The Rise of Cybersecurity

Design your cybersecurity strategy with Network Critical to protect and secure your network

Network Critical

The Window to your Network™

Contents

The Market and Its Threats

By the end of the decade, the worldwide cybersecurity market is expected to surpass US$ 300 billion. Because of the heightened attention on securing information in the wake of high-profile data thefts and breaches, cybersecurity is becoming a strategic requirement for enterprises. As it becomes more difficult to keep up with the rise in cybercrime and malware attacks on healthcare companies, governments, and education institutions, global spending on cybersecurity is increasing, often in exaggerated numbers that provide no guarantees. With the growing use of the Internet in both emerging and developed countries, cybersecurity solutions are expected to become more popular, however not always effective. Furthermore, the growing wireless network for mobile devices has increased data susceptibility, making cybersecurity a must-have for any company throughout the world.

A cyber-attack such as ransomware has a major human component. It takes advantage of system flaws along with psychological tactics such clicking phishing emails and extortion. Dealing with ransomware requires strategic planning as much as cyber tools.

Facing new challenges post-pandemic

With the COVID-19 pandemic, organizations needed to adapt to a new operational paradigm in which working from home has become the “new normal”, bringing new challenges to network security strategy. Businesses are speeding up their digital transformations, and cybersecurity has become a big worry. Following the COVID-19 outbreak, an increase in cybercrime has been reported in different organizations and ransomware has become one of the biggest menaces.

Ransomware attacks are more organized, targeting vulnerable industries such as healthcare, financial and educational institutions where the loss of services or data has devastating repercussions. Making it clear that no one is exempt, regardless of the size of the company or the industries to which they belong, everyone can be a victim of cybercrime. As a result of the increase in sophisticated cyber-attacks, enterprises have been urged to implement strict cybersecurity measures such as zero-trust security models and a multi-layered cybersecurity plan, supporting market growth.

The Objectives

It's clear that cybersecurity is a very present threat in today's technical world and because of this, the majority of network and security teams have a Cybersecurity Implementation Plan. However, whether this plan's objectives are actually being met is another threat in itself. To ensure your network management and network security teams fulfil a comprehensive cybersecurity initiative, follow this rule of 5:

1. Prioritize your network protection and indentification techniques
2. Implement prompt detection and swift response to cyber incidents
3. Achieve low recovery times from incidents and learn from the analsys
4. Effective deployment of existing and next-generation technologies
5. Prevention measure from the inside

Network Protection and Identification

Before we start thinking about protection and identification, lets get aquainted with what we need to protect from.

Here are the main four:

HUMAN ERROR

Keep up with regular training and testing of your human resources to minimise threat from human errors.

We recommend training and testing once a month.

EVOLVING THREATS

With a range of threat type, from organized, connected, persistent and unpredictable crime, a suitable plan needs to be in place to protect the network and identify the threats.

We recommend having a unique strategy for each threat type.

EXPANSION of ATTACK SURFACE

Everything is going online resulting in networks experiencing rapid growth. Is your network protection able to grow with your network?

With IoT and 5G, we recommend you implement protective technologies that can keep pace with your network.

BIG DATA

Big data isn't getting smaller. Our networks need to have sufficient protection and must have the ability to identify threats, no matter how big our data pools are.

We recommend having network monitoring tools that can see into 100% of your network.

Prompt Response to Incidents

The problem is that you cannot protect what you cannot see. Without monitoring the right tools to see the all the traffic, the security, speed, cost, and efficiency of your network are compromised.

The SmartNA™ range at *Network Critical* have lightning speed detection to incidents that you can't afford to have delayed. These solutions enable you to achieve the lowest response times to your cyber incidents and achieve your cybersecurity objectives.

