NIAGARA NETWORKS

TOP SECURITY TOOLS & TACTICS

TO PROTECT YOUR NETWORK IN 2019

KNOWLEDGE IS POWER!

IS YOUR NETWORK FULLY PROTECTED?

CAN IT FIGHT OFF SOPHISTICATED ATTACKS?

WILL YOUR NETWORK DEFENSES PROTECT AGAINST ALL THREATS ANTICIPATED IN 2019 AND ON?

Your network security is probably being tested on a daily basis. Potential threats and their potential solutions are part of a rapidly changing landscape that you need to constantly keep up with. What you knew last week may not be what you need to know today. Therefore - as a security pro - keeping up-to-date on the latest technology solutions is both your prerogative and your obligation.

Organizations need to leverage smarter systems and use flexible security architectures to enable context-aware security controls. Building resilient digital business systems that are versatile and dynamic allows security and risk leaders to prepare for and head off increasingly dangerous cyberthreats.

NSS Labs, Inc., a global leader and trusted source for independent fact-based cybersecurity guidance, suggests that “Threat actors are demonstrating the ability to bypass protection offered by conventional endpoint and perimeter security solutions. In turn, enterprises must evolve their network defenses to incorporate a different kind of protection” – which NSS defines as a breach detection system (BDS).

The challenge of catching and stopping those who try to circumvent system and network security controls requires new, flexible yet robust solutions from reliable sources.

This eBook presents some of the top tools and techniques that you will need to deal with the most relevant threats to your network. The following pages explore some relevant data, gathered by Niagara Networks, on the top enterprise security deployment tools and platforms in the industry for 2019.

NIAGARA NETWORKS

DEFENSE … IS THE BEST DEFENSE

Although the adage goes: “The best defense is a good offense”, in our world of IT, knowing who your specific adversaries are is next to impossible. Like cats, they hide in the shadows, lurk and then pounce when we least expect it. To mitigate, we need to ‘profile’ not the adversary, but rather what and where any potential attack will be made in our system. To paraphrase:

> “Today’s essential tools and techniques are enveloped by advanced strategy frameworks”.

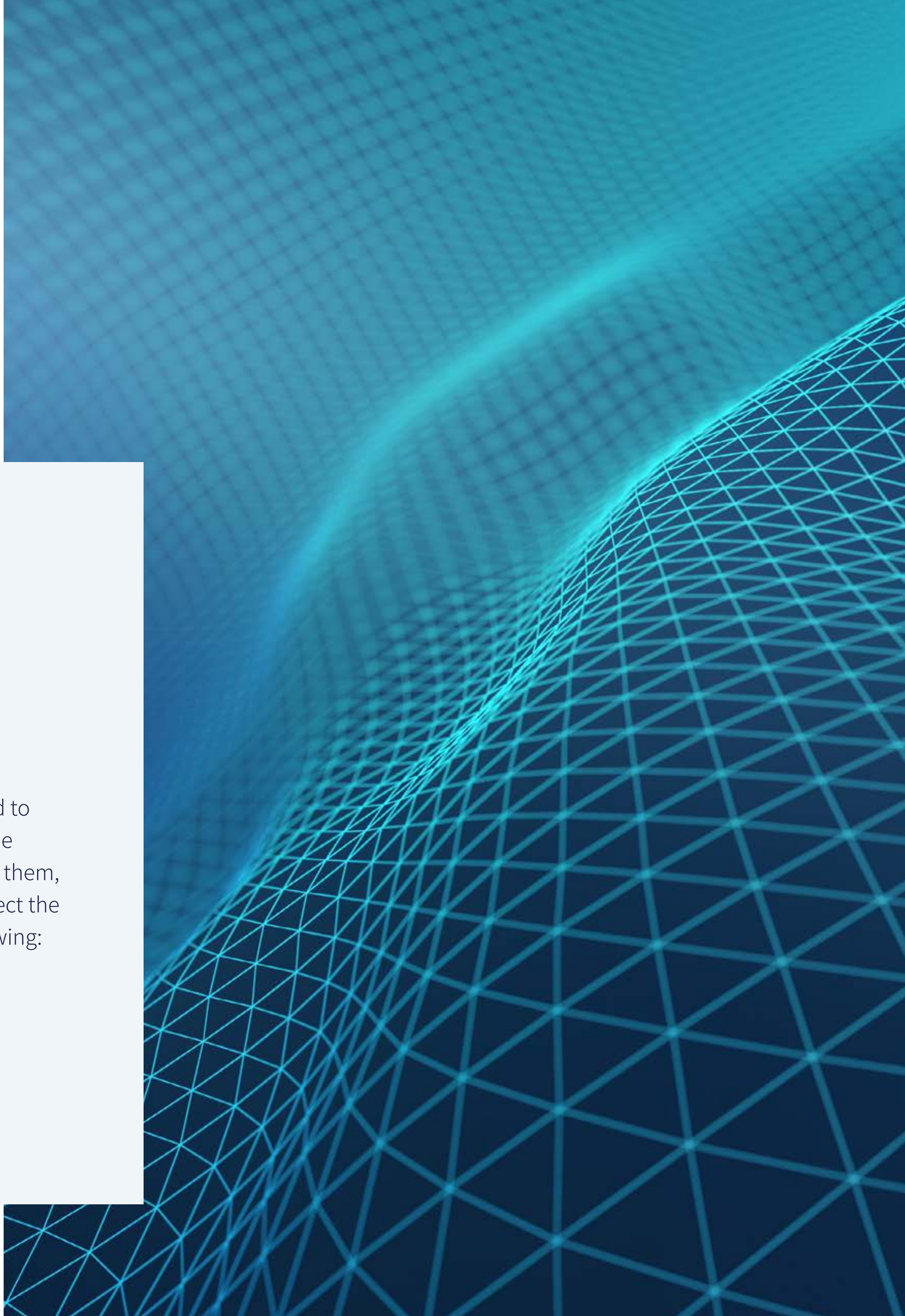
HERE ARE KEY TOOL CATEGORIES WE BELIEVE THAT EVERY SECURITY PROFESSIONAL SHOULD BE FAMILIAR WITH:

- Firewalls (FW/NGFW)
- Intrusion Detection & Prevention Systems (IDPS/NGIDPS)
  - Intrusion Detection Systems (IDS/NGIDS)
  - Intrusion Prevention System (IPS/NGIPS)
- Distributed Denial of Service (DDoS) protection
- Unified Threat Management (UTM)
- Endpoint protection (antivirus)

There are various methods of protecting our corporate networks, and they all include deploying enterprise security tools tailored to the specific industry, potential threats and, of course, the nature and architecture of the specific enterprise network. The enterprise needs to both identify weak points in its system, but also what and where the potential targets are, in order to set up the necessary mitigation and security.

Today’s essential tools and techniques are enveloped by advanced strategy frameworks, and they make up today’s elaborate network security shielding. Recently dubbed Breach Detection Systems (BDS), they include both the traditional devices and services, as well as their advanced, new generation (“NG…”) versions or offshoots, such as firewalls (NGFW), intrusion prevention systems (NGIPS), anti-virus software, secure Web and email gateways (SWG and SEG), and endpoint features like sandboxes. Together, they are a formidable array of physical and virtual appliances, cloud-based services and methods to detect attempts at malicious attacks, intrusion, virus implantation etc., and to protect networks from such breaches, and worse.

Like any tool, it needs a good ‘breaking-in’ phase to test its usability, its strengths and limits, and to see in which areas and in what ways fine-tuning may be required to further strengthen security robustness.



DON'T IMPLEMENT YOUR TOOLS WITHOUT:

- **Penetration Testing -** This is a service or method to periodically (often randomly) effectively test the system’s defenses by attempting to breach them, analyse weaknesses, and report and suggest solutions.

  In addition, both the users (or implementors) of the tools need to be properly trained, and general staff awareness should also be enhanced about the needs for such tools, how the tools affect them, and how the users may also (inadvertently and negatively) affect the network security. Therefore, we should also factor in the following:

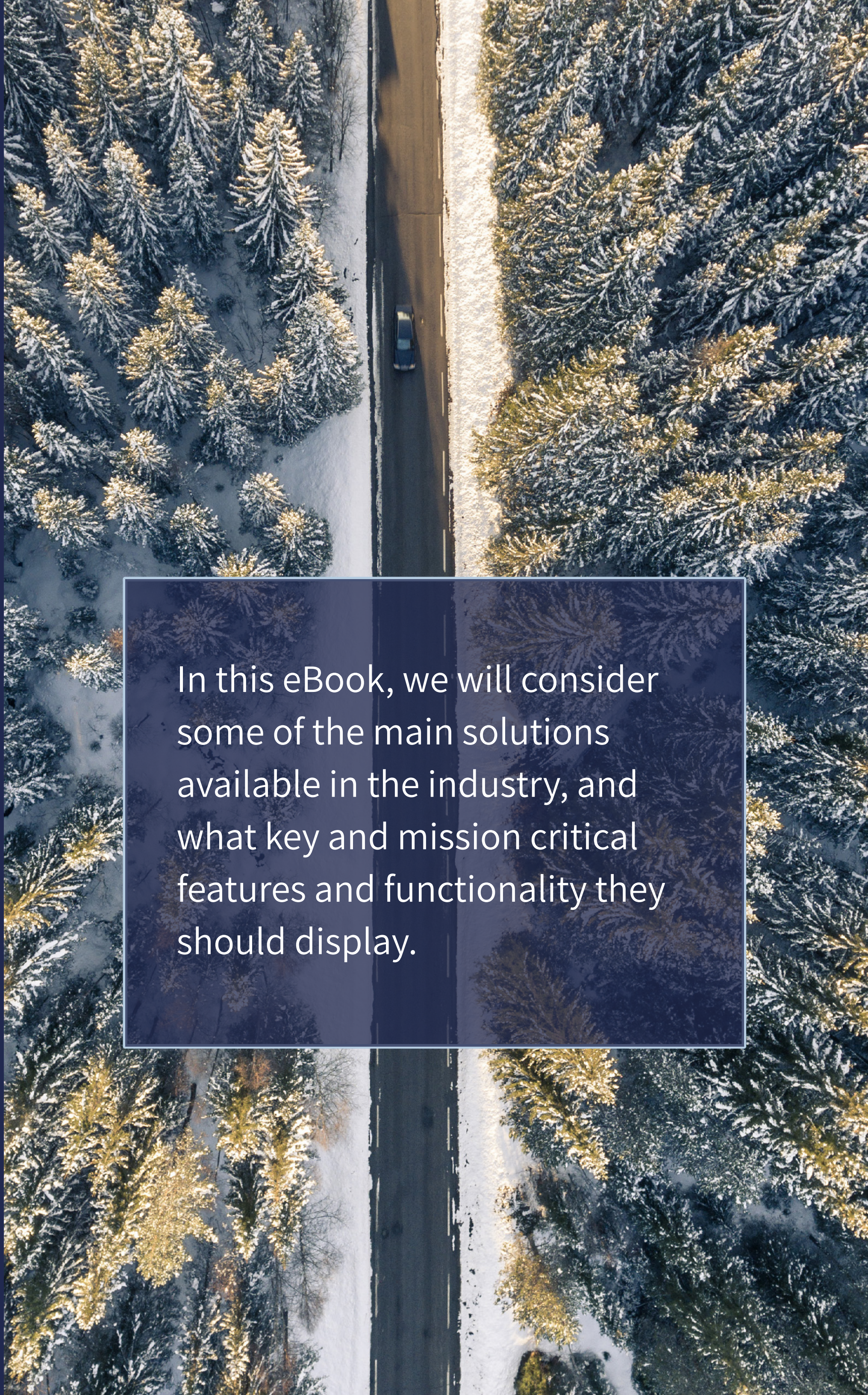
- **Staff Training -** It is important to factor in staff awareness of good practises in preventing breaches, as well as empowering personnel with steps to take in ‘what-if’ breach situations.

1 2 3 4 5 6 7

SMART SECURITY TOOLS AND TACTICS

There are various security tools and solutions available for securing organizational networks and ensuring their wellbeing, with many good applications available.

In October 2017, NSS Labs, Inc. announced the results of its Breach Detection Systems (BDS) Group Test. The study indicated that 44.1% of US enterprises deployed BDS products that provide enhanced detection of advanced malware, zero-day attacks and targeted attacks.



In this eBook, we will consider some of the main solutions available in the industry, and what key and mission critical features and functionality they should display.

1 NEXT-GENERATION FIREWALLS (NGFW)

A traditional firewall is only able to scan and control connections based on packet information available between layers two and four (-where the “layers” refer to OSI - Open Systems Interconnect model). A traditional firewall would likely include additional tools such as Network Address Translation.

