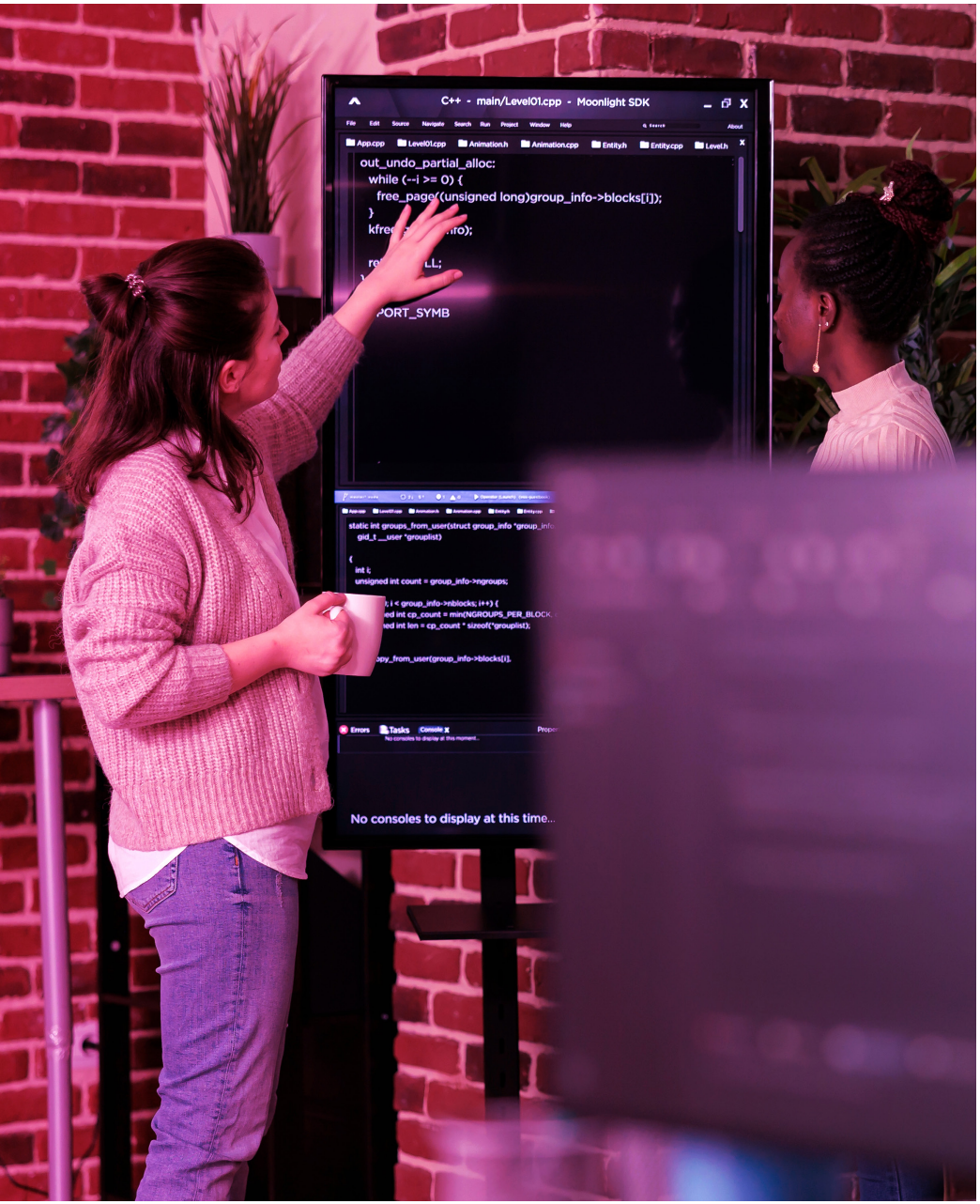
Identity and access management is a crucial aspect of cybersecurity for businesses, encompassing the processes and technologies used to manage and secure digital identities and control access to resources. Organisations face challenges in ensuring secure and efficient identity and access management practices, such as managing user identities across multiple systems, enforcing least privilege access controls, and preventing unauthorised access.

To be effective businesses need a seamless identity and access management solution deployed across their technology pillars, to provide a robust and comprehensive cyber solution.

Insight's team of experienced cybersecurity experts help by focusing on identifying and mitigating areas of risk and then supporting you to create cost-effective solutions that meet the requirements of your organisation's policies and processes. You will experience heightened security, reduced risks and improved efficiency with Insight's approach tailored to your business.

We can achieve this through:

- Taking you on the journey to zero-trust
- Taking a business-driven approach about access to data and applications
- Ensuring the right people have access to your applications and data.



Threat Detection & Response

Threat detection and response are critical components of a robust cybersecurity strategy for businesses. Organisations face myriad challenges in identifying and mitigating cyber threats, including the evolving nature of attacks, the complexity of IT environments, and the shortage of skilled cybersecurity professionals. Effective threat detection requires real-time monitoring, analysis of security events, and rapid incident response to minimise the impact of security breaches.

Insight's security experts can help you take a multi-layered approach to threat detection and response solutions across the technology domains in your business.

We create solutions using advanced tools, technologies, and our security consultants' expertise to identify and mitigate risks before they cause significant harm to your business. Insight uses technology such as SIEM and XDR, augmented by security analysts, to bring together the vast amounts of data generated by your security tools, to make intelligent decisions about threats and responses across your entire estate.

