

# PENTESEC PRODUCTS & SERVICES



## Introduction

From firewalls through to Incident Response and fully Managed Services, our teams of experts work with businesses of all sizes, in all sectors, to provide cyber security solutions and services that protect staff and data, secure networks, maximise return on investment and protect your business against ever evolving threats.

This list is not exhaustive as we add new technologies and services on a regular basis.

If you can't find what you're looking for, reach out to one of our team and we'll be able to recommend the right technology.



|  |   |
|--|---|
| Network Security/Firewalls                                       | 2 |
| Cloud Security   | 2 |
| Email Security   | 3 |
| Security Awareness Training                                      | 3 |
| Continuous Security Validation<br>(Breach and Attack Simulation) | 4 |
| Application Security/WAFs  | 4 |
| SASE   | 5 |
| Endpoint Security  | 6 |
| SIEM   | 6 |
| Vulnerability Management   | 7 |
| SOAR   | 7 |
| IOT  | 7 |
| IAM and PAM  | 8 |
| DDoS   | 8 |

## Pentesec Managed Services

|  |    |
|--|----|
| Managed SIEM .....                         | 10 |
| SOAR-as .....                              | 10 |
| Managed Detection and Response .....       | 10 |
| Managed Vulnerability Management .....     | 11 |
| Managed Firewall .....                     | 11 |
| Hosted Management .....                    | 11 |
| Managed Intrusion Prevention Service ..... | 12 |
| Pentest Plus Support .....                 | 12 |

## NETWORK SECURITY / FIREWALLS



Palo Alto Networks offer one of the worlds' leading zero trust network security platforms that secure a world where any user can work anywhere. ML-Powered Next-Generation Firewalls offer the perfect balance of security and performance.



Check Point Quantum Next Generation Firewall Security Gateways combine SandBlast threat prevention, hyper-scale networking, a unified management platform, remote access VPN and IOT security to protect you against the most sophisticated cyber-attacks.

## CLOUD SECURITY



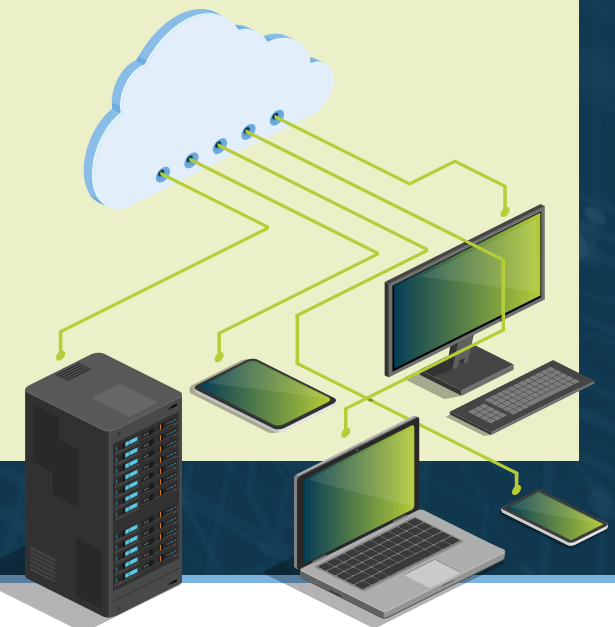
Prisma Cloud secures applications from code to cloud, enabling security and DevOps teams to effectively collaborate to accelerate secure cloud-native application development and deployment while protecting critical applications across multi-cloud and hybrid environments.



Rapid7's InsightCloudSec secures your public cloud environment from development to production with a modern, integrated and automated approach. InsightCloudSec allows you to manage cloud security posture, secure cloud workloads and govern Identity and Access Management from a single interface.



Check Point CloudGuard provides cloud native security for all your assets and workloads, across multi-clouds, allowing you to automate security everywhere, with unified threat prevention and posture management.



## EMAIL SECURITY

### proofpoint.

Proofpoint delivers the most effective unified email security solution to protect your people and critical data from advanced email threats. Our complete, extensible email security platform blocks malware and malware-less email threats, such as email fraud, also known as business email compromise (BEC).

