Peloton
CYBER SECURITY

Your guide to Peloton's suite of cyber security solutions

Discover how to make cyber security your competitive advantage.

A people-first approach to cyber security

At Peloton Cyber, our proven process starts with people—not tools and technology.

We know it's not possible to reduce your cyber security risk to zero. But we also know you can regain control and visibility over your threat landscape, and even turn cyber security into a competitive advantage.

To secure your business and its most critical assets, we help you build a sustainable and resilient cyber security strategy that can be measured, validated and continuously improved—with predictable costs.

As a Managed Security Services Provider (MSSP), Peloton focuses 100% on cyber security strategy and managed services, continuously optimising your cyber resilience. Our experienced team has helped ASX-listed to SMB organisations through countless cyber breaches, as well as helping them meet and build upon compliance requirements. We use these real-world experiences and learnings to deliver highly effective security outcomes focused on education, intervention and detection.

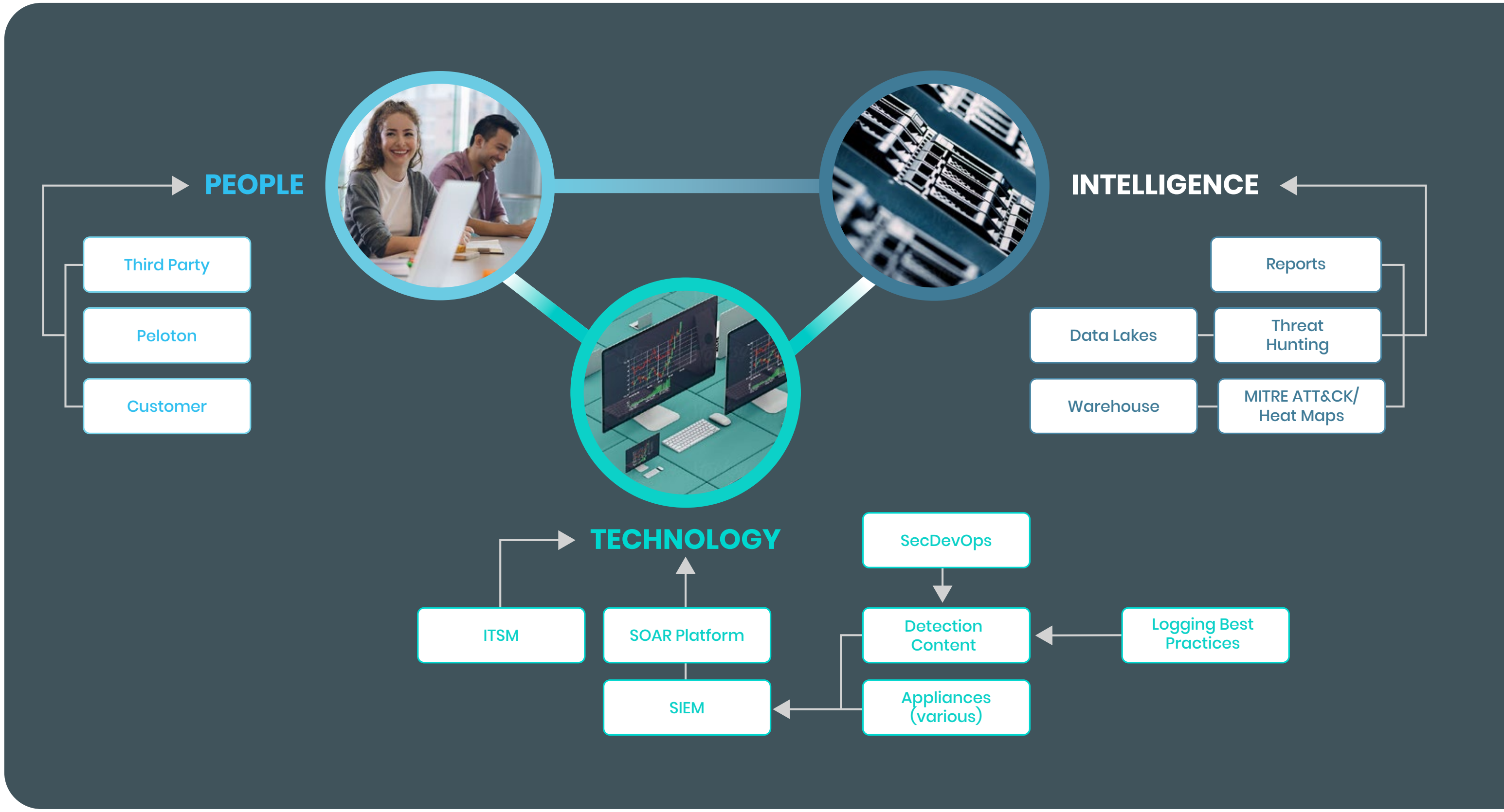
With Peloton, you get more than just security tools

