

Re **think** Security in the era of AI

Maximise the opportunity.
Minimise the risk.



Contents

- P 3 **Security in the era of AI**
- P 4 **AI is reshaping cybersecurity**
- P 6 **Securing the workplace in the era of AI**
- P 7 **Securing connectivity in the era of AI**
- P 8 **Securing hybrid cloud in the era of AI**
- P 9 **The Intelligent Security Blueprint**
- P 10 **Intelligent Security built on the award winning Logicalis Digital Fabric Platform**
- P 11 **With great power comes great responsibility**





Security in the era of AI

Maximising the AI opportunity while minimising the risk.

The speed of progress of AI is breathtaking. Quantum computing and GPTs (Generative Pre-trained Transformers) are turbo-charging digital transformation. The technologies have huge potential in cybersecurity and are fast becoming essential tools for all security professionals.

But AI and generative AI also create new risks. A [recent World Economic forum report](#) reveals that advances in adversarial capabilities (phishing, malware, deepfakes) present the most concerning impact of generative AI on cyber.

AI is also becoming an essential tool for cyber criminals and the threat is heightened by geopolitical instability and a global skills shortage.

This whitepaper looks at the challenge of how to enable your organisation to maximise the transformative opportunities AI offers, while minimising the risks it creates. We explore how innovative CISO's and CIO's are embracing the technology, while safeguarding their workplaces, connectivity, and cloud infrastructure.

A key consideration is whether you have the security skills inhouse to operate safely. By outsourcing the expertise, your defence posture shifts from reactive to proactive. Intelligent, always-on, managed security services use cutting-edge AI to stay ahead of the attackers. IT leaders can liberate internal teams to innovate with the emerging technologies, confident the organisation is protected.



AI is reshaping cyber security

AI is reshaping cybersecurity, both as tools for defenders and as weapons for attackers.

AI on the attack

While there is talk of hackers creating FraudGPTs and WormGPTs, the most eye-catching new risk created by generative AI is social engineering. Generative AI models, like those used in chatbots or text generators, can create highly convincing phishing emails, tailored social media posts, or even deepfakes to trick victims.

Generative AI may also help attackers create Zero Day ransomware for which there is no known patch. More innocently, generative AI also creates the risk of employees leaking sensitive data while using public GPTs.

AI helps hackers create polymorphic malware that constantly changes its signature, making it much harder for traditional security tools to detect. AI can also be used for automated attack generation which targets vulnerabilities at a far greater scale than human attackers could manage.



AI to the defence

Taking these threats into account, experts don't see AI creating completely new attack methods, and the technology is already being used to defend against existing threats. AI can analyse massive datasets of network activity, learning normal behaviour patterns and flagging anomalies that could indicate attacks. Generative AI further enhances this by creating more sophisticated models, better at mimicking normal activity for comparison. AI models can sift through historical threat data and ongoing network behaviour to identify patterns and predict potential future attacks. This helps cybersecurity teams proactively secure vulnerabilities. AI also helps analyse malware code, automatically identifying similarities, variants, and potential origins.

AI scans systems and codebases, hunting for potential vulnerabilities, and generative AI can take this further by helping to predict and design potential exploits, even for Zero Day vulnerabilities. AI can be used to automate certain security responses, such as isolating infected machines or blocking suspicious traffic. This speeds up reaction times and helps to contain attacks early.

According to the [World Economic Forum Global Cybersecurity Outlook Survey](#), only 10% of IT leaders believe that GenAI will give the advantage to defenders over attackers in the next two years.

We, however, believe this pessimism is unfounded. Security experts have more access to quantum computing and data to train AI to defend, than cybercriminals have to train AI to attack.

If CIO's and CISO's harness the right expertise they tip the balance in their favour.

86% of CIO's believe GenAI will alleviate skills gaps and talent shortages, Logicalis CIO report, 2024.



Securing the workplace in the era of AI

The big risks in the workplace are identity security and device security. Generative AI can be used to create realistic deepfakes or manipulate text to impersonate real people which trick employees into revealing sensitive access information.

In [August 2023](#) an employee of a software company was tricked into giving away their company multifactor authentication code because the attacker was using a deepfake audio of a familiar colleague.

AI, however, can counter intrusions by learning user patterns and flagging irregular access attempts. It is also essential to educate employees on the new risks from generative AI to help them identify and avoid social engineering attacks.

Some 84% of workers who use generative AI at work said they have publicly exposed their company's data in the last three months, according to a new [16-country study](#) of more than 15,000 adults by the Oliver Wyman Forum.

[Darktrace](#) researchers found a 135% increase in novel social engineering attacks from January to February 2023, corresponding with the widespread adoption of ChatGPT.



Securing connectivity in the era of AI

Networks need to support the growth of IOT, 5G, and edge computing. But the expanding attack surface presents more opportunities for cybercriminals.

Edge devices typically have less processing power and security features to cloud servers, which makes them more vulnerable. Processing data at the edge also creates risk.

AI can be used to secure networks and connectivity by analysing data streams at the edge in real time. It can identify unusual patterns that indicate malware, intrusions, and denial of service (DoS) attacks quicker than sending the data to the cloud for analysis.

It is essential, however, to implement robust security measures during the development of AI models for edge devices. This includes hardening the models against manipulation and poisoning attacks.



I see new threats in 5G,
given there's going to be
more data at the edge.