### mimecast

Defend against even the most sophisticated attacks and stay one step ahead of threats with Mimecast Email Security. From phishing and ransomware to social engineering, payment fraud, and impersonation, we block the most dangerous attacks, delivering world-class email security in the way that best meets your needs.



Harmony Email & Collaboration provides organizations with complete, full-suite protection that is constantly adapting and evolving to the ever-changing threat landscape, while providing security admins with an easy-to-deploy and manage platform, making your security offerings easy and efficient.

### Clearswift

Email Security

Clearswift offers a range of email security options and packages to suit individual requirements. Its Secure Email Gateway protects all incoming and outgoing email communications, while its Secure Exchange Gateway scans only internal email traffic. ARgon for Email is an add-on security solution that enhances the DLP capability of existing email gateways to improve security and reduce risk.

## SECURITY AWARENESS TRAINING

### proofpoint.

Proofpoint Security Awareness Training empowers your people to defend your organisation with a holistic solution resulting in 30% fewer clicks on real-world malicious links. It has been named a Gartner Leader in its Magic Quadrant for 6 years in a row. PenteseC are the only Proofpoint Certified Security Awareness Training Specialist in the UK.

### mimecast

Mimecast Awareness Training is designed with you and your learners in mind. Our solution brings together all the elements of effective security awareness continuously, in partnership with Email Security, and serves as a launch pad for reduced risk and a more resilient organization.

To learn more about how PenteseC's Services can benefit your business, contact us today:

**Call 0845 519 1337 or Email [sales@penteseC.com](mailto:sales@penteseC.com)**

## CONTINUOUS SECURITY VALIDATION (BREACH AND ATTACK SIMULATION)

### PICUS

The Complete Security Validation Platform from Picus is an award-winning Breach and Attack Simulation (BAS) solution that helps security teams to validate, measure and optimize security effectiveness. Achieve optimal protection from your security controls, discover and eliminate attack paths to critical assets and optimise detection and response capabilities with this leading solution.

## APPLICATION SECURITY / WAFS



CloudGuard AppSec is fully automated and leverages contextual AI analysis to provide precise threat prevention for modern web applications- lessening the need for on-going administration and increasing your application security at scale.



F5 BIG-IP Advanced WAF protects applications and APIs from bad actors and automated threats trying to steal data, take over accounts, siphon resources (for example, cryptomining), and exploit zero-day vulnerabilities. Deployable across multi-cloud, hybrid, and on-premises environments in various forms, BIG-IP Advanced WAF provides a robust suite of sophisticated protections while enabling security automation for DevOps and AppDev.

### RAPID7

InsightAppSec performs black-box security testing to automate identification, triage vulnerabilities, prioritize actions, remediate and reduce risks in modern web applications. Get actionable, accurate insights by leveraging industry leading attack frameworks, speed up remediation with self service access and integrate into developer workflows to prevent risks early.



## SASE



Prisma SASE simplifies operations by converging best-of-breed networking and security into a single service. Unified management and a shared data lake improve team collaboration and streamline operations. Prisma SASE is built in the cloud to secure at cloud scale while delivering exceptional user experiences. A truly cloud-native architecture provides uncompromised performance backed by leading SLAs.



The Netskope SASE combines Netskope's market-leading Intelligent SSE with its next-generation Borderless WAN to provide a cloud-native, fully converged, and single-vendor SASE solution. Netskope's converged SASE platform provides AI-driven zero trust security and simplified, optimized connectivity to any network location or device, including IoT.



Check Point Harmony Connect, the only prevention-focused Secure Access Service Edge (SASE) solution, is redefining SASE by making it easy to access corporate applications, SaaS and the internet for any user or branch, from any device, without compromising on security.

Built to prevent the most evasive cyber-attacks, Harmony Connect is a 100% cloud service that unifies multiple network security products, deploys within minutes and applies Zero Trust access policies with a breezy user experience for all.



Cato SASE Cloud is a proven SASE platform you can deploy today. Cato's cloud-native architecture converges SD-WAN, a global private backbone, a full network security stack, and seamless support for cloud resources and mobile devices.

