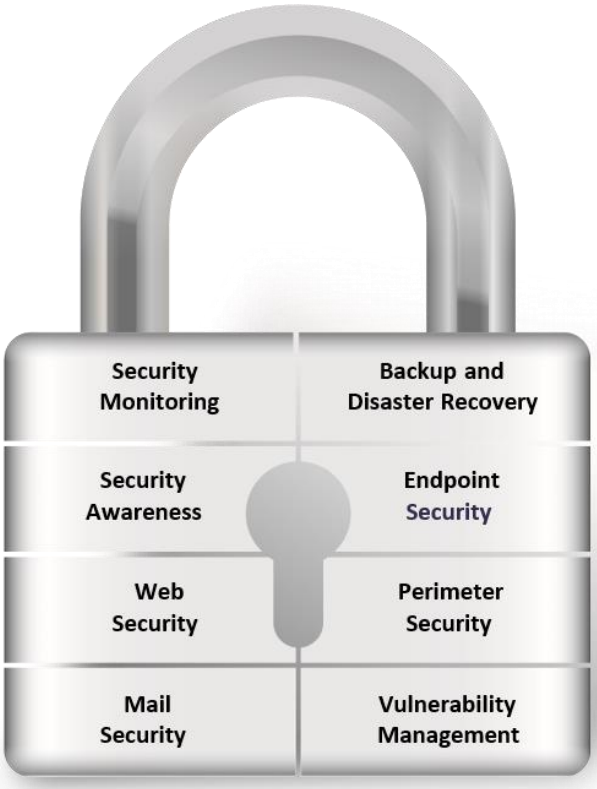
aptronics

# MANAGED SECURITY AS A SERVICE (MSAAS)




8 SECURITY SERVICES

**= 90% COVERED**

Adopting an 'it'll never happen to me' approach is tantamount to going skydiving without a parachute, and handing the task of cybersecurity over to IT teams that lack the specialist skills and security certifications is just as risky.

Managing multiple point products and technologies across an ever expanding corporate landscape has become an all-consuming task for resources already stretched thin by budget and skills constraints. Today's IT teams need managed solutions and services that can easily integrate with other existing technologies in a cost-effective manner to handle all aspects of cybersecurity on their behalf.

*MSaaS offers tangible benefits for your business by helping to:*

•Cut through the hype and track what matters most to your business without implementing unnecessary controls.

•Assess overall security posture and prioritise immediate areas that require attention to strengthen cyber readiness.

•Understand the security landscape with planning and strategy development tailored to your organisation's exact requirements.

•Enhance overall security posture with the right combination of controls and cultivate built-in resilience to enable efficient post-event recovery.

*Reinventing cybersecurity*

MSaaS is a model that provides cybersecurity solutions and skills on-demand, assuring your organisation benefits from having access to the right skills and the right levels of protection at the right time, to free up its own resources.

To solve more than 90% of all cybersecurity threats we've identified eight key areas that organisations need to have in place. Delivered as a fully-managed service, these cybersecurity offerings will form an effective security backbone from which the remaining 10% of threats and challenges can be addressed with a customised, tailored approach.

Our offerings within the Managed Security as a Service Model:

**Endpoint Security as a Service**

Superior, multi-layered endpoint protection on demand to stop threats regardless of how endpoints are attacked

**Perimeter Security as a Service**

Next-generation firewall capabilities to protect internal information assets from cyber threats.

**Vulnerability Management as a Service**

Ongoing proactive mitigation and prevention of exploitation of IT vulnerabilities that exist within a system or organisation.

**Mail Security as a Service**

Cloud-based email security and compliance solution that protects against malware, spam and data leakage to improve security and mail performance.

**Web Security as a Service**

Formidable internet security solution that delivers total visibility into network connections and protects against known and unknown web-borne threats.

**Backup and disaster recovery as a service**

Reliable backup, recovery and replication of all cloud, physical and virtual workloads with rapid disaster recovery for assured business continuity and information security

**Security Awareness as a Service**

Effective people-oriented security awareness education and training to minimise the exposure of information assets by employee action, whether deliberate or accidental.

**Security Monitoring as a Service**

Cost-effective 24x7x365 security operations centre (SOC) service to identify threats, mitigate risk and enable compliance.

## Endpoint Security as a service

Endpoint security is no longer just about antivirus. Instead it is a combination of sophisticated security controls that work together to deliver all aspects of endpoint threat mitigation. A comprehensive, well-coordinated, endpoint security strategy is a key foundational control to ensure organisational protection and minimise risk exposure.

The managed Endpoint Security as a Service from Aptronics allows you to empower your IT department to focus on their core mandate, switch up their productivity and achieve more with space to innovate.

Powered by Symantec Endpoint Protection (SEP), this service delivers superior multilayer protection for your endpoint devices against cyber hazards that threaten the confidentiality, integrity and availability of business assets. We'll take care of the day-to-day business of endpoint security, so your organisation can focus on driving theirs.