We can help you:

- Identifying threats earlier
- Reducing risks across your network
- Giving you actionable information on threats
- Automating threat defence

Human Factors

Even though security infrastructure, tools and controls are continuously improved and invested in, breaches are still happening, and they are not easy to identify and resolve. There are many specialized security controls for different kinds of threats, from attacks on endpoints to attacks on supply chains – but when you examine how these attacks happen, the main three reasons are:

- Passwords
- Phishing
- Patching

IT teams can use technology to help lower the chance of breaches, but end users will always have a role in supporting the security of an organisation. IT teams often concentrate on the technology, and sometimes the process, then forget the people side, when people can determine the failure or success of a project.

Empower your employees to become an impenetrable first line of defence against cyber threats with Insight. By taking a human-centric approach we can help you address vulnerabilities head-on, fortifying your security posture and minimising risks.

We help you:

- Measure and improve end user cybersecurity awareness.
- Provide training to developers on how to code with security in mind.
- Ensure your administrators have the skills needed to detect and respond to a cyber-attack.
- Reduce the risks of successful attacks.
- Save costs by avoiding data breaches.

Managed Security

The onslaught of security challenges is relentless, with organisations facing an increased rise in cyber threats from sophisticated hacking attempts to insidious ransomware attacks. Businesses must navigate complex regulatory compliance requirements, protect sensitive data, and stay ahead of ever-evolving cybersecurity risks. Security solutions provide numerous alerts and alarms but knowing which ones to act on with urgency is the key to prevent greater harm to your business.

These challenges combined, creates the need to deliver comprehensive and proactive cybersecurity solutions to safeguard the businesses from the diverse and sophisticated threats they face daily. Cybersecurity readiness and resilience is paramount to protecting the continuity and success of any modern business.

That's where Insight can help - our team of experienced security experts are available 24/7, supporting you to enhance your cybersecurity with proactive threat monitoring, detection and response with access to cutting edge technologies.

Our Security Operations Centre (SOC) delivers two managed services offerings, providing advanced threat detection, investigation, and response capabilities:

- Managed Endpoint Detection and Response (MEDR): Covering laptops, desktops, and mobile devices.
- Managed Extended Detection and Response (MXDR): Bringing together logs and feeds from a wide range of sources, offering the most robust detection capability for your environment.

Combining technologies such as AI, threat intelligence and analytics, our team of expert security analysts can detect and respond to threats to your environment in real-time.

We achieve this through:

- Proactive threat management.
- Expert security analysis and incident response.
- Access to advanced security technologies.
- Security strategy and roadmap guidance.
- Scalable and cost-effective model.

How we deliver

We'll help you strategise, implement and manage future-ready IT security solutions.

Assessment

- Help you to achieve accreditation against industry frameworks such as ISO27001 or NIS2
- Review your existing security controls and identify residual risks
- Help create a prioritised roadmap to achieve your desired level of security

Plan & Design

- Assist with translating your business challenges into security projects
- Support and guide you to selecting the appropriate vendors, products and services
- Envisioning workshops and technical design

Build & Implement

- Turn plans into reality – taking you from design to fully built and documented security controls
- Insight considers each project in the context of your overall roadmap
- Handover to your internal teams for management or transition to our managed services

Security Operations Management

- Support services keep your security controls working at their best
- Managed Services where Insight take responsibility for your security controls

Our Security Technology Partners

IT modernization is a team effort. We unite the capabilities of 6,000+ software, hardware and cloud partners and publishers with our team's extensive industry expertise under one roof to create best-in-class solutions that accelerate your transformation journey.

We work directly with leading technology companies so you can benefit from:

- A single point of contact to access the latest technology products and solutions.
- An ecosystem of collaborative, highly skilled teams to outfit and manage your IT environment.
- Competitive pricing and streamlined contract negotiation.
- Partner-agnostic solutions tailored to your specific needs.

Microsoft · cisco · aws · Google · paloalto NETWORKS · FORTINET · KnowBe4 · Barracuda · Check Point SOFTWARE TECHNOLOGIES LTD.

Why partner with Insight?

Cybersecurity is complicated — demanding an all-hands-on-deck approach from your end users, security teams and tools. That is why we've built repeatable methods and proven processes that yield successful results. Our experts will guide you from end-to-end, leading to improved efficiency, effectiveness, and strategic alignment.

We have:

20+ years of security transformation knowledge and experience

Deep partnerships with top tier providers

Solution-agnostic approach to find solutions best aligned to your needs.

Member of Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Cisco Partner

Advanced Security Architecture Specialized
SASE Specialized
XDR Specialized

Microsoft Solutions Partner
Security

Specialist
Cloud Security
Identity and Access Management
Information Protection & Governance
Threat Protection

Gold Microsoft Partner
Microsoft

Azure Expert MSP

Microsoft Solutions Partner
Microsoft Cloud

Next Steps

Contact Insight to enhance your cybersecurity strategy and day-to-day operations. With cybersecurity threats on the rise, protecting your business is crucial for continuity and success. Our comprehensive approach improves cybersecurity posture, identifies and mitigates risks, streamlines operations, optimises security controls, whilst maximising investments. Trust Insight's proven methods and expert guidance to strengthen your cybersecurity defences and drive business resilience and growth.