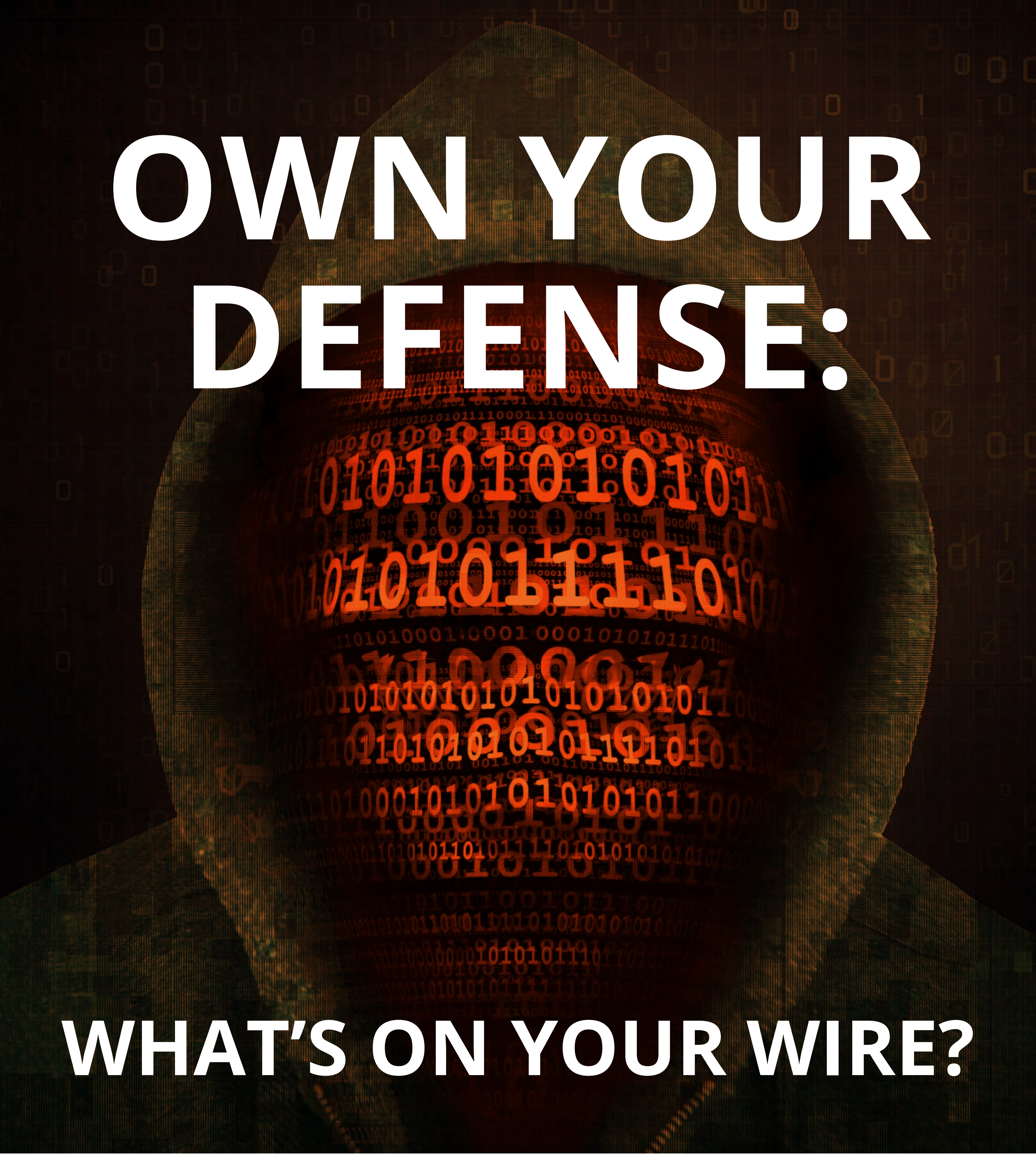


OWN YOUR DEFENSE:

WHAT’S ON YOUR WIRE?

NETSource
Secure by Design

Do you know what's one of the fastest growing industries in technology? Cybercrime. In 2016, the average consolidated total cost for data breaches affecting enterprise businesses was $4 million.[1] Unfortunately, the future doesn't look any brighter, as the global cost of cybercrime is expected to reach $2 trillion by 2019.[2]

Cybercrime has entered the mainstream. Each day brings forth a new article about an attack or new threat to monitor, often splashed across the web pages of the national news. Thieves always gravitate to where the big payloads are, and with the rise of new cyberattack methods, that bounty can include data, trade secrets, customer information – even virtual wheelbarrows full of bitcoin. However, it's not just big business that has to remain vigilant.

