My Security Console
Managed Intrusion Prevention and Response

My Security Console

A managed cybersecurity solution that provides advanced protection against online threats and prevents financial loss caused by security breaches, unplanned downtime, and data corruption.

Expertise & Technology

Systems are actively monitored using automated analytics and **live cybersecurity experts** who assess threat information and support IT personnel to quickly contain and resolve issues and keep your business up and running.

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.

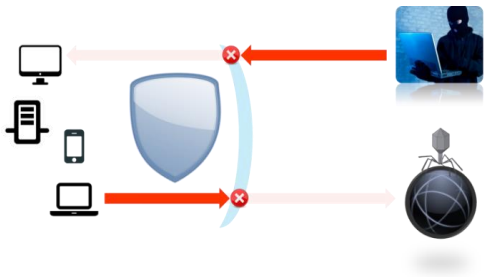
Cost Savings

Getting security right takes time and expertise. Getting it wrong can result in costly breaches, ransomware and lost revenue due to unplanned downtime. Our cybersecurity solution and experts solve this problem by taking on the cybercriminals allowing you and your staff to focus on the projects and activities that drive your business.

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.

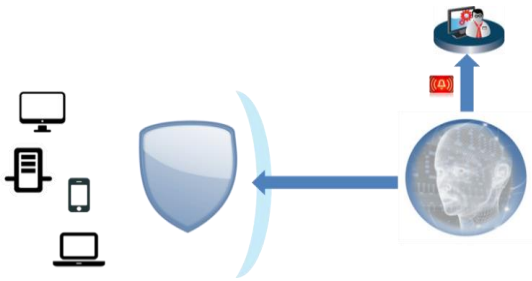


Professionally Monitored Security Service

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.

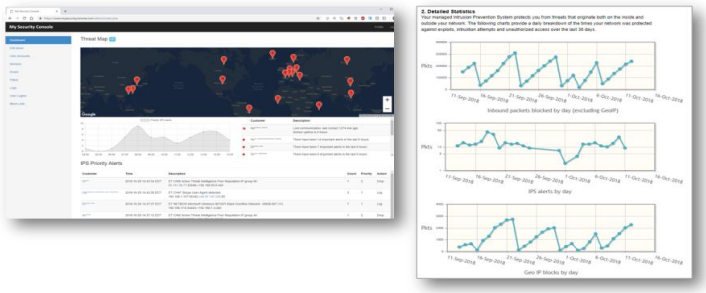


Cloud Network Scanners

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.



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

Your 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

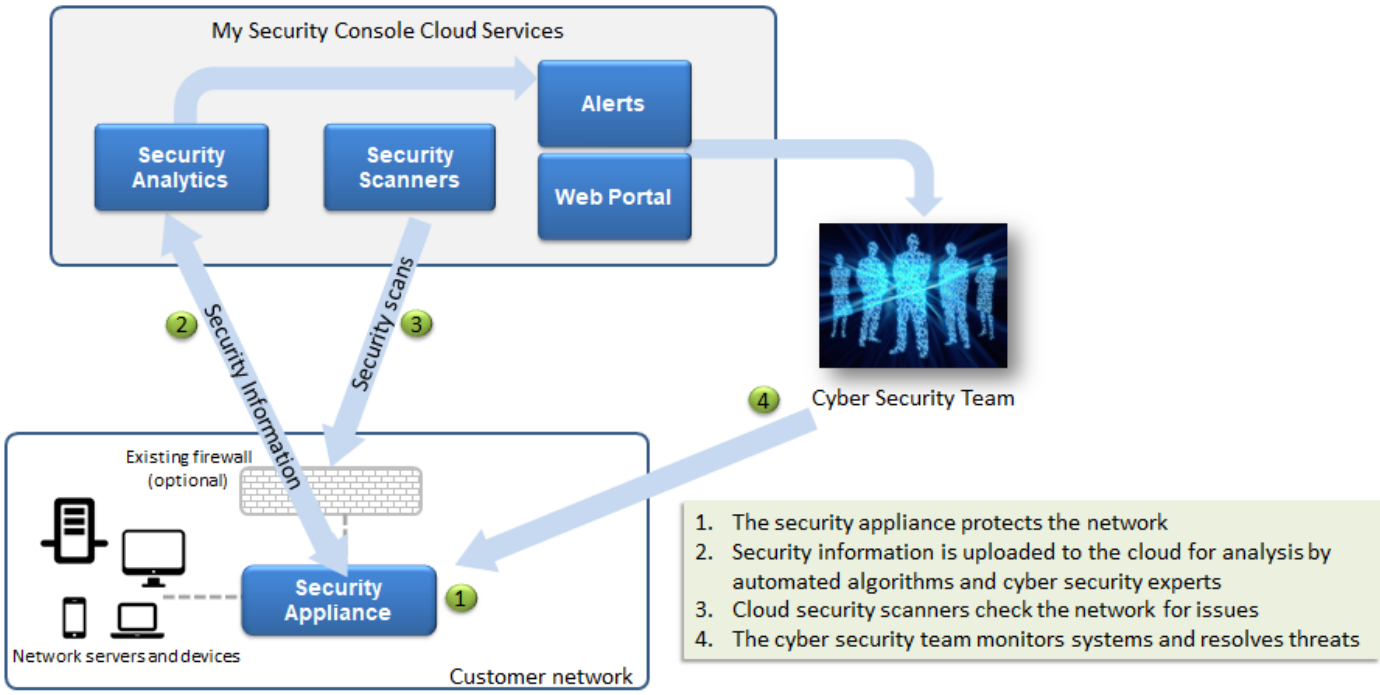
Cloud services and security experts continuously monitor your systems. Automatic alerts and notifications enable rapid response to critical security events.

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



FREQUENTLY ASKED QUESTIONS

I already have a firewall, why do I need this?

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

I already have anti-virus, why do I need this?

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 cyber security professionals. These rules monitor your 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 I need to replace my existing firewall?

If you already have a firewall protecting your network you've taken an important step in protecting your infrastructure. You can continue to use your existing firewall that provides basic network security policies along with the enhanced security capabilities that are part of the My Security Console solution.

If needed, the security appliance can be installed in your network in "transparent mode" either in front of your 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 and alerting.

FREQUENTLY ASKED QUESTIONS

Do I still need anti-virus?

Yes, you should still use anti-virus on all of your endpoints including desktops, laptops, tablets and mobile phones.

A proper security strategy consists of multiple layers of protection; that a includes network layer security which is provided by My Security Console, as well as endpoint security which is provided by your anti-virus.

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

I 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 network and 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 my network security?

Security analytics servers and network scanners continuously collect and analyze data from your security appliances. Our cybersecurity team also monitors your systems through the available security portal to quickly identify problems and work with your IT personnel to address any issues that may be detected.

How do I know if there is a security incident?

Our cybersecurity team monitors your systems and advanced analytics servers automatically generate SMS and Email alerts for critical issues they detect. We will notify you of security threats and any countermeasures that should be put in place or actions that should 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 your 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 is 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.