## Key features of Endpoint Security as a Service

Shrink the company's exploitable attack surface to the smallest possible footprint, which reduces business, technical and operational risk.

Access to a team of security professionals to enroll devices and protect corporate environment

Simplified process of on-boarding, managing and protecting users on any endpoint.

Maintain a proactive security stance with the ability to detect and prevent advanced threats and mutating malware, regardless of their endpoint attack.

Provide reporting, health checks, incident management and security maintenance.

## Perimeter Security as a service

In the digital age of cybercrime every single connection is a risk and cyberattacks can come from anywhere, including your own organisation.

The explosive growth of devices, the internet of things (IoT) and cloud services adoption have only made things trickier.

A comprehensive, well-coordinated, perimeter security strategy is one of the key foundational controls to ensuring organisational protection and minimising risk exposure.

*Reinventing cybersecurity for effective perimeter protection*

Old ways won't protect against new threats but you can give your organisation the upper hand in the crusade against cybercrime by bringing in the right skills at the right time with our Managed Perimeter Security as a Service offering.

**Delivered through our Cyber Defence Centre, using highly skilled resource Perimeter Security service provides**

Unmatched multi-layered security

High performance resource optimisation

Intelligent defense against malware and emerging threats

Single pane of glass management console

## Vulnerability Management as a Service

Software defects. Flawed account management practices and unsecure configurations are just a few of the biggest security vulnerabilities that can easily be exploited by cyber attackers. These vulnerabilities affect nearly every technology system, application or data point imaginable, whether old or new.

**Identify** – Defining business requirements by identifying assets to be scanned.

**Classify** – Making sense of vulnerability data in the environment.

**Remediate** – Prioritising remedial action to respond to vulnerabilities.

**Mitigate** – Ongoing policy and procedure enhancement to reduce future risk.

Nothing is immune and cybercrime incidents are skyrocketing. Fortunately, a comprehensive, well-coordinated, vulnerability management programme is one of the key foundational controls that can help proactively identify, mitigate and prevent the exploitation of IT vulnerabilities while helping to achieve statutory and regulatory compliance to minimize risk exposure.

Our skilled professionals will assist your organization in reducing its attack surface to the smallest possible footprint, providing an end-to-end service that handles all aspects of vulnerability management:

## Benefits for your business:

- Meet industry and regulatory requirements with auditable processes.
- Improve your overall IT governance with ongoing discovery of active systems and devices.
- Maintain a proactive security stance by purging vulnerabilities before they're exploited.
- Reduce complex and labor-intensive tasks with automation and integrated workflows.
- Boost the agility of remediation activities and reduce business risk exposure and protect critical data.
- Lower the cost of security control by reducing the frequency and impact of incidents.

## Web Security as a Service

Existing Network security deployments are feeling the pressure from rapid adoption of cloud service and increasing use of the web. With the demands of roaming users and slew of new endpoint device types with which employees wish to access organization apps and data directly, network security has become extremely complicated.

While the traditional approach to web security won't cut it anymore, a comprehensive, well-coordinated, web security strategy is necessary as one of the key foundational controls to ensure organizational protection and minimize risk exposure.

*Reinventing cybersecurity to solve business dilemmas*

With managed internet security services offerings, your organization will benefit from real time protection against known and unknown web-borne threats.

**Delivered through our Cyber Defense Centre, this web security service covers:**

**Readiness** – We'll connect your laptop, devices, firewalls and proxies while our skilled engineers define and distribute security policies.

**Protection** – The right level of protection with turntable URL filtering, malware scanning and advanced protection.

**Monitoring** – keep an eye on internet usage, threats and incidents by users/location/application in real-time.

**Mitigation** – Reduce the likelihood of future vulnerabilities through ongoing policy and procedure tweaks to respond to user behavior and cyber security trends.

## Mail Security as a Service

Email forms a key part of any modern business but for all its benefits, email is a substantial security risk. As the number one attack vector for cyber criminals, thousands of new scams and fresh malware are deployed by criminals daily making email security a clear priority.

A comprehensive, well-coordinated, email security strategy is one of the key foundational controls to ensuring organizational protection and minimizing risk exposure.

Aptronics will deliver an end-to-end managed Mail Security service through a secure email platform. Put our in-depth understanding of local regulatory and compliance control requirements to work for your organization and reduce complexity of protecting your people and data from malware, spam and theft.

*The right protection at the right time*

Using Mimecast Email Security, the most comprehensive cloud based security and compliance solution available, we're perfectly positioned to take the load off your IT administration team.

You can rely on our managed security service to:

Mitigate risk of advanced email threats.

Protect your people against social engineering and impersonation attacks, like whaling

Neutralize weaponized attachment threats and malicious file content.

Enable effortless email encryption and secure delivery.