The wide, ever-evolving scope of cybercrime tools is hitting everyone, right down to mom-and-pop-sized operations. The cybercrime industry is outpacing the security industry in terms of innovation, technology, and speed to market, which makes it even harder for small- to medium-sized businesses to keep up – they simply don't possess the security capabilities or staff. They can be seen as easy targets for a quick buck.

But there is a solution. Every size of company must make a mental shift and realize that cybercrime is an imminent threat. It's not if it will happen; it's when it will happen.

Your first line of defense is to know what's on your wire – which cyberattacks pose a threat to your business, and how do these threats spread? By gaining an understanding of your vulnerabilities, you can take the right measures to steady yourself for an attack.

Table of Contents

Today’s Top Cybersecurity Threats:

MALWARE

Think of malware as the umbrella policy for all other cybersecurity attacks. In its most basic definition, “malware” is shorthand for malicious software, including everything from computer viruses, worms, Trojan horses, spyware, ransomware, and more.

While certain forms of malware demand their own place on the list of top cybersecurity threats – ransomware, we’re looking at you – it’s important to discuss malware as a whole category. The main reasons: the rise of Android malware and the prevalence of mobile devices.

Android is the most used platform in the world. Between 2013 and 2014, over 200 million of shipped smartphones were Android-based, and by 2016, over 8 million of those Android smartphones were infected with malware.[3]

The two most common forms of malware on mobile devices are Trojans and malvertising. With Trojans, users are often tricked into loading and installing the virus. With malvertising, the malware is hidden within an online ad. Click on the ad, and your smartphone becomes infected.

How does this affect your business?

In a BYOD poll, 87% of respondents reported that they rely on their employees to access business applications from their personal smartphones.[4] This means that malware doesn’t even have to fight to get past the security measures of your network. If malware is on an employee’s phone, it’s got a direct line in.

Without the proper protocols and security measures in place that include smartphone use, your company won’t stand a chance staving off infection.

Today’s Top Cybersecurity Threats:

RANSOMWARE

There is no bigger cybersecurity threat in the world right now than ransomware. This form of malware is slamming businesses across the globe, grabbing headlines, and shutting down entire networks by taking data hostage in exchange for payment in bitcoin.

While ransomware started out targeting individual computers, it is now able to infect multiple machines in multiple locations. Ransomware stealthily infects a machine, sometimes locking it up completely, other times encrypting data and files so they’re unusable.

A hacker then contacts the victim, explaining that, in order for the issue to be resolved, a ransom must be paid. While an LA-based hospital received a $3.7 million ransom notice, the average ransom demand is $300 per infected device or computer.[5] Businesses are faced with a choice – pay the fee or lose their valuable data.

With the average ransom so low due to the volume of computers ransomware can infect within a business, SMBs are particularly vulnerable. Profits are based on the volume of companies affected and how far into their networks a hacker can reach, not the size of the company. Therefore, most companies choose to pay, as for an SMB, taking the pay hit is often the less costly alternative.

Recently, Petya ransomware constituted the biggest global hit yet, locking computers throughout the U.S. and Europe. The Ukraine was affected the hardest, with Petya infiltrating their government, banking systems, and electricity grid. The ransom, again, was $300 per computer.

Further complicating this situation, the email address of the Petya ransom was shut down by the email provider, thereby eliminating the primary outlet in which to pay the ransom. Computer systems had to be taken offline – even the radiation monitoring system at Chernobyl – and all the data held hostage was lost.

This provided a new dilemma with ransomware – the elimination of choice. With providers actively shutting down accounts linked to ransomware, we may be collectively entering in a situation where no one wins.

Today’s Top Cybersecurity Threats:

NATION-STATE ATTACKS

With the hack of the Democratic National Committee during last year’s presidential election, nation-state attacks took center stage in the American consciousness. The national headlines generated by the incident served as a wake-up call to American citizens, as this type of activity has been going on for years.