The next-generation firewall (NGFW) takes the traditional firewall and adds intrusion prevention systems (IPS) and application awareness (Layer 7). NGFWs also include other functionalities such as TLS/SSL termination and inspection, deep-packet and malware detection as part of broader breach detection systems (BDS).

Since downtime is unacceptable, correct deployment of the NGFWs, such as active-active clustering, will empower a definitive uninterrupted operation. During maintenance, system modules will be able to be maintained node-by-node without a service break - even those operating with different software versions or hardware combinations.

WHAT TO LOOK FOR IN NEXT-GENERATION FIREWALL (NGFW):

DEEP PACKET INSPECTION (DPI)

It should include an advanced form of network traffic scanning and classification, enhanced detection of advanced malware and zero-day attacks, capable of application classification and more. NGFWs equipped with DPI capability should also provide dynamic updates that can be automated, with recommended policy configurations and vulnerability-based protection fingerprints.

CENTRALIZED MANAGEMENT SYSTEM

The team managing your system needs to be able to accumulate and monitor data across all the security inspection and defense mechanisms, and be able to instantly respond to any threat or anomaly. The NGFW system should be able to integrate with the other security systems and enable the team to observe and manage all firewall activity through a single dashboard. For example, it should enable managing network ports and IP addresses, updating new network information to identify new malware attacks, as well as displaying the system performance and result analysis.

SSL DECRYPTION

Depending on the enterprise’s security policies and restrictions, a significant percentage of its network data traffic is SSL-encrypted. Network security managers need to take into consideration that there is an increase of HTTPS adoption and SSL on many websites. The firewall must be able to identify, decrypt and inspect SSL traffic and also be capable of bypassing specific segments of SSL traffic according to policy rules.

2 INTRUSION DETECTION & PROTECTION SYSTEMS (IDPS = IDS + IPS)

1
2
3
4
5
6
7

Intrusion detection systems (IDS) and Intrusion protection systems (IPS) are either stand-alone systems or often combined as IDPSs (intrusion detection and protection systems).

2.1 INTRUSION DETECTION SYSTEM (IDS)

The intrusion detection system (IDS) is a network monitoring tool used to surveil network traffic. If malicious activity is detected by an IDS, an automated warning will be sent to the system administrator and the source of the traffic may be blocked to secure the network. There are a variety of IDSs, including:

- Network Intrusion Detection Systems (NIDS)
- Host Intrusion Detection Systems (HIDS)
- Signature-based IDS