SmartNA™

SmartNA-XL™

SmartNA-PortPlus™

SmartNA-PortPlus HyperCore™

The SmartNA™ range offer high quality core features:

- Zero packet loss with total traffic capture
- Load-Balance traffic to multiple monitoring and analysis tools
- Intelligent aggregation of traffic from multiple Network TAPs or SPAN ports
- Single pane-of-glass GUI, Drag-n-Vu™
- Rule optimisation engine calculates all filter rule interaction automatically
- Intelligent traffic filtering, ensuring that security and monitoring tools see all the data you need
- Application layer visibility allows for efficient packet processing on individual L7 protocols

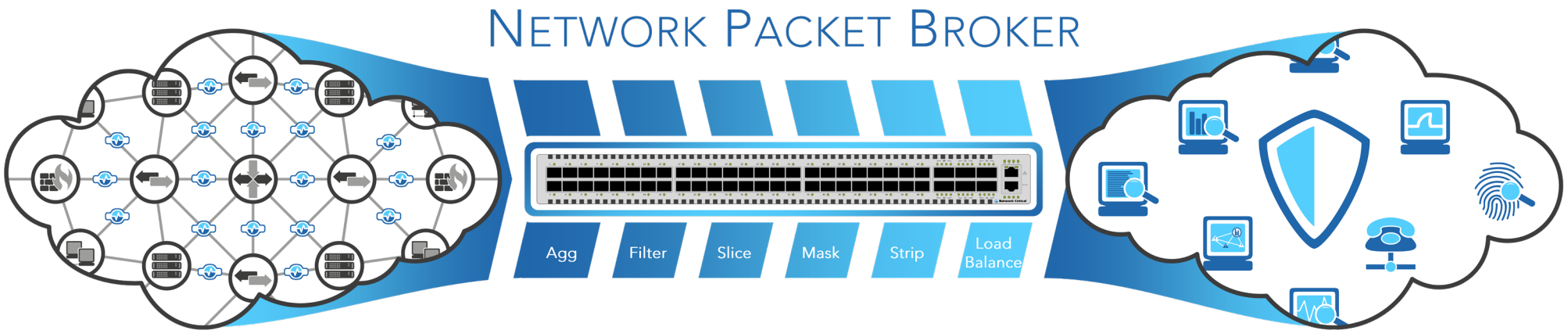
The Right Solution To Secure Complete Network Visibility

Our Network TAP range allows for complete, **100% visibility**, into your network. So you can be alerted, in real-time, on any and all issues that your network may be facing.

Network Packet Brokers are able to reduce resource waste, costs and of course, possibilities of hacking. This is because NPBs can apply specific rules and filters before they forward the traffic to your various network tools, such as performance management, network security, and other monitoring tools.

The *'Broker'* in Network Packet Broker refers to its ability to combine, integrate, separate, manipulate and process inputs from many sources, delivering the data to a wide variety of appliance and tool destinations. Delivering the right data to the right tool will optimize security and performance.

Network Critical's **SmartNA™ Network Packet Broker** range are hybrid, so in 1RU device, you get both Network TAP technology as well as Packet Broker technology. This makes our packet brokers highly effective in saving costs, and rack space.