Chinese hackers first began attacking the U.S. in 2005. In 2007, the entire country of Estonia was under a complete digital invasion. In 2008, NASA found a worm infecting the computers of the international space station. A few months later, computers at the Pentagon were hacked, allegedly by the Russian government.

As the earlier-mentioned Petya ransomware proved, nation-states are attacking all facets of other nation-states – government institutions, infrastructure, banking, and business. What’s worse, though, is that these attacks aren’t done for financial gain. The goal is to cripple a country and bring about the downfall of its government.

We are at the point now where these nation-state attacks will soon be labeled as acts of war, as they possess the potential to inflict more long-term damage than an influx of troops. Our own country recognizes this new fact of life by having defense operations that cover five domains – air, land, sea, outer space, and cyberspace.

When you have entire government agencies solely dedicated to cyberattacks – both investigating attacks and defending against threats – it’s obvious we’ve entered a new age of warfare.

Today’s Top Cybersecurity Threats:

DDoS ATTACKS

DDoS, or Distributed Denial of Service, attacks saw rampant growth in 2016, up nearly 40% from 2015.[6] Often a favorite weapon of the hacker collective Anonymous, the goal of a DDoS attack is disruption – using a flood of requests to bring down a system or network to gain easier entry for nefarious purposes like data theft. DDoS attacks have also been used to take out the websites of political parties, governments, and financial institutions.

DDoS attacks have benefited greatly from the development of multi-vector attacks, in which attack vectors are combined to confuse defenders and boost attack volume. The growth of the Internet of Things (IoT) has also generated new channels in which to infiltrate businesses.

With sensors being common in everything from consumer devices to equipment in the manufacturing plant, a hacker or hacker group can gain entry from any number of the devices that constitute an IoT network. If the gateway to the internal network isn’t properly secured, access can quickly be granted, spreading a virus to take control of IoT devices, smartphones, desktop computers, and servers.

Just gaining access to one IoT device can quickly lead to the creation of a botnet – a collection of internet-connected devices that the hacker can control through command and control software, even after devices are rebooted. One compromised device sets off a chain reaction throughout the network, granting access to hundreds of devices. The hacker then has a giant botnet to carry out large-scale DDoS attacks either against your own company or others.

Today’s Top Cybersecurity Threats:

ZERO-DAY VULNERABILITIES

A zero-day vulnerability can be compromised in two ways – via an undisclosed hole in software and through factory-default usernames and passwords. When discussing software, “zero day” refers to the unknown nature of the hole by the developers. Hackers search out these holes and then exploit the vulnerability to gain access to secret data or introduce malware, spyware, ransomware, and other malicious software into your system.

Patches are used to solve holes in software, but they don’t always catch critical vulnerabilities. While software companies release patches on a regular basis, a patch may not cover everything. When a critical vulnerability is discovered, it’s a race against time to close the hole before it’s exploited. It’s important to note that browsers are also vulnerable to holes, so it’s best to set up automatic updates or update the browser itself on a regular basis.

Factory-default usernames and passwords present a different sort of problem. New equipment for your network typically comes with default settings so you can first get your hardware online and then change the username and password. However, user error often involves negligence of updating that username or password.

Also, many of these factory defaults are easily discovered by running a simple algorithm, and when it comes the sheer number of IoT devices, there is ample opportunity to search for one single device in which the default username and password hasn’t been changed. This is the method that the creators of Brickerbot, Mirai, and Hajime all used – exploiting factory defaults to build a botnet composed of hundreds of thousands of devices.

Currently, many manufacturers are taking matters into their own hands by removing factory-default settings. However, for existing devices – particularly IoT devices – it’s a good idea to check that all factory-default settings have been changed.

Today’s Top Cybersecurity Threats:

THE HUMAN ELEMENT

A 2015 survey revealed that 37% of security breaches were caused by human error.[7] This really comes as no surprise to any person involved in IT. As human beings, we’re just not that smart about internet security. We send sensitive data to the wrong people. The most common passwords used include “123456” and “password.” Way too many people think “qwerty” is a tricky password. To top it off, we forget unlocked laptops on trains, lose flash drives, and never download security or malware detection software on our smartphones.

Speaking of smartphones, we’re way too susceptible to phishing and man-in-the-middle (MITM) attacks. As proof, the same survey that placed human error as the top threat to security in 2015 named phishing a top threat in 2016.[8]

In their own ways, phishing and MITM attacks can be considered products of human error, as their sole purpose is to trick people into believing a lie. Phishing scams utilize emails, websites, and phone calls to trick people into giving away personal information such as login credentials or account information.

