PERFORMANTA

SAFE XDR

Minimise risk.
Feel assured.
Be cyber safe.

Digital risk in 200 words

Security is now foundational to business growth to support collaboration and data sharing, supply chain management, end user engagement, and successful e-commerce.

Succeeding as a business means putting yourself in the firing line of cyber threats, every single day.

Digital companies face three challenges to the outcomes they seek:

01.
The cyber threat is growing and evolving, and breaches are more frequent and severe.

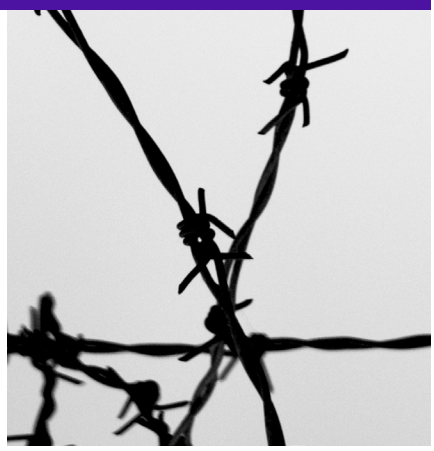
02.
Digital disruption such as cloud migration and remote working complicates IT, taking away control from defenders and making it harder to be safe.

03.
European regulators are baring their teeth, dishing out hefty fines for data privacy transgressions.

Despite prodigious cyber security expenditure, the problem is getting worse[1]. Why? Because few organisations have visibility and control over their entire attack surface. They can't see the gaps in their defence that attackers can.

Criminals can break into organisations in a matter of clicks. An estimated 2,200 cyber security attacks are detected each day[2]. The stakes are high: the average cost of a cyber-attack is €180,000 with 60% of smaller companies going out of business within six months of an attack[3].

Worldwide cybercrime costs are predicted by McKinsey and Co to hit $10.5 trillion annually by 2025[4] representing the greatest transfer in wealth in history.



1. In 2023, global security and risk management end-user spending reached an estimated $188.1 billion [https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024]
2. https://www.getastra.com/blog/security-audit/cyber-security-statistics/
3. https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf
4. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Why companies don't have the security they need

Companies are poorly served because free market economics don't really apply to the cyber security market. There are three reasons why:

01.

Disorientation: the market is large, fast growing and fragmented. 250 new companies are created every year offering new (minimum viable) solutions to new threats. There are around 4,000 cyber security companies worldwide, that spend a third of their income on marketing. The market is noisy and difficult for buyers to navigate.

02.

Motive: unintentionally, the cyber security industry has turned into big pharma: instead of focusing on solving the root cause of the problem, it does what makes the most money[5].

03.

Buyers have no way of assessing the quality of what they are buying. Few vendors are transparent about how their solutions work. It is not the best products and services that succeed, but the best marketed ones[6].

What is it about the cyber security industry that requires such a brutal investment in persuasion?

It is a 'market for lemons'[7]. Buyers don't know which vendors to trust, so they ask the analysts.

The cyber security analysts' prescription

The cyber security advice you get from analysts is the same advice you might receive from your grandparents: do the basics well:

- Validate that your existing security controls are working as expected
- Mandate multi-factor authentication (MFA)
- Use auto-generated passwords where MFA is not possible
- Maintain an inventory of IT assets and patch them regularly
- Impede attackers with proactive detection and response controls
- Rehearse what you would do when a security incident happens.

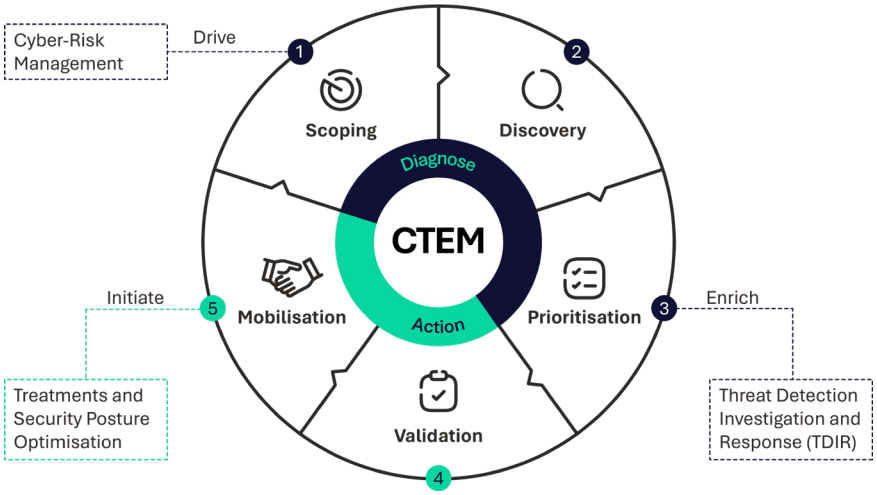
The trouble is that we don't. Security is complicated and the risks are ever-changing. **In Performanta's experience for example, basic controls like anti-virus are active on only 70-80% of clients' devices and that up to 25% of devices in a network are not regularly patched.**