Paul Kurtz, Chief Cybersecurity Advisor, Splunk



Securing hybrid cloud in the era of AI

Securing a hybrid cloud environment is a complex operation. Often you will have different suppliers using different configurations and languages. According to the [PWC Global Digital Trust Insights Report](#), the hybrid cloud is the top security concern for nearly half of all enterprises.

AI has a big part to play but it is not infallible. It can analyse vast amounts of data across hybrid clouds, identifying anomalies and breaches faster than traditional methods. AI can also automate repetitive tasks like vulnerability scanning, log analysis, and incident response. Generative AI can be used to adjust security controls based on real-time threat intelligence and changing risk profiles.

But complex hybrid cloud environments can lead to misconfigured security policies, which AI may not always detect. Also, AI models can be like black boxes, making it difficult to understand how they arrive at security decisions. Therefore, human oversight is essential and it is best practice to regularly test and monitor AI models for vulnerabilities that could introduce new security risks.

97% of enterprises admit to having gaps in their cloud management plans.

[PWC Global Digital Trust Insights Report](#)










The Intelligent Security Blueprint

Many organisations focus on one area of the security fabric, but at Logicalis we recognise in today’s cybersecurity landscape there are no silos. Organisations must look across the entire footprint, from Secure Connectivity, Securing the Cloud, Securing the Hybrid Worker and weaving Secure Operations across the entire organisation.

With Logicalis Intelligent Security, the blueprint for change helps guide your journey so you can start every day with confidence.

 <p>Advisory</p> <p>GRC consulting to help organisations understand the rapidly evolving and expanding world of governance risk and compliance. Knowing your legal and regulatory obligations and your specific risk tolerance is the first step to determining your required security posture, capabilities and processes.</p>	 <p>Secure workplace</p> <p>Securing worker communications such as email and chat, the devices they work from and how they access the systems they use to do their job are critical security components.</p>	 <p>Secure connectivity</p> <p>The network is the foundation of everything from connectivity to how staff access and use systems. Today, threat actors understand the criticality of the network and if they undermine it, an organization is highly vulnerable and potentially ceases trading. Networks need to be secure to enable safe IOT, 5G and edge computing.</p>	 <p>Secure hybrid cloud</p> <p>Today data lives in multiple places, sometimes on premise, sometimes in the cloud, and sometimes in SaaS services where you have little control. Organizations today need to adopt a zero trust approach to who accesses what data and when, how it is protected and crucially, how it is recovered.</p>	 <p>Secure operations</p> <p>The Logicalis Security Operation Centre (SOC) provides eyes on glass of highly trained security analysts 24/7 across three global security regions, providing best practice proactive protection and incident response services. The SOC operates as an extension of your team and alleviates the budget drain and HR burden of recruiting, retaining and training your own people.</p>
---	--	---	--	--



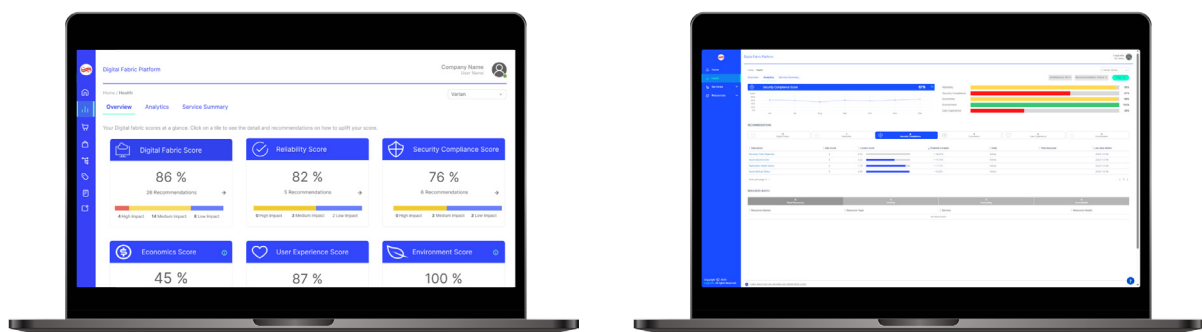
Intelligent Security built on the award winning Logicalis Digital Fabric Platform

Logicalis provide customers with access to their award-winning Digital Fabric Platform (DFP), providing a real-time view of your managed environment across key areas such as reliability, security and compliance, economics, user experience, and environmental impact.

Your Security and Compliance score helps you quickly understand if your organisation is protected against threats, your data is secure, your systems are up to date, and everything is under warranty and compliant.

Utilising the Digital Fabric Platform allows you to quickly understand if your organisation is protected against threats, your data is secure, your systems are up to date, and everything is under warranty and compliant.

The DFP also utilises AI and benchmarking to provide advanced reporting and recommendations that can help further improve your security posture.



Take a look at our Security and Compliance demo here:

<https://www.logicalis.com/managed-digital-fabric-demo-sign-up>



**With great power comes
great responsibility**

The era of AI presents us with tremendous opportunities for growth and progress. However, it also demands that we rethink security and take proactive measures to safeguard our workplace, connectivity, and cloud infrastructure.

By taking an intelligent approach to security and leveraging AI's power, we can maximise the benefits while minimising the risks it poses.

With Logicalis working hand in hand or by your side, you are empowered to detect and respond to any threat. Stay hypervigilant in the face of new risks and begin every day with confidence.

**We are Architects of Change.
We help organisations succeed in a digital-first world.**

At Logicalis, we harness our collective technology expertise to help our clients build a blueprint for success, so they can deliver sustainable outcomes that matter.

www.uki.logicalis.com