MITM attacks involve a malicious person inserting himself into a conversation or impersonating another party to receive or intercept information. These events most often occur in real time, without the target suspecting any bad intent.

Rounding out the top threats due to the human element are physical insiders and credential theft. These are the bad apple employees who use their access to data to hurt the company. This is a most unfortunate situation, as there’s really not many preventable actions a company can take other than to conduct reference checks and examine a prospect’s work or criminal history before hire.

Today’s Top Cybersecurity Threats:

NETWORK TRAFFIC

Most companies have very little knowledge of what’s going on in their network. How many employees access Facebook or Twitter the moment they log in on a Monday morning? Many cyberattacks originate through social media, and the network being used by your employees on a weekday is going to be yours.

Sadly, employees are also accessing a lot more than social media. Watching Comcast, HBO, Netflix, and Hulu is not uncommon. People swipe away on Tinder and check their Instagram accounts. They surf the web for everything and anything, and “not safe for work” doesn’t mean they’re not looking at it.

Your network traffic is made up of a mess of things that have nothing – but, at the same time, everything – to do with your business. It’s not just a worry of productivity; it’s the multiple tendrils reaching into the depth of your systems.

To combat the situation, many companies have initiated “no social media” policies. Others are locking down employees’ smartphones and tablets and installing security applications. Companies also track network traffic.

Determining what’s acceptable at work has to be based on your corporate culture, your expectations of employees, and the risk of losing trust within your organization. It can be a tricky line to walk, but it must be done to limit security threats.

Today’s Top Cybersecurity Threats:

THE IT ELEMENT

Over the last decade, we’ve seen IT departments transform from a business support role to a driver of profits. However, someone still has to do the dirty work – all the maintenance tasks that keep your business and network running smoothly. Chances are, your IT staff is feeling a little swamped, and this can greatly affect security.

The exponential growth of big data means that IT staff and your network infrastructure are dealing with a huge influx of data from many disparate sources at an unprecedented clip. Without proper staffing or a partnership with an IT support provider, it’s easy to fall behind.

Your IT employees can also easily fall into alert fatigue, the point where IT personnel become desensitized to security warnings. This can lead to a failure to respond appropriately to warnings – a situation that cyber attackers are more than happy to exploit.

In an effort to shore up profits, IT departments often face budgetary constraints. This can limit the depth of the security measures your company implements or limit the resources available to accurately monitor your network.

When this happens, your company not only loses proper visibility but also gives up a measure of control. Profits cannot come at the expense of robust security, as a costly breach or damage to your network from a virus can affect the future of your business.

The NETSource Solution

Spending on cybersecurity is expected to reach $101 billion by 2018, as the attacks keep on coming.[9] Mobile and cloud security markets are growing, and threat intelligence is a vital part to any security plan. As former FBI Director Robert Mueller once said, there are only two types of companies, “those that have been hacked and those that will be hacked.”

Whether you’re an SMB or a Fortune 500 organization, cybersecurity demands dedication, proper staffing, and round-the-clock monitoring to defend your assets throughout every phase of a cyberattack. On average, over 4,000 ransomware attacks transpired per day in 2016.[10] You need an end-to-end solution to ward off all threats to your network and protect your data and applications from breaches and theft.

NETSource solves your security challenges by first performing a security audit to determine your network’s strengths and weaknesses. We then guide customers to the appropriate security solutions, perform risk assessments, implement best practices, and formulate security investment strategies for the future.

The NETSource NETSecure^{SM} product suite is built upon 4 pillars that deliver security to every device attached to your network – Rapid Incident Response, Enterprise Protection, vSOC, and Managed Optimization Services. These protection suites are customized to your business to deliver a complete, integrated security solution.

The NETSecure^{SM} Product Suite:

RAPID INCIDENT RESPONSE

RAPID INCIDENT RESPONSE

It is impossible to block every threat that comes across your network wire. That is why Rapid Incident Response is a necessity. NETSource Rapid Incident Response helps businesses of all sizes contain and recover from threats so they can resume normal operations quickly and efficiently.

This suite of security protocols provides instant visibility of transactions across all the devices, applications, and platforms that compose your network, spanning every branch location. Terms and conditions for instant response services are established before any cybersecurity incident occurs so that the protocols and procedures are already in place to mitigate the unpredictable and urgent nature of a volumetric security threat.