Gartner, a leading global cyber security analyst firm, recognises that few organisations have the resources to protect themselves completely, so must make the best use of the resources that they have.

5. https://www.amazon.co.uk/Cyber-Builders-Essential-Building-Cybersecurity/dp/173823410X
6. Former MBA students, look up George Akerlof's work on information asymmetry in markets, which drives out quality.
7. https://www.debatesecurity.com/downloads/Cybersecurity-Technology-Efficacy-Research-Report-V1.0.pdf

Continuous Threat Exposure Management

Gartner prescribes Continuous Threat Exposure Management (CTEM), an approach that identifies and prioritises action to mitigate the most severe risks to your business before attackers can exploit them. The key steps are depicted, below.



CTEM is a smarter way to keep your business safe from cyber threats.

According to Gartner, CTEM can help organisations reduce breaches by two-thirds by 2026[8].

What would a cyber safety solution that reliably protects companies with a growing volatile attack surface look like?

Companies want to be cyber safe

In the real world, people still value peace-of-mind above and beyond the promise of security and risk reduction. We should feel secure AND know that we are secure.

Cyber security alone is not enough, businesses want to be "cyber safe"

8. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

Our cyber safety solution

Safe XDR

Safe XDR is the first platform in the market built to deliver CTEM. It combines ASM and XDR technologies in a single platform that provides the visibility of your attack surface and the control you need to feel cyber safe.

01.

Encore Attack Surface Management (ASM) service that provides an attacker's view of your attack surface and shows gaps and misconfigurations in your defences that create risk.

02.

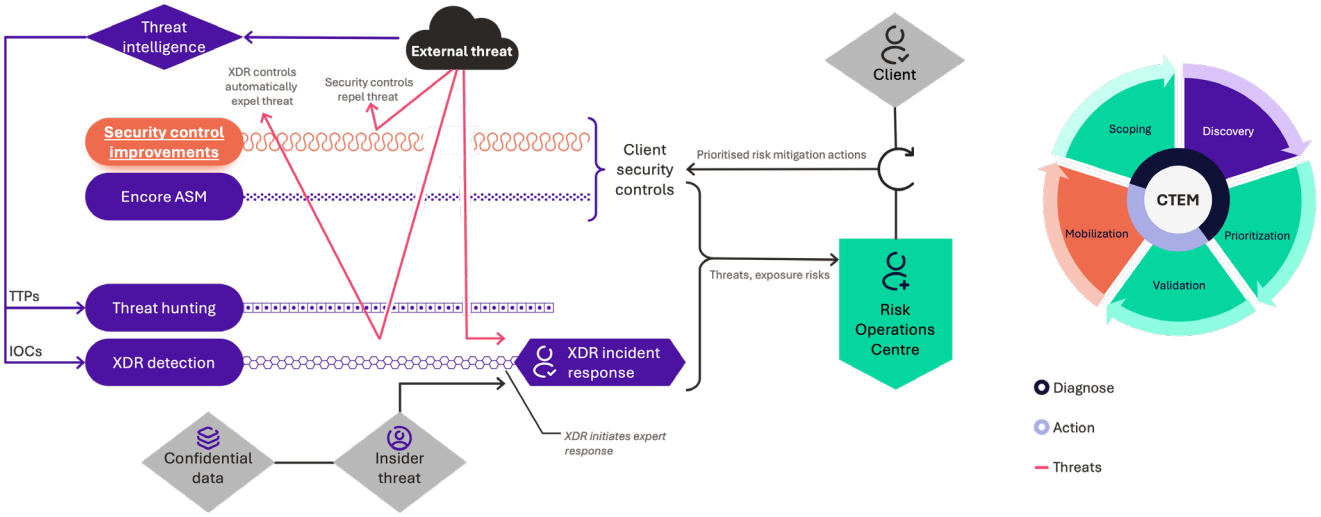
Extended Detection and Response (XDR) service that proactively hunts for evidence of attack, supported by automation that empowers analysts and reduces response times.