Any solutions we recommend are 100% aligned to your unique business needs and context. With a clear focus on validated risk reduction, we combine people, intelligence and technology to deliver:

- **A clearer strategy**
  We'll help you determine what your acceptable risk level is and develop a strategy to help you maintain it.

- **More visibility**
  We'll give you access to transparent reporting that reveals threats and remediation actions, empowering leaders with knowledge.

- **More confidence**
  Know that the investment you make in your security strategy will reduce risk and deliver the expected value.



Everything we do is backed by our values

Generosity

We give our customers more in value than we receive in payment.

Better Together

We focus on serving people. The total will be greater than the sum of the parts.

Integrity

We shoot straight, especially when it’s hard.

Grit

We strive to fulfil our purpose and passion with uncommon resilience.

Insatiable Curiosity

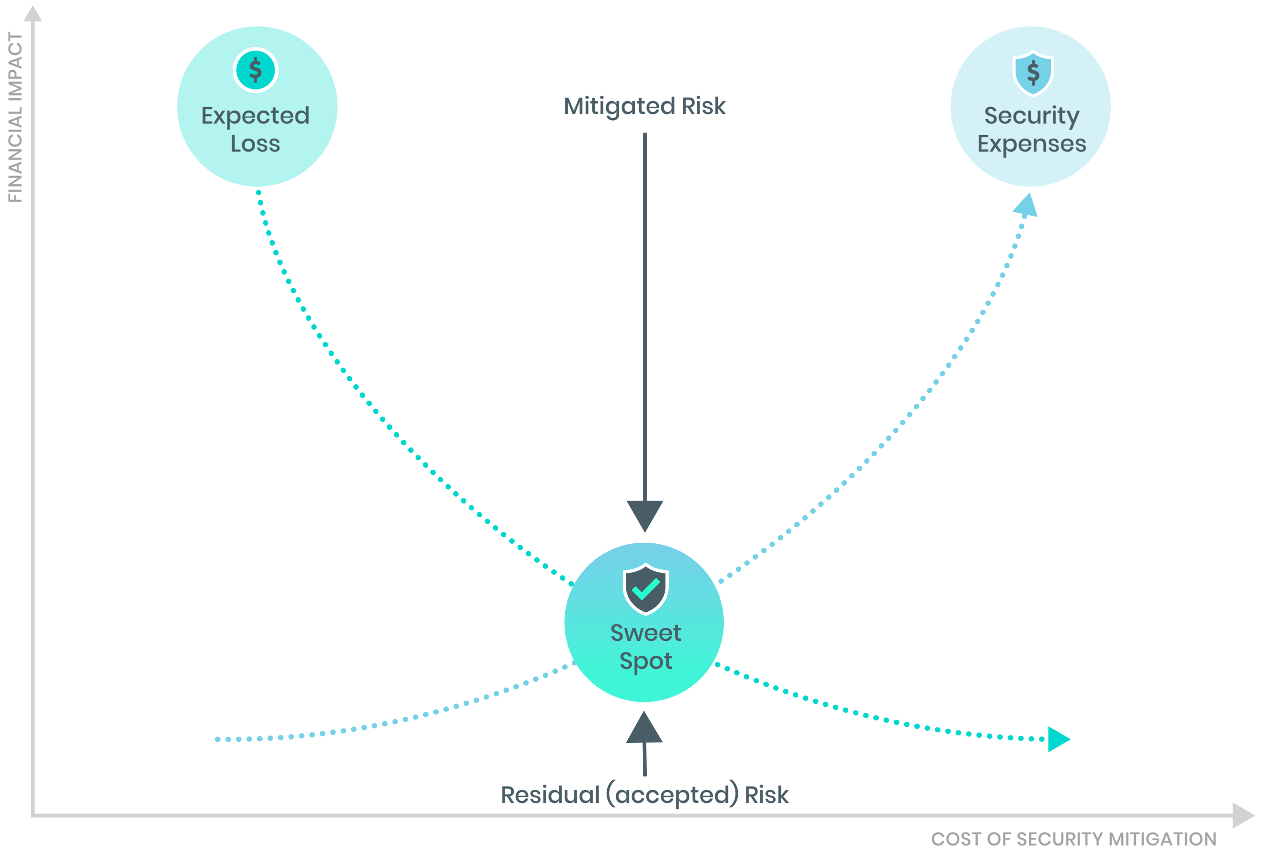
We never stop learning – we know how much we don’t know.