Rapid Incident Response is broken down into 5 services to successfully hunt threats in real time, visualize the complete attack kill chain, and quickly remediate the attack:

RAPID RESPONSE TIME	PREPARATION, COORDINATION, AND MANAGEMENT	DETECTION AND ANALYSIS	CONTAINMENT, ERADICATION, RECOVERY, AND FORENSICS	NOTIFICATION REQUIREMENTS ASSISTANCE
Time is the most important factor in detecting a security breach. The faster a breach is detected and contained, the less damage there will be.	NETSource can work with your existing staff to provide additional resources to prepare for and effectively manage serious breach situations.	Rapid Incident Response identifies the threat, provides visibility of the attack, and determines, analyzes, and monitors the extent of a breach.	NETSource's certified forensic unit collects system images and network traffic to maintain a proper chain of custody.	If it is determined that any private data was lost in a breach, NETSource will help you meet regulations or compliances that require your organization to proactively notify impacted individuals.

The NETSecure^{SM} Product Suite:

ENTERPRISE PROTECTION

ENTERPRISE PROTECTION

As cybersecurity threats continue to evolve and become more complex, organizations must keep pace with rapid technological innovation. In short, it’s an arms race, and organizations have fallen behind. NETSource Enterprise Protection levels the playing field.

Enterprise Protection is a custom-built security tool for providing mobile data and application security for both employee-owned and corporate-issued mobile devices. It features advanced applications for security and privacy risks, identifying and blocking malicious applications before they can do damage.

With the increased integration of mobile devices throughout your enterprise network, traditional firewalls no longer provide sufficient protection from port-hopping applications and malware. Enterprise Protection identifies internet-based bad actors across all ports and protocols to block cyberthreats and data leaks.

Other services of Enterprise Protection include 24/7 security operations and increased visibility, detection, and response time to threats. Endpoint protection is vital for IoT networks and attached devices. With managed firewall deployment, NETSource configures and monitors firewalls, intelligently identifying and blocking attacks.

Additionally, Enterprise Protection incorporates penetration testing for vulnerability assessments and provides security, compliance, and operational reporting. Enterprise Protection effectively flips the table on cyberattacks by aggressively attacking cyberthreats themselves, working to eradicate the root of the problem by evicting the criminals that wish to harm your company and network.

The NETSecure^{SM} Product Suite:

VIRTUAL SECURITY OPERATIONS CENTER (VSOC)

vSOC provides 24/7, 365 days-a-year security operations, incident management, and event management services for your company. Even today's largest enterprise corporations have a hard time keeping up with new threats and retaining the proper staff to handle emergency response for ever-changing security challenges. Our vSOC team provides your IT department with advanced threat intelligence and up-to-date security threat alerts to your business as well as remediation guidance to solve any issues.

With the NETSource vSOC service bundle, clients are provided with all the software, hardware, and sensors needed to actively analyze and monitor network threats. vSOC will intelligently identify internet-based applications across all ports and protocols, enforcing granular access policies for users, locations, and applications.

The center will pinpoint your critical assets that are vulnerable to attack and detect and monitor the indicators of a breach attempt, effectively blocking cyberthreats. Additionally, vSOC performs threat analysis, reporting, and log retention, simplifying the process of collating and correlating data to continually update an actionable network defense plan.

Clients can also opt for a Virtual Chief Information Security Officer (vCISO). This service supplies experienced, certified security professionals to augment your team and help establish, improve, and manage your security and risk program. It also assists your enterprise in preparing for external reviews of regulatory compliances and federal standards, such as HIPAA/HITECH, PCI, DSS, SOX, JSOX, and NIST 800-53. Look to vCISO to help with your network's physical security, InfoSec risk management, disaster recovery and business continuity, access control testing, and attain compliances.

MANAGEMENT
OPTIMIZATION
SERVICE (MOS)

The NETSecure^{SM} Product Suite:

MANAGEMENT OPTIMIZATION SERVICE (MOS)

MOS protects and optimizes your internet service throughout your entire network. Security threats are moving from servers to users, which vastly increases the pathways a virus can use to infiltrate your network. Additionally, security appliances are getting easier and easier to bypass.

