MY SECURITY CONSOLE

Managed Intrusion Prevention

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 and unplanned downtime and data corruption.

Expertise & Technology

Systems are actively monitored using automated cloud analytics and real cybersecurity experts who assess threat information and alert and support your team to quickly contain and resolve issues and 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 and helps identify systems infected with advanced 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.

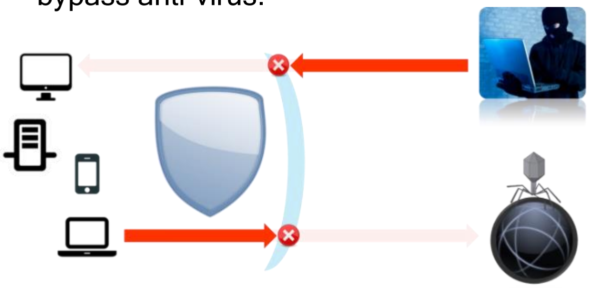
Multi Layer Defence

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 internal systems that are infected with malware that is able to bypass anti-virus.

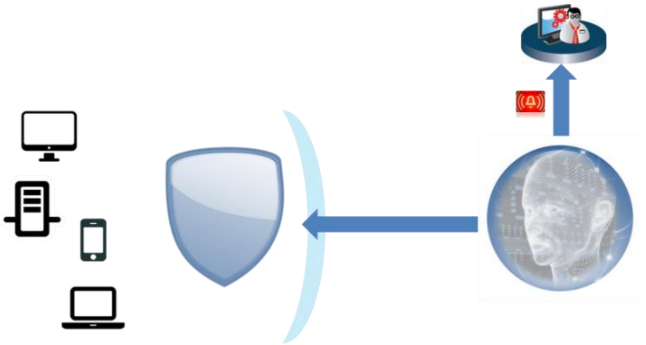


Professionally Monitored Security Service

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.

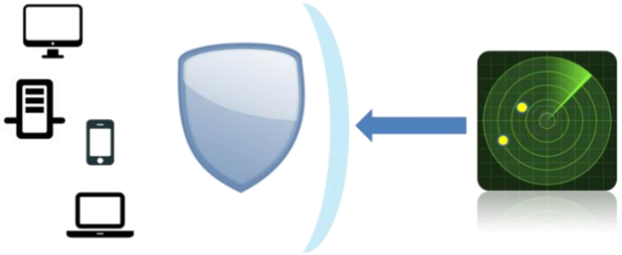
Advanced Cloud Algorithms

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



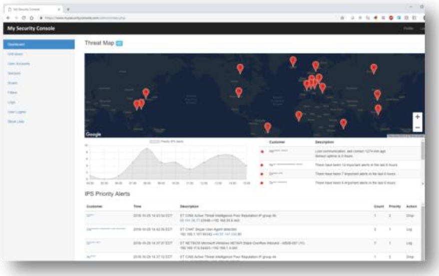
Cloud Network Scanners

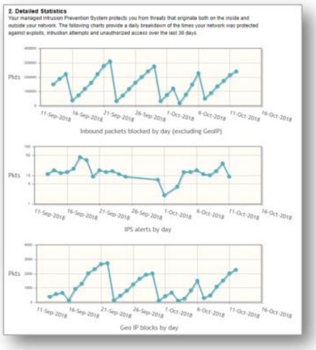
Cloud-based network scanners regularly check your network for unauthorized entry points and firewall misconfigurations.



A Management Portal

Administrator and end-user portals provide detailed security information, statistics, reports, remote monitoring and management to help keep cybercriminals out and your customer's 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?

Multi Layer Threat Intelligence

Each device is continuously updated with the most current threat intelligence gathered from information sources worldwide.

Benefit: Arms devices against malicious traffic before it penetrates the network edge.

Inline Intrusion Prevention

Advanced cybersecurity systems inspect all network traffic to protect against known and emerging cyber security threats.