Finding your cyber security sweet spot

To build your cyber resilience, Peloton Cyber starts by identifying your 'crown jewels'. This is the intellectual property, assets, suppliers, partners, platforms or processes that, if stolen or shut down, would disable your business or destroy your competitive advantage.

Next, we help you design a multi-layered, risk-based and threat-focused defence strategy based on the latest intelligence and data from cyber insurers and other parties, tailored specifically to your business.

It's all about finding your sweet spot. This is the acceptable level of risk for cyber security investment versus potential losses and putting the right level of controls and reporting in place to measure, manage and optimise it based on your changing context.



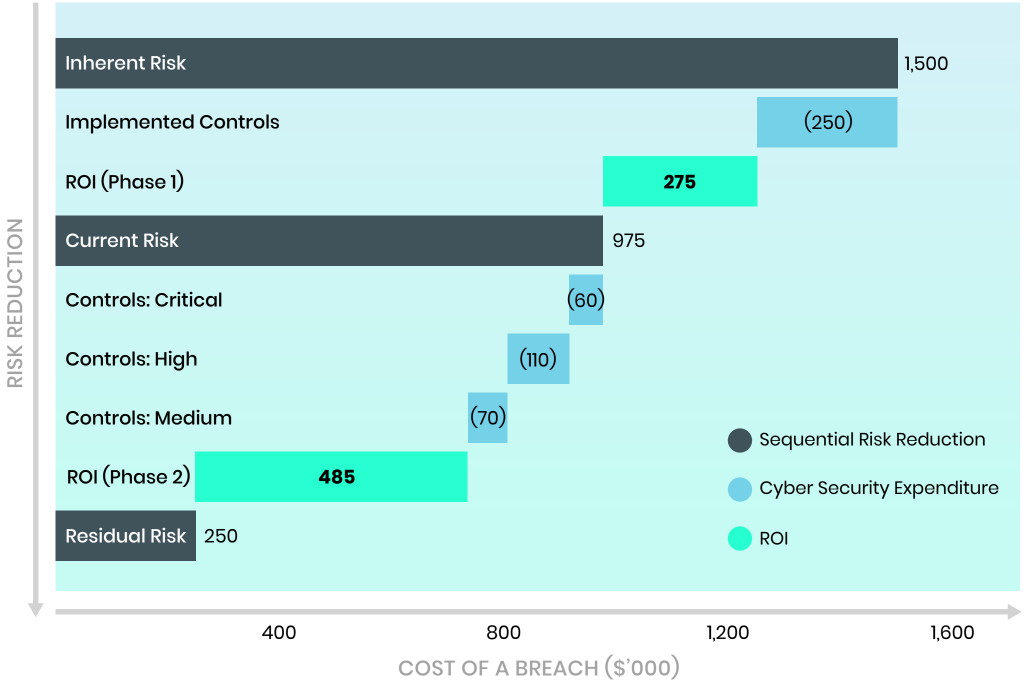
Expected Loss
Incorporates primary loss (direct impact) as well as secondary loss e.g competitive advantage loss, reputational damage, etc.