2.2 INTRUSION PREVENTION SYSTEM (IPS)

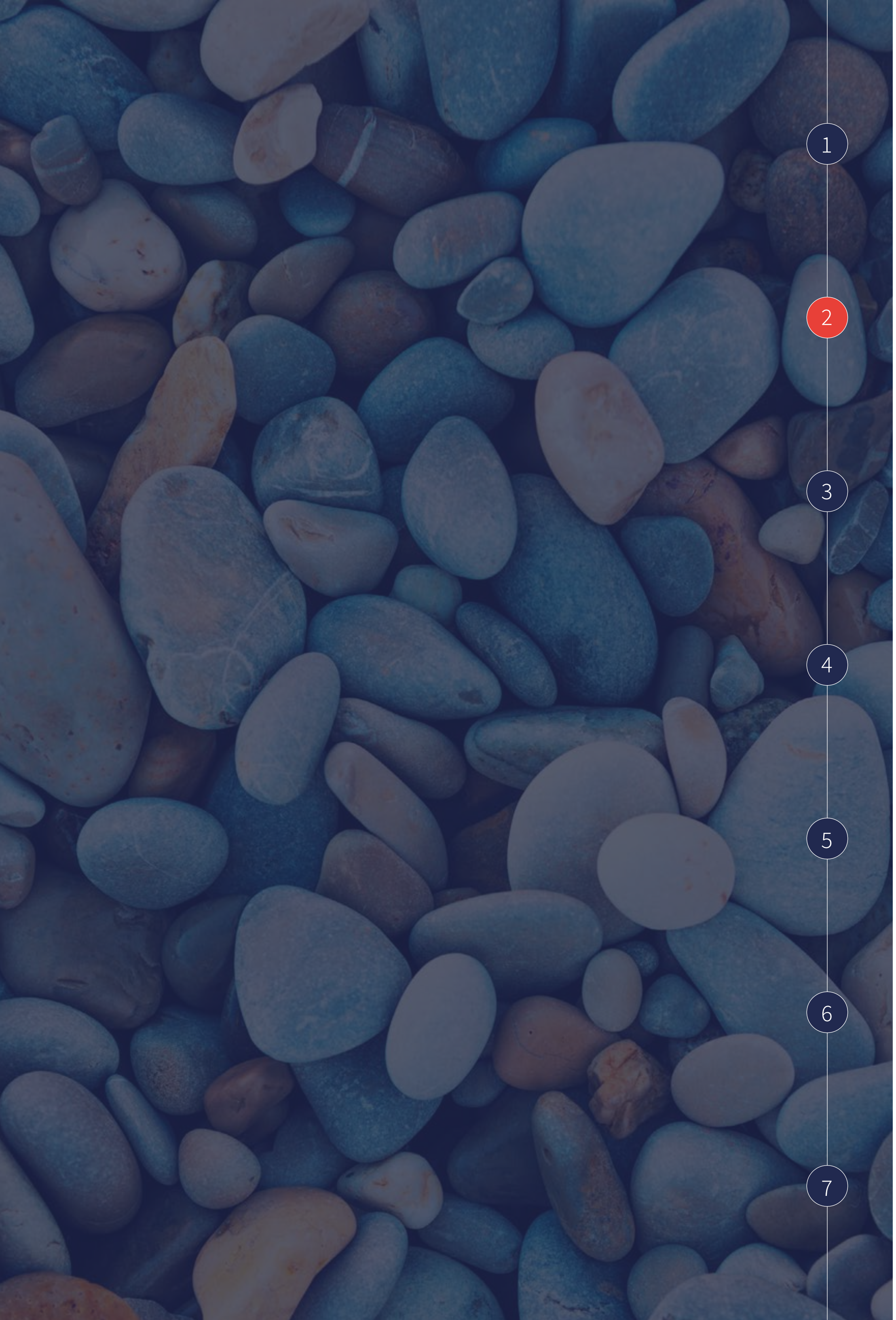
An Intrusion Prevention System (IPS) is a threat prevention solution that examines network traffic to identify threats to the system and prevent intrusion. Whereas the intrusion detection system (IDS), detects and alerts upon unwanted attempts to access your network, the intrusion prevention system (IPS) is designed to actually block and prevent such access.

2.3 DETECTION METHODS

In order to detect and identify malicious data packets, two types of detection methods are generally used.

The first type of detection method is Signature-Based Detection. Signature-Based Detection uses the signature, or recognisable pattern of an exploit to identify malicious data packets. It relies on a database of signatures, which is used to recognise threats.

The other type of detection method is based on traffic heuristics or on Statistical Anomaly Detection. Statistical Anomaly Detection creates an average set of behaviours by tracking legitimate traffic over a period of time. After this baseline is defined, the IPS will take steps to protect the network against any traffic that falls outside of these set behaviors. Such traffic heuristics are useful in detecting threats that are yet unknown in the industry and do not have an identifiable signature. IPS may be combined with IDS to automatically protect your network from identified threats.



WHAT TO LOOK FOR IN INTRUSION DETECTION AND PROTECTION SYSTEMS (IDPSS):

COMPREHENSIVE, AUTOMATED DETECTION CAPABILITIES

The IDPS should be as automated as possible, and empower the security team to monitor and investigate alerts, tune detection capabilities and ensure that the system is not only looking for the latest threats – but can deal with them.

ABNORMAL BEHAVIOUR DETECTION MECHANISM

This capability uses smart algorithms to monitor network traffic and activity on a constant basis, and storing and comparing the traffic behaviour for specific days and hours. By studying 'normal' patterns and then comparing against what may seem to be abnormal traffic activity for a similar or particular day of the week, time and month - the mechanism can notify security administrators of possible excesses in expected thresholds.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

This module collects, logs and manages warnings and alerts. A SIEM is entirely out-of-band, typically not even processing a copy of the data traffic directly, but logs metadata and alerts from other tools. It integrates and evaluates threat intelligence against known system weaknesses for better management and prioritization of security controls.

