My Security Console
Managed Intrusion Prevention and Response

My Security Console

My Security Console is a white-label managed cybersecurity solution providing your customers with advanced protection against online threats and security breaches to prevent financial loss caused by viruses and malware, ransomware, unplanned downtime, and data corruption.

Expertise & Technology

Systems are actively monitored using automated analytics and live cybersecurity experts who assess threat information, alert, and support your team to quickly contain and resolve issues to keep your customer's business up and running.

Turnkey Solution

Easy to deploy. Our system requires no additional resources and no upfront costs or changes to existing firewall, anti-virus or backup solution configurations. Inserted at the network edge, the system protects against inbound threats, prevents users from accessing malicious sites, helps identify and isolate systems infected with malware able to bypass and hide from anti-virus.

Increased Revenue

Increase your monthly recurring revenue and gain a reliable, uncomplicated way to get your customers the comprehensive network security they need to operate in today's market. We provide you with the tools and resources to help you grow your earning potential without increasing your workload.

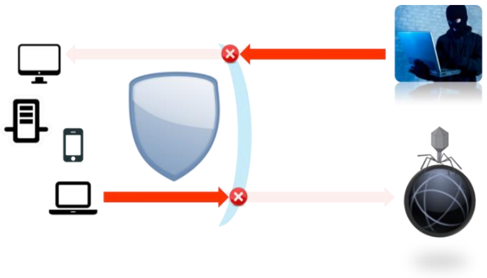
Multi Layer Defence

Advanced security algorithms continuously gather and analyze threat intelligence data from reputable information sources around the world. Our systems use this data to seamlessly update all deployed devices, arming them with the most current defence rules that dynamically block advanced threats and malicious traffic before it penetrates the network edge.

WHAT IS MY SECURITY CONSOLE?

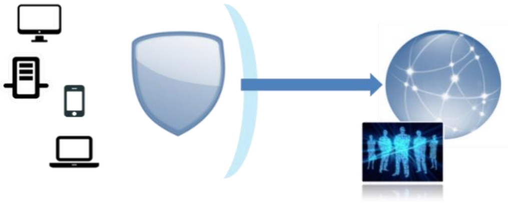
Intrusion Prevention & Threat Intelligence

Armed with the latest threat intelligence our security system blocks inbound threats and prevents users from accessing malicious sites and content. It also helps identify and isolate internal systems infected with malware that can bypass anti-virus.



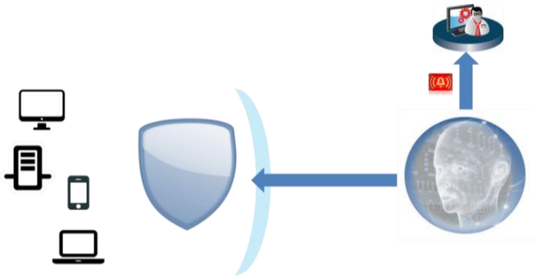
Professionally Monitored Security Service

Security information is streamed to the monitoring servers where trained cybersecurity experts analyse the information to identify issues and work with your IT staff to contain and mitigate threats.



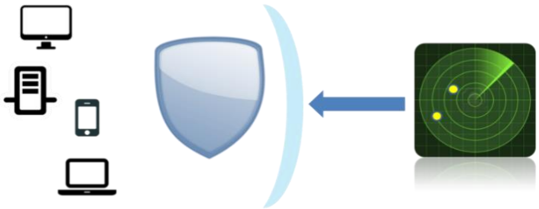
Advanced Cloud Algorithms

Advanced algorithms analyze security information to detect hidden issues and alert monitoring staff about any issues that require immediate attention.



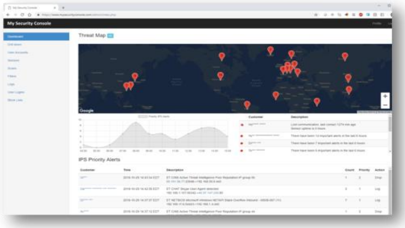
Cloud Network Scanners

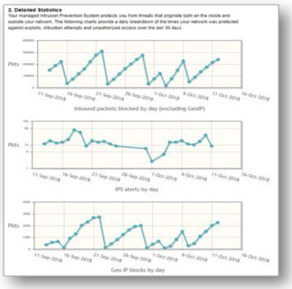
Cloud-based network scanners regularly check your network for unauthorized entry points and firewall misconfigurations.



A Management Portal

Administrator and end-user portals provide detailed security information, statistics, reports, remote monitoring and management to help keep the cybercriminals out and your business up and running.





2. Detailed Statistics

Your managed Intrusion Prevention System protects you from threats that originate both on the inside and outside your network. The following charts provide a daily breakdown of the times your network was protected against exploits, intrusion attempts and unauthorized access over the last 30 days.