Customers easily connect physical locations, cloud resources, and mobile users to Cato SASE Cloud, and IT teams immediately benefit from the agility of a unified network and security service managed through a single, self-service console.

## ENDPOINT SECURITY



Harmony Endpoint is a complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. It prevents the most imminent threats to the endpoint such as ransomware, phishing or drive-by malware, while quickly minimizing breach impact with autonomous detection and response.

This way, your organization gets all the endpoint protection it needs, at the quality it deserves, in a single, efficient, and cost-effective solution.



SentinelOne Singularity XDR simplifies modern endpoint, cloud, and identity protection through one centralized, autonomous platform for enterprise cybersecurity. SentinelOne Singularity makes machine-speed decisions against threats on the front lines, equipping every endpoint and workload—no matter their location or connectivity—to respond intelligently with powerful static & behavioural AI.

## SIEM



InsightIDR from Rapid7 is a lightweight, cloud native SIEM platform that allows you to own the entire attack surface with more signal and less noise. Complete with embedded threat intelligence, InsightIDR continuously monitors your security environment to detect behaviours that foreshadow a breach.



To learn more about how PenteseC's Services can benefit your business, contact us today:

**Call** 0845 519 1337 **or Email** [sales@penteseC.com](mailto:sales@penteseC.com)

## VULNERABILITY MANAGEMENT

### **RAPID7**

Rapid7 InsightVM assesses and prioritizes risk based on various relevant factors, such as its potential impact to your business and what attackers are actively doing in the wild. InsightVM leverages our unique Real Risk Score that combines CVSS base metrics of business impact and exploitability with measures of exposure to give you a more granular view of what's relevant here and now.

## SOAR



Cortex XSOAR is a comprehensive security orchestration, automation and response (SOAR) platform that unifies case management, automation, real-time collaboration and threat intelligence management to serve security teams across the incident lifecycle. XSOAR allows you to respond to incidents with speed and scale by ingesting data from across your environment before executing automatable, process-driven playbooks to enrich and respond to these incidents.

### **RAPID7**

Rapid7 InsightConnect is a standalone orchestration and automation solution that accelerates and streamlines time-intensive processes—with little to no code. With 290+ plugins to connect your tools and easily customizable connect-and-go workflows, you'll free up your team to tackle other challenges, while still leveraging their expertise when it's most critical.

## IOT



Armis is the leading asset intelligence and security platform purpose-built to protect the extended asset attack surface, including managed, unmanaged, IT, OT, IoMT, IoT, cloud and connected 5G assets. Armis allows you to discover every asset in your environment with 100% visibility and rich context to track behaviour, detect threats and help you take action to protect your business.



## IAM AND PAM



One Identity can help unify your approach to managing access rights for better visibility and control, verify everything before granting access to your most-important assets and help you adapt to an evolving threat landscape.



Okta Workforce Identity Cloud provides easy, secure access for your workforce so you can focus on other strategic priorities—like reducing costs, and doing more for your customers. Empower your people, protect your data, and accelerate your business with an Identity-first security solution built for today's dynamic workforce.

## DDOS



Radware provides automated DDoS protection from fast-moving, high-volume, encrypted or very-short-duration threats and is part of Radware's attack mitigation solution. It defends against IoT-based, Burst, DNS and TLS/SSL attacks to secure organizations against emerging network multi-vector attacks, ransom DDoS campaigns, IoT botnets, phantom floods, and other types of cyberattacks.

## DNS SECURITY



With Infoblox Advanced DNS Protection, your business is always up and running, even under a DNS-based attack. Infoblox ADP blocks the widest range of attacks, such as volumetric attacks, NXDOMAIN, exploits and DNS hijacking. Unlike approaches that rely on infrastructure overprovisioning or simple response-rate limiting, ADP intelligently detects and mitigates DNS attacks while responding only to legitimate queries by using constantly updated threat intelligence, without the need to deploy security patches.