## Backup and Disaster Recovery as a Service

Data is the lifeblood of any business, if your organization fell victim to a cybersecurity attack, would you need to pay a ransom to keep your doors open, or would you be able to carry on business as usual, because you've got the right backup and disaster recovery plan in place? That's just security. Is your current backup and disaster recovery solution geared to address the issue of compliance?

With the General Data Protection Regulation and the Protection of Personal Information Act looming, a comprehensive well-coordinated, backup and data recovery strategy is one of the key foundational controls in ensuring organizational protection and minimizing risk exposure.

*Reinventing your perspective of BaaS and DRaaS to solve business dilemmas.*

To empower your organization with the right skills at precisely the right time without burdening your IT team with additional responsibilities for enterprise-wide backup and disaster recovery, we've reinvented our managed service offering with cybersecurity now at the core of its design.

Aptronics ia a Veeam ProParter and our certified engineers are ready to help your company:

**Backup** – meet specific backup needs while ensuring the fastest, most efficient backup possible.

**Recovery** – Recover entire virtual machines(VM) or individual files based on business needs.

**Replication** – Minimise disruption by failing over to a replica virtual machine to avoid data and productivity loss, bringing recovery time to less than 15 minutes.

## Security Awareness as a Service

Even with smartest technology in place, your company will still face significant risk if you underestimate the role people play in security, as the human element is the top contributing factor to escalating corporate cybercrime figures.

This makes a comprehensive, well –coordinated security awareness strategy one of the key foundational controls to ensure organizational protection and minimize risk exposure.

*Reinventing cybersecurity to solve business dilemmas*

People will stick to security policies and procedures if they're aware of what's at risk, and their role in maintaining security, which means they need security awareness training. But who in your organization has time to run workshops and engage with every single employee? Let us handle it, rather than expecting your IT administration to tackle such mammoth task.

**Our Team is ready to engage with your employees on a 12- month security awareness program to ensure:**

A sense of personal responsibility for information security in the business.

A culture of security based on each person's role in securing assets.

The right attitude and skills to use information assets in a secure manner.

Increase awareness of information security threats and possible business impact.

Acceptance of roles and responsibilities of securing organization-wide information.

## Security Monitoring as a Service

The Dark Web never slumbers and organisations are under constant attack from cyber criminals.

A comprehensive, well-coordinated web security strategy is one of the key foundational controls in ensuring organizational protection and minimizing risk exposure but without the right skills and massive budgets, managing the complexity of Security Information and Event Management and Log Management tools can be a fearsome task.

Similarly, extracting and applying meaningful information gathered from such security solutions is a task best left to experts.

### *Reinventing cybersecurity to solve business dilemmas*

to reinvent the way your business does cybersecurity, we've made it possible for your organization to benefit from our specialist skills and world-class technologies at a fraction of the cost, through a Security Monitoring as a Service managed offering.

Delivered through our Cyber Defense Centre, our skilled professionals provide a cost- effective subscription-based 24x7x365 security operations centre (SoC) for resource-sensitive businesses.

### *The right skills at the right time*

We can make your organization transform how threats are identified, risks are mitigated and enable compliance with a unified situational awareness platform the proactively detects threats and delivers timely, actionable insights. With certified SOC Analysts remotely managing your on-premise deployment 24/7, you'll gain the advantage of visibility, health monitoring and situational awareness without hiring the skills full-time.

### *We make cybersecurity work for you*

We're here to give your business exactly what it needs – simplified security intelligence. We'll help your organization to assess its information security stance and identify exactly what's needed to protect your business –critical services and data. Mothing more, nothing less. No unnecessary controls, just the right levels of protection at the right time.

With our eight core cybersecurity managed service offerings you're free to build your cybersecurity armor as you need it, addressing priorities now and extending protection later while keeping costs predictable and transparent.

These eight core offerings work together to protect your business against 90% of cyber threats out there. As for the other 10% our team of skilled professionals are ready to help you reinvent your organization's approach to cybersecurity with a tailored, business-specific approach to protecting your people, infrastructure and data from harm.

**Enjoy the peace of mind that comes from:**

**Continuous monitoring and incident management**
Improved network security stance with constant monitoring and notification of potential incidents before impact.

**Security reporting** – increased awareness through periodic reporting of critical controls, compliance concerns and incidents.

**Compliance automation** – Assistance from certified professionals in meeting compliance obligations around PCI-DSS, HIPAA, etc.

**Health monitoring and feedback** – Log management requirements are met and system health is regularly checked and assured.

**With the human touch** – one-on-one regular consultations with your Aptronics Security Analyst to recap security concerns and system health

Connect with us

Speak to an Aptronics consultant today to discover how our Managed Security as a Service offering can reduce costs, reduce risk and improve the compliance status of your organization.

(T) 011 577 0800

(E) info@aptronics.co.za

(W) www.aptronics.co.za