WHAT SETS US APART ?

Advanced Threat Intelligence

Threat intelligence combined with advanced security features and support traditionally only used by large enterprise.

Benefit: Protect your business with enterprise grade security at an affordable price point.

Inline Intrusion Prevention

Intrusion Prevention inspects all inbound and outbound traffic to protect against known and emerging cyber security threats.

Benefit: Detect and block malicious activity outside and inside your network.

Reduced Attack Surface

Advanced firewall rules restrict traffic to and from specific countries, reducing unnecessary exposure to remote threats.

Benefit: Reduce risk by limiting the locations from which your systems can be accessed.

Live Cybersecurity Experts

The network is monitored by cybersecurity experts who assess information and offer expertise and support to IT staff to prevent issues, save time and keep your business running.

Benefit: Prevent breaches and costly downtime, allowing staff to stay focused on the day-to-day of your business.

Monitoring and Alerting

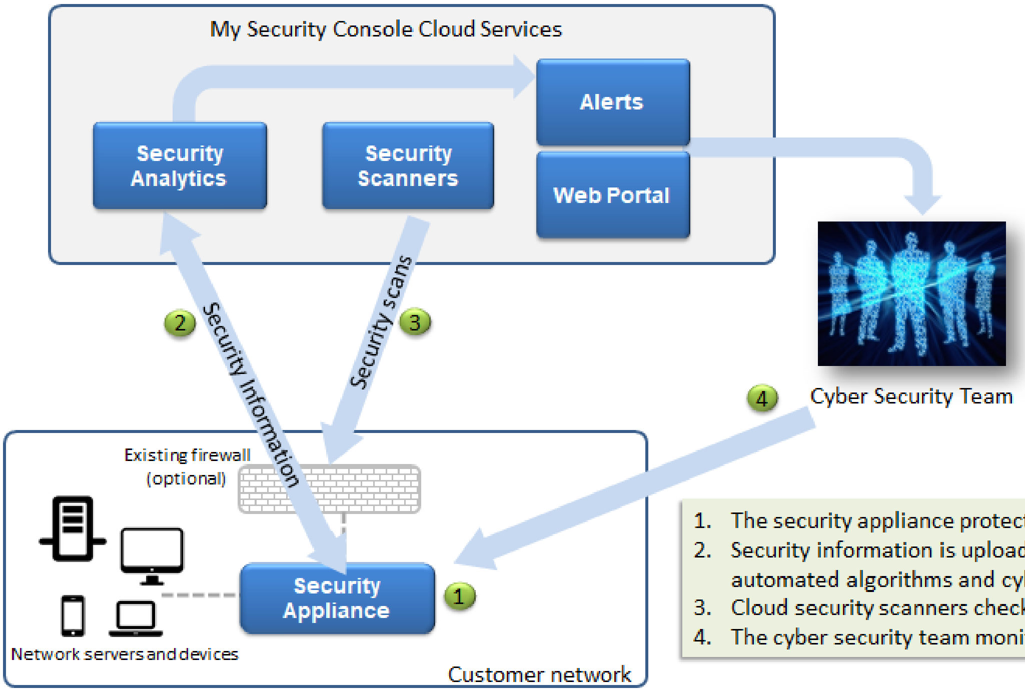
Cloud services and security experts continuously monitor your systems. Alerts and notifications enable rapid response to critical events and isolation of infected systems.

Benefit: Quickly respond to critical threats and minimize the impact of potential security breaches.

Remote Scans

Cloud security scanners check external access to your network, protecting it from unauthorized access due to incorrect security policies or configuration errors.

Benefit: Prevent breaches caused by human error and common firewall misconfigurations



1. The security appliance protects the network
2. Security information is uploaded to the cloud for analysis by automated algorithms and cyber security experts
3. Cloud security scanners check the network for issues
4. The cyber security team monitors systems and resolves threats

FEATURES

Feature	Benefit
Network Security Appliance	Stop threats at the network level and protect all your devices including servers, desktops, laptops, mobile phones, tablets, servers, printers, and surveillance cameras.
Inbound Intrusion Prevention	Inspect all inbound network traffic to detect and stop threats from the Internet attempting to get into your network.
Outbound Intrusion Prevention	Inspect all outbound network traffic to prevent users from accessing malicious content on the internet and detect suspicious activity on your network.
Country-based blocking	Customize network rules to allow or deny traffic from specific locations.
Malicious IP blocking	Custom malicious IP list blocks network traffic to and from known malicious IP addresses to protect all your devices from known hostile systems.
External Network Scanning	External network scans detect open ports that may allow hackers access to the network or the systems connected to it.
Curated Intrusion Prevention Rules	Custom Intrusion Prevention rules inspect all network traffic to detect and prevent threats at the network level.
Honeypot	Detect viruses and other threats attempting to spread to other systems on the network to stop hackers in their tracks.
Live Monitoring	Monitored by trained cybersecurity experts to detect malicious activity and alert IT staff to critical security issues.
Endpoint Security	An optional secure endpoint agent allows compromised hosts to be rapidly isolated from the network preventing hackers from using an infected machine as a springboard to attack other systems.
Threat Intelligence	Customers are provided with regular reports and updates on the security status of their network and provided with important information on latest threats and how to stay safe.