Benefit: Detect and block malicious activity outside and inside the 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 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

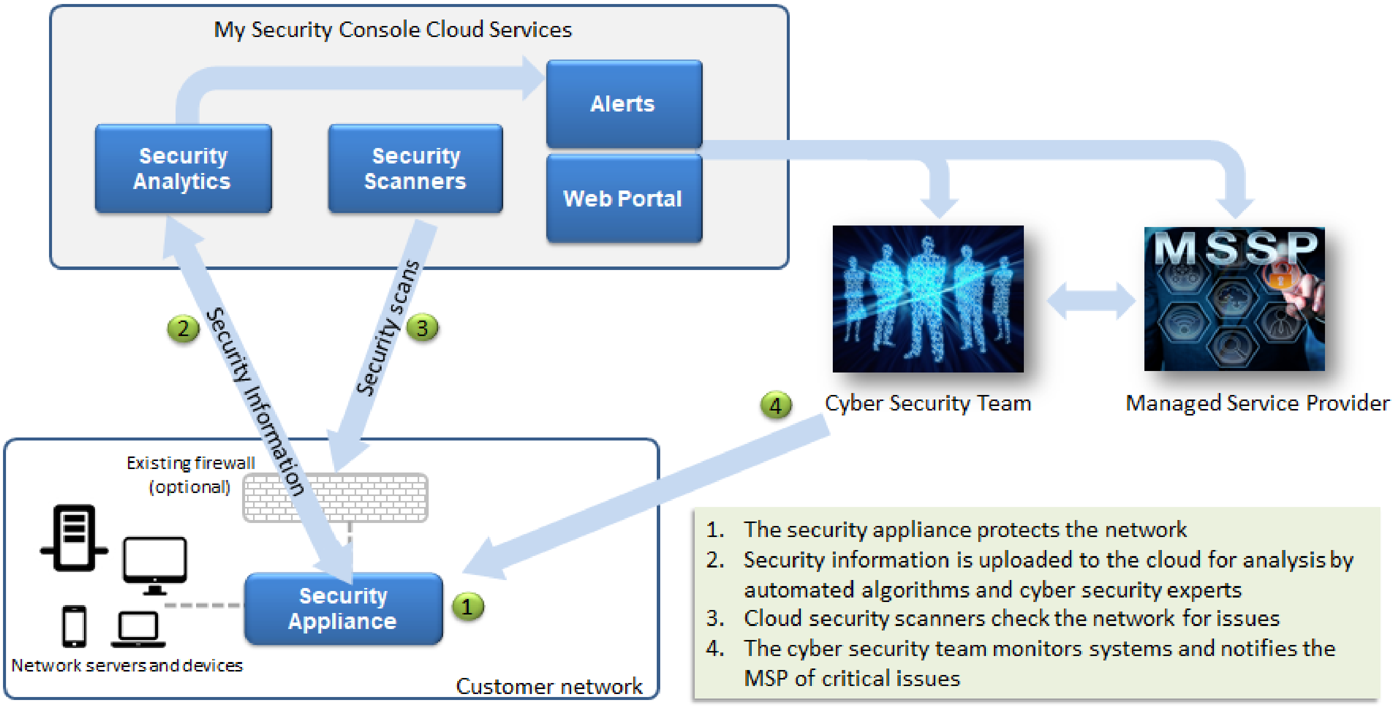
Cloud services and security experts continuously monitor your systems. Automatic alerts and notifications enable rapid response to critical security events.

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 notifies the MSP of critical issues

COMMONLY 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 the network from connecting to malicious servers on the internet. When someone is tricked into clicking on a malicious link, a 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 a remote worker to access systems through the firewall also gives hackers the same access.

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.

Most users already have anti-virus, why is this needed?

Anti-virus is a critical component of a robust cybersecurity 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 with many instances of malware now able to bypass and remain hidden from anti-virus.

Once a hacker is able to trick a user or bypass anti-virus software and install a Trojan or backdoor, they own the network. They remotely control infected systems to explore the network, infect more systems, encrypt hard drives, steal business and client information and copy files to their servers, allowing them full access to the IT infrastructure. Antivirus isn't looking for such activity and does little 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.

COMMONLY ASKED QUESTIONS

Is anti-virus still needed?

Yes, anti-virus should still be used on all of 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 complimentary and together provide the best possible protection against different types of vulnerabilities.

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

The security appliance provides an additional layer of security that may be able to detect and stop attacks that bypass anti-virus systems. It contains thousands of rules that are constantly being updated by an army of cybersecurity specialists allowing it to protect 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 the 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 to that, 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 client-facing IT security staff of any security threats and countermeasures that should be put in place or actions that need to be taken.