03.

Risk Operations Centre (ROC) that prioritises exposure risks, develops risk mitigation plans, provides execution support to clients and ongoing service management.

Safe XDR not only protects your IT, it identifies the weaknesses in your defence, prioritises risk reducing actions, and helps you implement them.

We don't just tell you what's wrong, we identify the problems to solve and show you how.



Stage	Safe XDR solution
Scoping	ROC expert reviews cyber risk assessment and security controls.
Discovery	ASM team identifies assets visible to an attacker and validates that security controls are working. XDR team detects and responds to cyber security threats.
Prioritisation	ROC expert assesses likelihood that asset could be compromised and prioritises attack surface exposure risks that need to be validated.
Validation	ROC expert assesses the impact to the business of the prioritised exposure risks being exploited.
Mobilisation	ROC expert plans with client how to mitigate the vulnerabilities that present the greatest risk. If necessary, ROC organises support.

We support you on your journey from cyber secure to cyber safe.

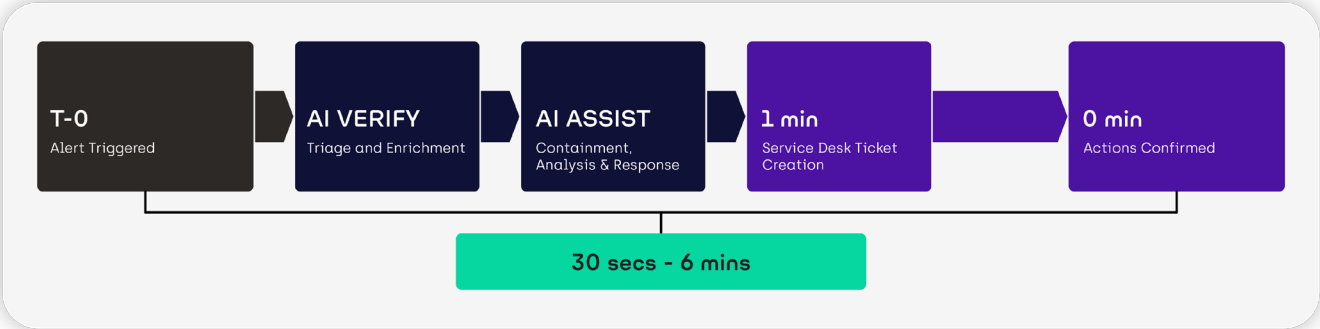
The benefits of Safe XDR are:

01.
Improved security posture, reducing the risk of being breached

02.
Better decision-making about your security investments.

03.
Increased efficiency: helping you to automate security tasks.

Our Safe XDR Service, powered by our Safe Platform drastically reduces time to remediate from 1 hour and 15 minutes to 25 minutes and with Microsoft Copilot for Security down to between 30 seconds – 6 minutes.