1 2 3 4 5 6 7

3 DISTRIBUTED DENIAL OF SERVICE (DDOS) PROTECTION

One of the easiest forms of assault on an enterprise network is a Denial of Service (DoS) attack – with its more robust offshoot, a Distributed DoS (DDoS) attack. Basically, this is a form of storming another network by sending a large amount of traffic towards it, thus overloading and overextending its resources. In its October 2017 study, Neustar reported that attacks of this kind have increased, and "…attackers seem to be more deliberate with their strikes, launching targeted volleys that successfully breached defenses at a higher rate."

The stretching of resources, leaves the defenses, overwhelmed, overextended and busy dealing with the massive influx, thereby facilitating the incursion of attacking malware during the 'confusion'.

The best advice for selecting a DDoS solution, is to combine several solutions to cover all potential attack points in your network. Some of the products that offer these different DDoS mitigation components include new generation and Web application firewalls (NGFW & WAF).

On the other hand, the most effective DDoS protection solutions are service-based. The reason is that most enterprise data centers have a limited pipe for inbound data so that even if your firewall can block DDoS traffic, your pipe is still overwhelmed. Service solutions make a point of having almost unlimited network capacity.

WHAT TO LOOK FOR:

LAYER 3 TO LAYER 7 PROTECTION

Protection of layers 3-4 (network and transport layers) that affect the communication network, and those of layer 7 (directly affecting applications) is required to provide full stack DDoS protection when used with an application gateway.

INTELLIGENT FINE-TUNING

Over time, as the DDoS mechanisms study the application's traffic, it selects and updates the profile that is the most suitable for the system. The profile will self-adjust as traffic changes over time.

SERIOUS SERVICE PROVIDERS

Both Internet and cloud service providers have teams that are assigned to mitigation of malicious traffic. However, according to Sean Leach at "NetworkWorld" online, the reliable ones are the "Cloud mitigation providers [who] are experts at providing DDoS mitigation from the cloud", thanks to their expertise, resources and commitment.

1
2
3
4
5
6
7

4 UNIFIED THREAT MANAGEMENT (UTM)

Another combined set of solutions can be found in the Unified Threat Management (UTM) solution. Although its combined components (i.e. for its target solutions) may differ from vendor to vendor, much of the functionality and most of the security features are common.

This is an all-in-one solution that incorporates VPN protection, firewalls, anti-spyware, anti-viruses, spam and content filtering, and other security methods needed to protect networks and provide layered protection for organizations of any size.

Some vendors use the UTM term to refer to SMB-level products, though many of the industry's current UTM market leaders do not. The network security domain is expanding rapidly and UTM solutions are becoming more powerful and enterprise-ready.

WHAT TO LOOK FOR:

ANTISPAM FILTERING

Email spam consists of unwanted messages (sometimes legitimate commercial ones, but more often malicious or fraudulent ones). The antispam feature should examine and detect an e-mail spam and tag it with a preprogrammed string and/or move it to a SPAM storage folder.

WEB AND CONTENT FILTERING

Web and Content filtering should let the network manager (or single user) manage certain types of Internet traffic by preventing access to inappropriate Web content. Identification is based on a blacklist of prohibited sites and a list of objectionable keywords, that is periodically updated.

FILE-BASED ANTIVIRUS

A file-based antivirus feature should scan application layer traffic to check for viruses against a virus signature database. It will collect received data packets until it has reconstructed the original content (such as an e-mail file attachment), and then scan that content for abnormalities that may indicate a malicious insertion.

5 ENDPOINT PROTECTION

Endpoint security (including anti-virus) generally deals with devices connecting to an enterprise network and the risks that are involved with them (usually, inadvertently) passing viruses and malware that may penetrate the system. Such devices – the endpoints – include mobile phones, laptops, tablets and such, but may also include data center servers as well.

The additional protection afforded by good endpoint security protects the network at the point of entry for any potential attack, and can also offer additional protection for sensitive data being sent out to the endpoint devices themselves.

WHAT TO LOOK FOR:

FULL DISK ENCRYPTION (FDE)

FDE protects data by converting it into unreadable code that cannot be easily deciphered by unauthorized persons. Disk encryption uses disk encryption hardware or software to encrypt data that goes on a disk or disk volume data storage to prevent unauthorized access to it.