Security Expenses
Total cost of implementing security mitigation measures.

Sweet Spot
The optimal level of security that provides maximum mitigation at the desired cost.

Meeting point between mitigated risk and residual (accepted) risk.

For example, there is no point investing $100,000 to protect your key assets if the potential loss is only $70,000. We help you validate your risk mitigation strategy with tangible proof of the return on your investment, and clearly demonstrate the baseline level of investment required to balance acceptable financial loss with mitigation costs.



A four-step process geared for cyber resilience

WHAT IS CYBER RESILIENCE?

According to Harvard Law School, cyber resilience is *"A dimension of cyber-risk management, representing the ability of systems and organizations to develop and execute long-term strategies to withstand cyber events; an organization's ability to sustainably maintain, build and deliver intended business outcomes despite adverse cyber events."*[1]

[1] Harvard Law School, 2021, Principles for Board Governance of Cyber Risk

01

Understand your cyber risk

Our quick-start program gets you started with:

- Asset discovery
- Vulnerability assessment
- Cyber risk assessment
- Identity assessment
- ASD Essential Eight review

02

Develop a strategic plan

To address your risk, we help you with:

- Business case
- Defined security program
- Board reporting
- Defined success criteria
- Security metrics
- Risk appetite

03

Reduce your cyber risk

Execute on the strategic plan to reduce your risk with:

- Security operations (SIEM)
- Vulnerability and patch management
- Endpoint detection and response
- Supply chain risk assessment
- Network security review
- Incident response plan
- Security awareness training

04

Manage your cyber risk

Reduce and manage your cyber risk in a sustainable way:

- Virtual CISO / security manager
- Ongoing risk management
- Internal audit
- Security metrics
- Policy development
- Threat modelling
- Business continuity
- Security hardening
- External certification

We draw on globally recognised best-practice frameworks including NIST Cyber Security Framework, ISO27001, ASD Essential Eight and FAIR to put the most effective protections and protocols in place while you continue to pursue growth and innovation.

Strategic Services

Embed cyber security into the core of your business

Through our comprehensive range of strategic cyber security services, Peloton can help assess your current exposure to risk and formulate a plan to remediate it.

Vulnerability Assessment

Involve a deep investigation into your systems, along with remediation strategies. They are a valuable addition to your cyber security toolkit, helping you understand and act upon weak spots in your cyber defences.

Peloton uses industry best-practice frameworks and best-of-breed tools to execute a point-in-time scan of your IT environment, including cloud workloads, web applications, APIs, OT/IoT, on-premises infrastructure, and mobile or end-user computing.

In the process, we:

- Discover assets and vulnerabilities
- Exploit identified vulnerabilities
- Provide advice on the risk and remediation of vulnerabilities to provide a known state of vulnerability risk

Penetration Testing

A powerful way to track down security vulnerabilities and fix them before hackers find them. Think of it as ethical hacking, or a simulated attack with a positive outcome.

We actively test the current defence of your web applications, infrastructure and cloud services with both industry-leading and Peloton-developed tools and techniques, to simulate how a sophisticated threat actor could exploit any weaknesses.

Our testing strategies include:

- Web application penetration testing
- Cloud security assessments
- Red team adversarial simulation
- Identity and access audits
- Wireless infrastructure penetration testing

Following the test, you get a full report with remediation recommendations and actions.

Risk Assessment

Cyber breaches can have a critical impact on any organisation. It's why every security program in every organisation needs to know where potential weak spots lie, so you can work to address them.

Our independent, holistic cyber risk assessment helps you:

- Uncover and understand where risks lie
- Understand cyber threats your industry may be vulnerable to
- Assess the impact of these risks on your business
- Plan how to remediate and mitigate those risks

Working closely with your team to understand how your business uses technology as a strategic asset, we use industry-standard frameworks to assess your current versus desired maturity. Key risks are then documented and quantified before prioritising a remediation roadmap.