Recovery Times

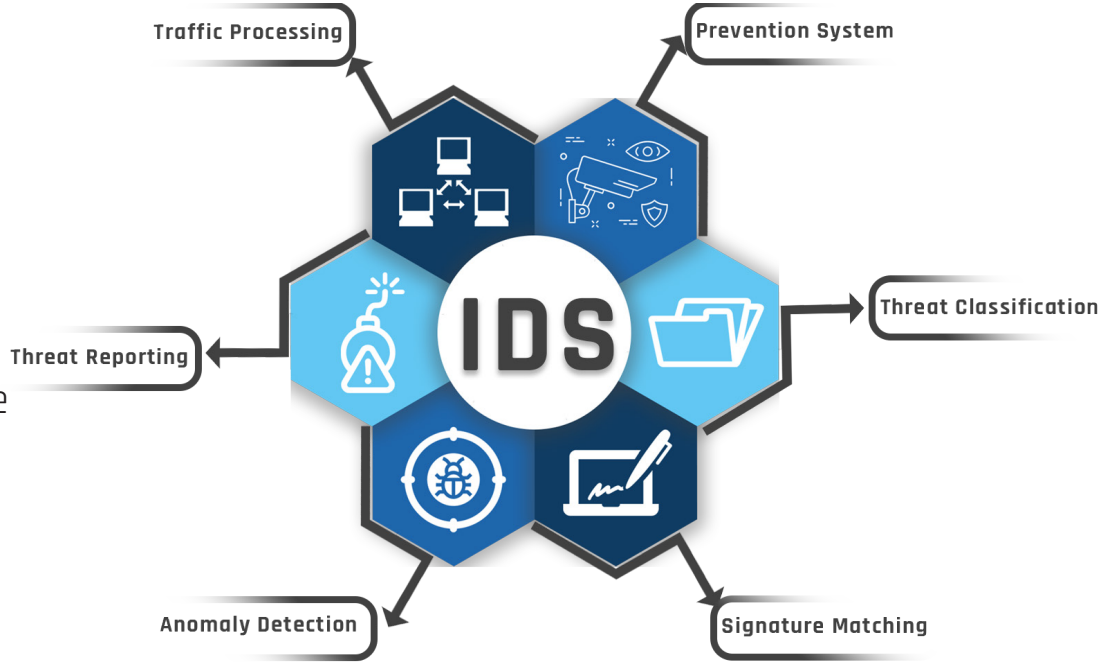
With the SmartNA Bypass TAPs you can have ultra-low recovery times with failsafe technology. The Bypass TAP with consistent heartbeats can be implemented alongside Inline monitoring tools, to add a layer of protection.

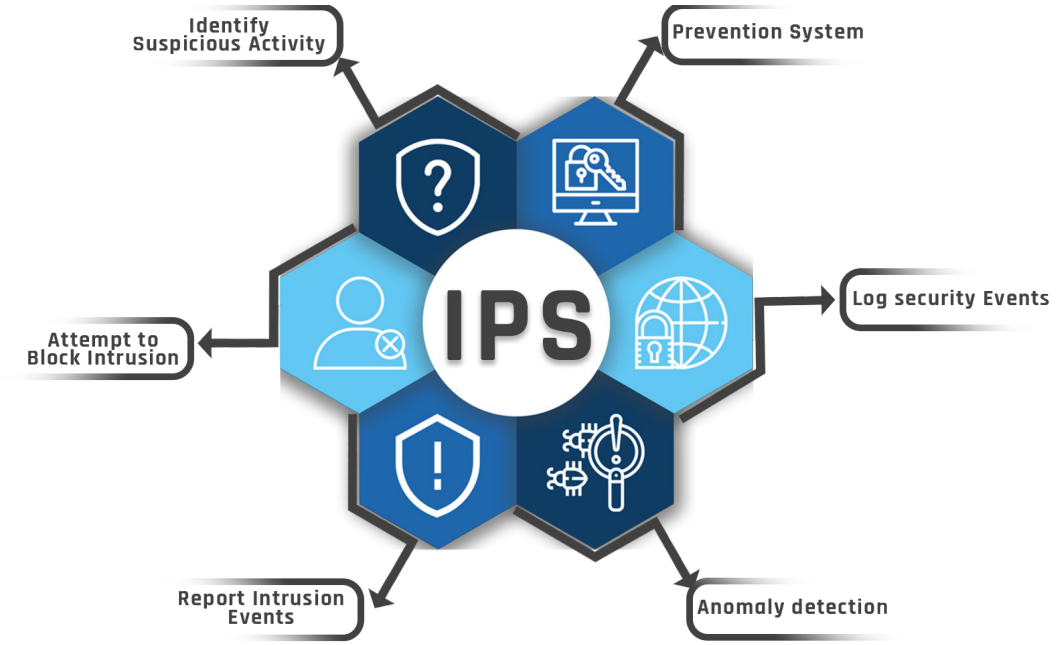
If the monitoring tool suffers a problem, our Bypass TAP will reconnect the active network link ensuring that network traffic flow is maintained, minimizing traffic loss, and achieving a rapid recovery.