To learn more about how PenteseC's Services can benefit your business, contact us today:

**Call** 0845 519 1337 **or Email** [sales@penteseC.com](mailto:sales@penteseC.com)

## INCIDENT RESPONSE

### **RAPID7**

Whatever your incident response needs, Rapid7 offers proactive and reactive services to give you the confidence to remain cool, calm, and collected while managing a potential crisis. From incident management to detection and analysis, Rapid7's Incident Response connects you with the best consultants to start you on the path to better protection.



Check Point Incident Response is a full-featured service to help you immediately respond to a cyberattack. After full containment, Check Point work with you to strengthen your cybersecurity controls to thwart further attacks.



Palo Alto Networks Incident Response is provided by Unit42 which provides access to one of the world's largest and most experienced threat intelligence teams. PAN's team of more than 200 cyberthreat researchers includes threat hunters, malware reverse engineers and threat modelling experts who enable you to apply a threat-informed approach to prepare for and respond to the latest cyberthreats.



## PENTESEC MANAGED SERVICES

### Managed SIEM

Designed to identify unauthorised access from external and internal threats, our service highlights suspicious activity, helps you to rapidly identify threats and provides you with visibility into your users, devices and potential attackers.

Managed SIEM helps businesses address pain points such as lack of visibility, alert fatigue and slow response times. We deliver key security outcomes for our customers ensuring that the technologies, processes and people are aligned to achieve your business' security goals.

### SOAR-aaS

SOAR-as-a-Service lets you integrate your existing security controls (where they might not previously have been able to integrate), automate processes and activities, allowing your team to triage and investigate alerts at machine speed - reducing the risk that you'll miss something in the onslaught of data you collect. PenteseC Automation gives you the upper hand when it comes to detecting and responding to threats or breaches that could impact your business systems, across the enterprise environment.

### Managed Detection and Response

Designed for organisations seeking a lightweight, automation-first, enterprise-grade solution, PenteseC MDR excels in prevention, detection, response and threat hunting across endpoints, cloud and IoT. We provide enterprises with the visibility, analytics and AI-driven automation needed to protect against known and unknown threats, detect and hunt malicious actors and remediate endpoints at machine speed.



## PENTESEC MANAGED SERVICES

### Managed Vulnerability Management

Designed to help you identify, assess, prioritise and protect assets within your security infrastructure, Managed VM provides you with a deeper understanding of risk. You will be able to align to common goals across your security/IT teams, gain accountability from technical teams and a genuine reduction in risk and accelerated achievement of goals and greater support from leadership as a result. With the help of our service, YOU can easily prove the efficacy of your security program.

### Managed Firewall

Managed Firewall Complete service provides administration, monitoring and maintenance of firewall infrastructure, freeing you from policy management, upgrades and patch deployment and allowing you to focus on what really matters. Whether your firewalls are based on premise, in the cloud or you operate a hybrid environment, we provide an industry-leading service and skillset that enhances your overall security posture, while saving you time and money.

### Hosted Management

PenteseC's Hosted Management Service is designed for 'Ultra High Availability', which means you are no longer vulnerable to hardware, power or configuration failures that lock your team out of your management gateway and prevent you from making Firewall changes.

We utilise multiple UK Based data centres located in different areas, to ensure our service is always live. Our expert engineers monitor performance 24×7, delivering patches and upgrades on your behalf and making regular policy and database backups to enable you to roll back any unsuccessful or damaging changes made.

## PENTESEC MANAGED SERVICES

### Managed Intrusion Prevention Service

PenteseC's Managed Intrusion Prevention secures your network against known threats and prevents them from exploiting any known vulnerabilities. We define, design and deliver best fit IPS policies after thorough analysis of your existing setup allowing you to maintain a strong security posture. With weekly profiling of new signatures and emergency patching of critical signatures, our expert team will ensure you're not at risk.

### PenteseC Plus Support

PenteseC 'Plus' support is a phone-based support service, providing industry leading Check Point Certified support.

PenteseC make a strong commitment to regular training of our support staff, removing the need for 1st line support all together, ensuring our customer get access to highly skilled engineer on their first call.