DATA LEAK PREVENTION (DLP)

DLP is aimed at stemming the loss of sensitive information. By focusing on the location, classification and monitoring of information at rest, in use and in motion, this solution assists IT in stopping the numerous leaks of data that occur each day in unwary enterprise traffic.

APPLICATION WHITELISTING

A method that specifies an index of approved software applications that are permitted to be present and active on a computer system. The purpose of whitelisting is to protect computers and networks from potentially harmful applications.

ANTIVIRUS AND ANTI-MALWARE PROTECTION

Software solutions to detect and protect against malicious implants and infestations.

6 PENETRATION TESTING

1 2 3 4 5 6 7

A penetration test (or pen test) or White Hat Attack is a sanctioned attack on a computer network. The purpose of this intentional attack is to identify any potential weaknesses in the network and address them before a hacker is able to exploit them. It is typically performed by external 3rd party specialists – though it can also be run in-house.

It is a form of active 'audit' to test the robustness and (im) permeability of the network, and the generated reports will provide insight into network strength and weakness issues such as:

- Risk Identification
- Vulnerability Scan
- Data Analysis

Penetration Tests should be performed on a regular basis to ensure that your network is secure, but also whenever you make changes to your network or network management, update applications or apply security updates. Ideally, testing new or updated applications should first be performed prior to their general or full deployment (for example in a controlled test environment such as a lab or dedicated, independent device not connected to the network). If the application/service/etc. passes the lab test, then it can be deployed and tested in production.

WHAT TO LOOK FOR:

- Robust 'poking' into the network to test its defenses, alerts and responses. Based on your network's configuration, among the various pen test activities, you should be able to assess:
  - Multiple attacks and scope-based configurations
  - Phishing attacks against Wi-Fi networks
  - Packet capture and attacking (including cracking WPA and WEP)
  - Host discovery and port scanning, OS detection and IDS evasion
- A real-time view of what the pen test is doing in the network
- Comprehensive reports on both strengths and weaknesses of the network defenses with explicit breakdowns by potential risk or vulnerability category (for example: data loss, unauthorised web-access and mobile breach)

7 STAFF TRAINING

A critical line of defense in protecting the network is the ability of the staff to prevent breaches. The most sophisticated 'locks' and 'measures' will be virtually powerless if someone 'leaves the door open', so to speak.

According to a 2016 study by PhishMe (now Cofense – promoting incident-response technologies), the majority of hacks are initiated by employees clicking on emails containing some form of malware: "91% of cyberattacks and the resulting data breach begin with a spear phishing email".

Essential training of staff with regards to awareness of breaching threats, prevention of such and what to do in scenarios where something may occur (even if only suspected) are critical to complete an enterprise's network security strategy.

In his recent (Sept. 2017) Cybersecurity Business Report entitled Please Don't Send Me to Cybersecurity Training, Steve Morgan lists 8 offerings from security awareness training vendors that provide training, simulations and tips.

WHAT TO LOOK FOR:

- IT general (introductory) training and periodic extended training on new issues, system risks and counter-methods.
- Staff training and periodic refresher courses, either frontal or online, with test questions to check staff awareness and comprehension.

NIAGARA NETWORKS

NIAGARA KNOWHOW TO THE RESCUE

As the number and nature of network and cyber security threats increase and evolve at an exponential rate to harm and even bring down networks, so must the preventive and active inoculation measures to counter them. It's quite literally a battle for survival.

Niagara Networks solutions are on the front lines, and we're ready and able to offer you our experience to help you integrate, implement, manage and monitor security tools, and empower the best possible defenses for your network.

Find out how to protect your network critical and sensitive data breaches, and optimize the deployment of your network security tools for better protection and availability. Check out the following resources:

Niagara Networks Visibility Adaption Layer

Implementing Inline Security Tools

What Is Network Visibility?

Resource Center

Contact Us

ABOUT NIAGARA NETWORKS

Niagara Networks provides high performance network visibility solutions to allow seamless administration of security solutions, performance management, and network monitoring. Its products deliver significant advantages in terms of network operation expenses, downtime, and total cost of ownership. Niagara Networks offers all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb, including taps, bypass elements, packet brokers and a unified management layer. Thanks to its integrated in-house capabilities and tailor-made development cycle.

Niagara Networks is agile in responding to market trends and in meeting the customized needs of service providers, enterprise, data centers, and government agencies.