Learn from Analysis

After a thorough examination of your network traffic, the data can reveal valuable insights that will give your business a better understanding of your network's performance and security. If an issue is detected, the data gathered will help your team to address it.

As a result, total network visibility is required to deliver all of your network traffic to the monitoring tools. You can use it to examine real-time data and respond to problems as they arise. However, it is also vital to incorporate historical data in the analysis, as this will provide information about precedent incidents that will aid in the detection of a current threat to your network.





Our products provide your security systems with complete, uncompromising visibility into your network. You will find that this helps to keep pace with increasing network speed and complexity, while gaining the insight needed to better detect and contain breaches.

With the SmartNA™ range of packet brokers you can filter the traffic sending it to the monitoring tools to be analyze, enhancing your IPS (Intrusion Prevention System) and IDS (Intrusion Detection System).

Existing and New Technologies

You'll be wanting to deploy existing and next-generation technologies to achieve your cybersecurity objectives too. *Network Critical*'s next-generation network packet broker, the **SmartNA-PortPlus HyperCore™** is a new and superior technology that is suited to evolving, growing and futuristic 5G networks, with speeds up to 400Gbps.

Network Critical's packet broker optimizes network infrastructure without compromising operations or security.

Key Features

- High density, high performance and scalable. Network and server ready base unit 32 x 10/25/40/50/200/400G interfaces
- Non-blocking architecture, **Line Rate System Throughput 12.8 Tbps**
- Aggregate, Filter and Load Balance core network traffic across existing and future tool portfolio
- Custom P-Tag functionality enables complex traffic processing workflows
- **Programmable architecture** purpose-built to support **workload density**, emerging protocols and **new technologies**

Benefits

- **Scalable to 256 ports** of 10/25/40 and 50G. Saving rack space and all speeds protect against obsolescence
- Performance to accommodate all network speeds
- Extends existing tool life and leverages new tool acquisition
- Pinpoint tool optimization
- **Future-proofing the visibility solutions**

Protect your Network from the Inside

Network Critical recognizes that network and security managers have a stringent job to secure their network from outside threats. However, upon research, internal human error from within the company poses an equally high threat to networks, and security measures must be put into place to ensure no mistakes can be made.

In recent years, we have seen a rise in attacks that have begun within the internal network. Today's cybercriminals use sophisticated exploits to lure unsuspecting persons to click or do something to breach the network via a backdoor. In some cases, this can give hackers access to the whole network including all devices connected to the internet of things (IoT).