Identity and Access Assessment

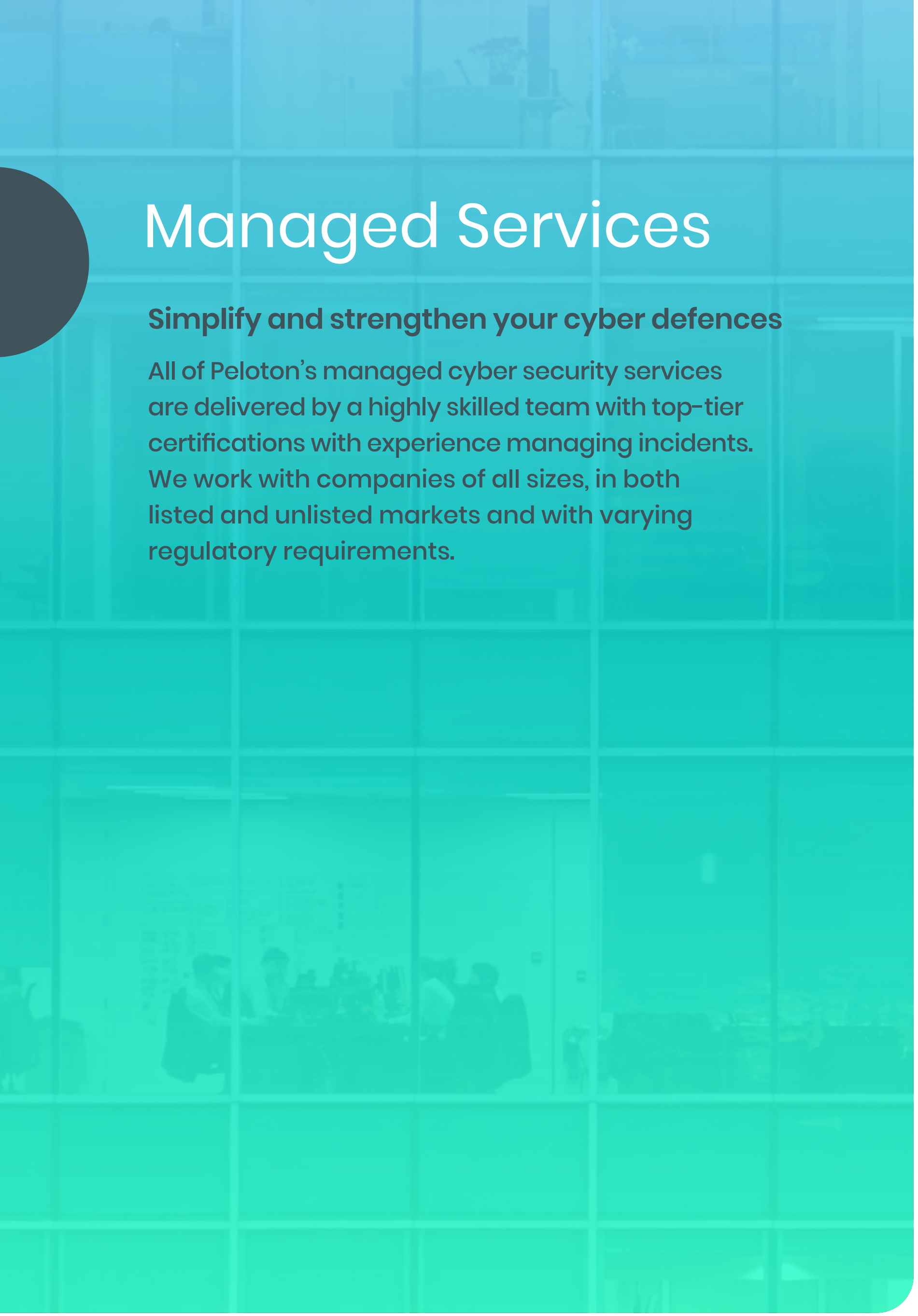
Most information security incidents occur because of compromised user accounts, due to things like poor password hygiene, phishing attacks, and a lack of multi-factor authentication. These can lead to breaches that effectively give threat actors access to your entire business.