FREQUENTLY ASKED QUESTIONS

Many businesses already have a firewall, why is this needed?

Most firewalls only support very simple policies for securing network traffic and do nothing to prevent computers inside your network from connecting to malicious servers on the internet. When someone is tricked into clicking on a malicious link, your firewall will not stop that computer from connecting to servers controlled by hackers and downloading viruses or other malware disguised as a PDF file or other content.

When you forward ports in your firewall, in most cases those rules apply to everyone on the internet: the same policy that allows your IT administrator remote access through the firewall also gives hackers access to those same ports.

The security sensor includes a mature and robust Intrusion Prevention engine that scans all inbound and outbound traffic for threats. Detailed rules can be created to define what traffic is allowed in and out of the network including restrictions by geographic location. The cloud security scanners regularly scan the network to look for open ports that could provide hackers with unauthorized access.

Users already have anti virus, why is this needed?

Anti-virus is a critical component of a robust cyber security strategy. Unfortunately, while anti-virus solutions prevent many attacks, hackers are constantly adapting their approach in what has become a never ending cat-and-mouse game between anti-virus vendors and cyber criminals.

Once a hacker is able to trick a user or bypass anti-virus software and install a Trojan or backdoor, they own your network. They remotely control infected systems to explore your network, infect more systems, encrypt your hard drives, steal your business and client information and copy your files to their servers, allowing them full access to your infrastructure. Your antivirus isn’t looking for such activity and does nothing to prevent it.

The network security appliance includes advanced Intrusion Prevention capability with rules that are updated regularly by a large community of open source and corporate cyber security professionals. These rules monitor network traffic for patterns that are known to be associated with specific attacks, blocking the network activity and alerting the cybersecurity team to take the appropriate defensive countermeasures.

Do clients need to replace their existing firewall?

Customers can continue to use an existing firewall that provides basic network security policies along with the enhanced security capabilities provided by the security appliance and cloud services.

The security appliance can be installed in the network in “transparent mode” either in front of the existing firewall or behind it, significantly enhancing security capabilities with features such as Intrusion Prevention, Geo IP security policy enforcement, external vulnerability scanning and automated cloud monitoring & alerting.

FREQUENTLY ASKED QUESTIONS

Is anti-virus still needed?

Yes, anti-virus should still be used on all endpoints including desktops, laptops, tablets, and mobile phones.

A proper security strategy consists of multiple layers of protection. That includes network layer security provided by the security appliance as well as endpoint security which is provided by anti-virus.

The two technologies are complementary and together provide the best possible protection against different types of vulnerabilities.

Clients have anti-virus and still got infected, would this have helped?

My Security Console provides an additional layer of security that may have been able to detect and stop the attack. It contains thousands of rules that are constantly being updated by an army of cyber-security specialists and automated algorithms, allowing it to protect your systems against a huge number of attacks and vulnerabilities. Hackers are always finding new ways to bypass security systems. The best strategy is to use a layered approach to security that includes the right mix of technology and human expertise to protect your business.

Who monitors network security?

Our trained cybersecurity experts monitor systems through the available security portal and cloud services to quickly identify and address any issues that may be detected.

In addition, security analytics servers and network scanners continuously collect and analyze data from security appliances. Critical events that require immediate attention generate alerts sent to our cybersecurity team and your client-facing IT security staff.

How do I know if there is a security incident?

The solution generates automated alerts and our cybersecurity experts will notify your IT security staff of any security threats and countermeasures that should be put in place or actions that need to be taken.

Does My Security Console include endpoint protection?

My Security Console includes an optional endpoint agent that allows the cybersecurity team to rapidly isolate infected systems from the rest of the network. This prevents a PC that has been breached by hackers from being used as a springboard to infect other systems on the network and access or encrypt any information they contain.

What do you mean by Advanced Threat Intelligence?

My Security Console servers continuously collect information about new and ongoing threats from a variety of reputable third-party sources around the world and from our own cloud analytics engine. This information is combined into a set of rules that are used by advanced Intrusion Detection and Prevention engines to block malicious traffic based on a number of factors including IP address, URL, TLS certificate fingerprint, traffic behaviour, and network packet payload.