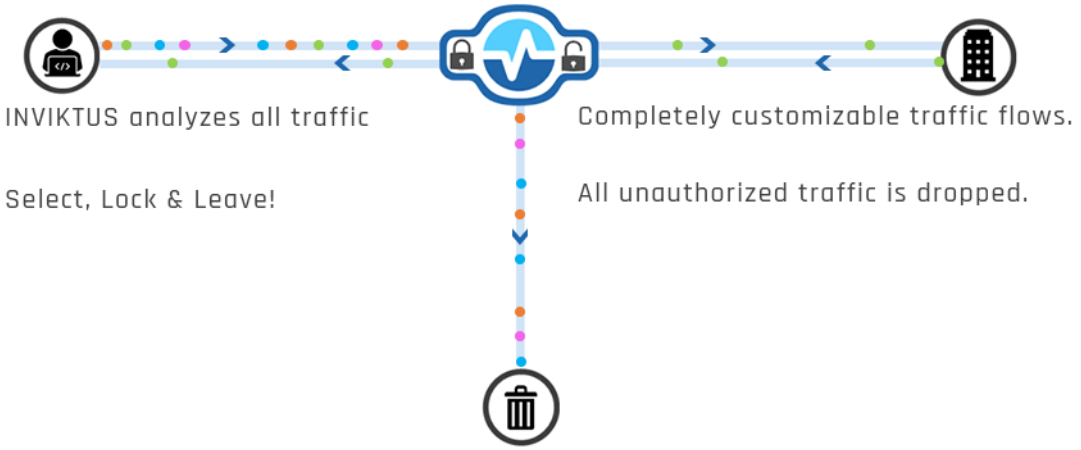
INVIKTUS

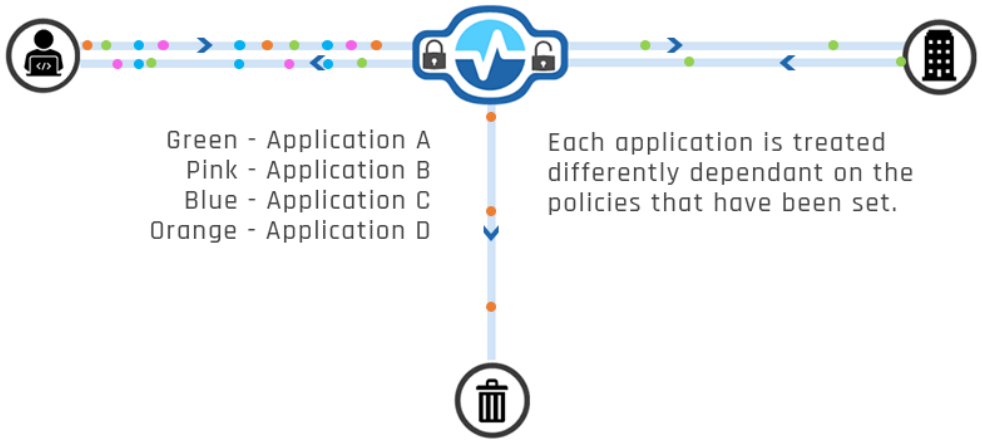
Invisible · Unhackable · Always Protected

The Future of Network Security at your Fingertips

Network Critical's **INVIKTUS cybersecurity system** is the strongest low level security for your critical network, enabling complete reliability and security from layer 1.

This additional internal security layer has been designed from the ground up with the security and network managers in mind. Network Critical knows that users of this device need a **low-cost**, **easy-to-use**, and **highly reliable** device to secure the network, reach objectives, and stay within budget.





With policy-based configuration, INVIKTUS knows if your network team has made a mistake and will not allow the changes made until the policy is met.

The 1U device provides **'Lock and Leave'** functionality. This means upon configuration, INVIKTUS works in the background with low maintenance requirements. It has been created to be **completely invisible** from the network as it doesn't have any IP or MAC address. Therefore, exterior threats that gain access to your network cannot detect your internal security layers.

Hackers cannot threaten what they cannot see!

A Competitive Advantage Solution

Due to the increase in cyber threats organisations must continue to innovate and update in order to stay ahead of threats like ransomware. A concentrated, multi-directional, multi-layered effort that encompasses all endpoints is the best strategy an organisation can use to prevent and recover from a cyber-attack. Maintain your team's cyber awareness by continuing to train them.

Cybersecurity must now be viewed as a competitive advantage for businesses. Companies who have been the victim of a cybercrime have suffered not just financial losses, but also a reputational hit that is nearly always irreversible. When it comes to developing a business strategy, investing in cybersecurity is a must because it attracts brand awareness, loyal customers, and profitable partnerships.

When we build our solutions at Network Critical, we keep these factors in mind. Learn how to gain a competitive edge and reduce corporate risk by implementing a cybersecurity strategy.

CONTACT US

Head Office, UK +44 (0) 118 954 3210

US Office, GA +1 (470) 554 7170

or

sales@networkcritical.com