Peloton's identity and access assessment gives you the visibility you need to identify these compromised accounts along with prioritised recommendations for remediation.

With a primary focus on Active Directory (AD) accounts, we will:

- Test all password hashes to reveal weak passwords by:
  - Uncovering common passwords against a 1.3B word list
  - Cracking weak hashes with the brute force of 5.6T iterations
- Correlate AD and Azure AD metadata
- Provide a list of immediately actionable steps

Our remediation program includes a workshop to prioritise a focused program of work, along with resource, capacity and change management planning. Post-remediation we provide metric reporting and compliance improvement strategies.



Managed Services

Simplify and strengthen your cyber defences

All of Peloton's managed cyber security services are delivered by a highly skilled team with top-tier certifications with experience managing incidents. We work with companies of all sizes, in both listed and unlisted markets and with varying regulatory requirements.

Vulnerability Management

Unpatched vulnerabilities can pose a critical risk, giving adversaries an easy way into your systems. Our vulnerability management service helps detect, assess and provide remediation advice for vulnerabilities across your entire technology stack so you can take corrective action before they are exploited.

We will:

- Continuously assess vulnerabilities and apply a risk rating based upon our own field experience in managing security incidents and the techniques used by threat actors to exploit vulnerabilities, along with leading frameworks and threat intelligence sources
- Provide a monthly vulnerability assessment report that contains key status, count and remediation advice for all vulnerabilities detected
- Perform an annual vulnerability exploitation on identified critical and high-severity vulnerabilities

It is all designed to give you a complete picture of all your assets so you can drive down risk across your organisation.

Endpoint Detection and Response (EDR)

Monitoring your endpoints is a great place to start in reducing the risk of cyber attack on individuals and your business.

The Endpoint Detection & Response (EDR) component of Peloton's Defender offering is based on Microsoft Defender for Endpoint (MDE), a market-leading endpoint security offering, developed and backed by Microsoft that prevents the most sophisticated cyber attacks, including ransomware, banking malware, and even malicious behavioural activity around zero-day vulnerabilities.

In implementing your MDE solution, Peloton applies deep expertise and customised detection content to help protect against the most advanced threats.

In this service, we:

- Apply best-practice policies for MDE
- Integrate EDR into the Peloton Defender ecosystem, including SIEM and SOAR
- Detect issues based on behavioural actions to prevent the most advanced threats

It is all backed by Microsoft's threat intelligence, plus custom detection content by FalconForce, tuned by Peloton.

Virtual Chief Security Officer (CSO)

Whether you are without a security leader in your business, you need some help doing the heavy lifting or just want an independent view of your cyber resilience, Peloton is your ideal partner.

As your Virtual Chief Security Officer (CSO), we will help you identify your cyber risks, define your security roadmap, and execute on it. We can also help you raise awareness in your business about cyber risks, educate your teams and act as both advocate and adviser.

We are not afraid to roll up our sleeves and get in the trenches with you to help reduce your cyber risk and govern your security program.

Security Operations Centre (SOC)

Sleep well knowing that your business is protected with Peloton's Security Operations Centre (SOC), which provides 24×7 detection and response to potential threats in your environment.

We use ongoing, best-in-class security monitoring to detect the tactics, techniques and procedures used by threat actors in cyber breaches. If a threat is detected, our team of cyber security experts perform rapid incident analysis and provide remediation advice to reduce the impact of any breaches.

SOC monitoring, detection and response are aligned to your unique business context. While this is identified in an initial cyber risk assessment, our security engineering team then develop detections at each stage of an attack (mapped to the relevant business processes identified) and then track and validate detections across the MITRE ATT&CK framework.

Key components of our SOC service include:

- **Security Incident and Event Management (SIEM)**
  Constant monitoring of active and emerging cyber threats, aligned to your business context
- **Security Orchestration and Automated Response (SOAR)**
  Behind-the-scenes processing of your critical cyber security data

GET IN TOUCH

Together let's make
cyber security your
strategic advantage.

www.pelotoncyber.com.au

1300 735 686

Head office:
Level 11, 45 William Street,
Melbourne, VIC 3000