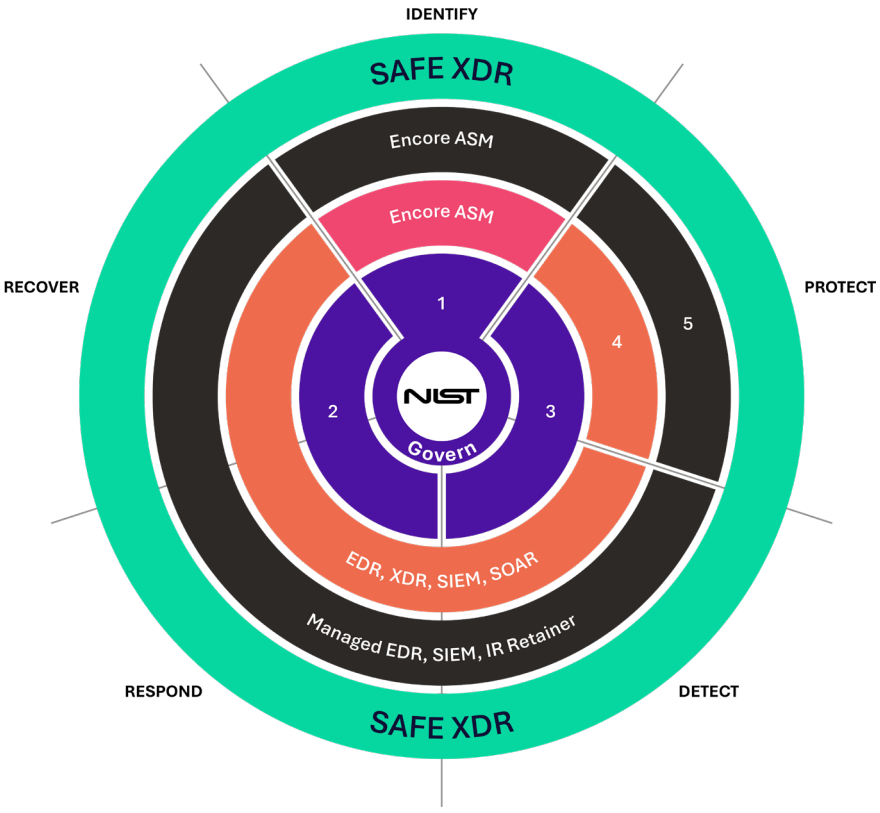


Safe XDR portfolio

Safe XDR provides in a single package, all the capabilities you need to be cyber safe.

You make have these services already or you may wish to build your own solution. We can provide the consulting, products and services you need to build and operate your own solution. Our portfolio is illustrated, below.

1. **Strategy and maturity assessments, Security controls review, Security assurance, Compliance**
2. **Readiness, Digital forensics, Additional IR support**
3. **Architecture development, Design & Planning, Deployment support**
4. **Cloud, endpoint and network security controls, IAM, PAM, DLP and GRC**
5. **Managed security controls**



Consulting | Microsoft product | Performanta product | Performanta service | Safe XDR service

Outcomes Safe XDR delivers

Role	Business outcome	Technical outcome
CEO	Greater likelihood of achieving business goals Preservation of reputation	Transparent accountability for cyber safety
CFO	Regulatory compliance Reduced risk to long-term profitability	Minimised cyber risk management cost
CRO	Reputational protection	Effective internal and third-party cyber risk management
CIO	IT security based on informed balance of cost, risk and opportunity	Uncomplicated cyber security that enables business agility
CISO	Resilience aligned to business strategy and goals	Identification and protection of business-critical assets Proactive management and improvement of security controls.
Client, Regulator	Assurance about the quality of your security controls	Compliance with current and impending regulation (eg NIS2, DORA)

Why Performanta

Would you prefer your important operation be performed by a surgeon or a Nobel prize-winning anatomy professor? Cyber safety needs to be delivered by practitioners, not theoreticians.

Our heritage

Performanta's heritage is in providing professional services to technology companies: initially Forcepoint and CyberArk, then HP and ArcSight, and most recently to Microsoft. They use our highly trained, highly capable engineers to fix their clients' intractable deployment and configuration problems.

Our cyber safety approach

Our approach to cyber safety is to create solutions such as Safe XDR that are engineered at a fundamental level to identify exposure risks and avoid incidents . When incidents arise, we don't just tell what incidents we have resolved, we tell you why they happened and what you need to do to prevent future incidents. If necessary we will help you prevent them. We then use reverse-engineering to determine how to automatically prevent further incidents.

Safe XDR

Safe XDR is the world's first fully integrated, CTEM-enabling platform developed with over a decade of frontline experience of combatting cyber attacks.

We go beyond the traditional XDR solutions that detect and respond to threats. We don't simply treat cyber security maladies, we identify cyber health improvements that make the biggest difference and we help you achieve them.

How clients benefit

Performanta's clients benefit from our security operations centres and threat intelligence sources located in Europe, the BRICS countries and Africa, which give us early visibility of new exploits tested in these regions where defences are weakest, before being used global cybercrime campaigns, in the West.

We are transparent about how our solution works. We live by our reputation. We are big enough to deliver and small enough to care.

Who we are

Performanta is a stable, profitable, multinational company that specialises in cyber safety.

Founded in 2010, we have grown to over 180 security professionals. We provide risk and resilience consulting, managed detection and response, and continuous threat exposure management services, with a human touch. Our focus extends beyond your security controls, to your wellbeing. We work tirelessly with clients to manage the cyber security risks.

Performanta is a leading Microsoft Solutions Partner. We have been nominated by Microsoft to join its Intelligent Security Association (MISA), a worldwide group comprising 300 of its most proficient partners.

Performanta is approved to design, develop and operate security solutions for on-premises and cloud service users. We specialise in Managed Extended Detection & Response (MXDR), Identity and Access Management, and Threat Protection.

We work with enterprises across many industry sectors, that require a cyber safety service. Operating from the UK, South Africa, North America and continental Europe, our teams deliver global services with a local feel.