A chief component of MOS is the optimization and fortification of your firewalls. With MOS's automatic configuration, your firewalls run at peak efficiency while providing deep defense against cyberattacks.

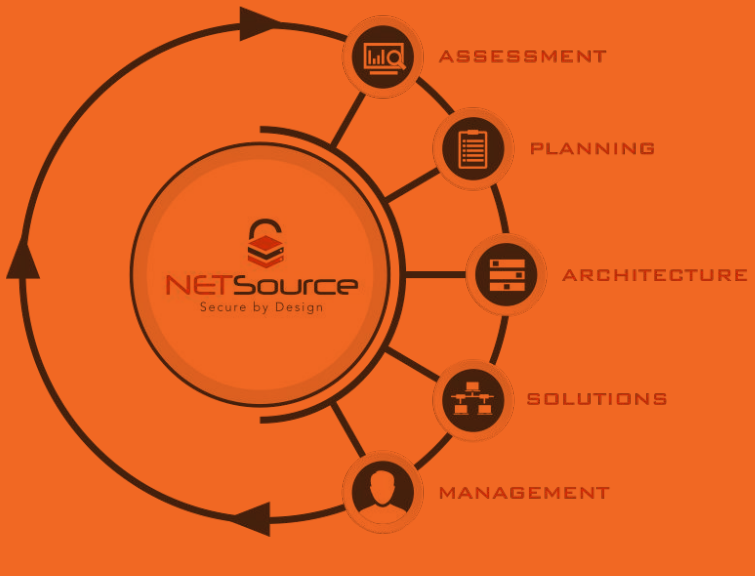
NETSecure^{SM} MOS is a key tool in preventing data breaches. It ensures the policies and internet protocols deployed are clean and efficient and that they spread to include every connected device. MOS also keeps deployments relevant, providing updates on a regular basis.

With traditional firewall appliances no longer offering protection against today's top cyberthreats, MOS is a necessity for complete security coverage and protecting internet access.

A traditional firewall basically controls the traffic that is allowed to enter or exit your network through a specific point. It doesn't possess any next-generation features, such as application awareness, identity awareness, Integrated Intrusion Protection Systems, or the ability to utilize external intelligence sources. MOS possesses all of these attributes and is seamlessly integrated with every component of the NETSource cybersecurity solution.

MOS continually monitors firewalls and provides instant notification of any perceived threats. It protects against port-hopping applications and malware, preventing access to unused services or applications that could cause security hazards on specific targets within your network. It will also help clean up networks clogged with traffic, offering ease-of-use to your employees and customers.

NETSource SUPPORT SERVICES



When you partner with NETSource, you get first-class technical support through our **24/7 Security Operations Center**. Over 50 engineers and technicians are available, day or night, to tackle your urgent issues. Additionally, we provide dedicated labs for the development and testing of customer solutions.

NETSource also has strategic partnerships with manufacturers such as Palo Alto Networks, Fortinet, Gemalto, and ForeScout, allowing priority access to their technical support teams. We can provide end-to-end, large-scale design, procurement, integration, maintenance, and management of all your data networking equipment and applications, including migrations and upgrades. We accommodate all infrastructure architectures and provide seamless coast-to-coast coverage.

NETSource will keep you informed of all technology requirements, helping you manage complexities of internal and external compliance obligations. By working with our team, clients gain a mature security position for protection against advanced threats, employee error, and network performance slowdowns.

To learn more about how NETSecure Solutions can minimize your exposure to security threats, contact one of our experts today.

www.netsourcesecure.com
(303) 948-3360

NETSource

Secure by Design

www.www.netsourcesecure.com | (303) 948-3360

[1] SecurityIntelligence | https://securityintelligence.com/media/2016-cost-data-breach-study/

[2] SecurityIntelligence | https://securityintelligence.com/20-eye-opening-cybercrime-statistics/

[3] Nerds Support | https://nerdssupport.com/rise-android-trojan/

[4] Syntonic | https://syntonic.com/byodresearch/

[5] CNBC | http://www.cnbc.com/2016/02/17/ransomware-is-targeting-us-companies-of-all-sizes.html

[6] Neustar | https://www.neustar.biz/about-us/news-room/press-releases/2016/ddos-soc

[7,8] Data Privacy Monitor | https://www.dataprivacymonitor.com/cybersecurity/deeper-dive-human-error-is-to-blame-for-most-breaches/

[9] Forbes | https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#5398c44d6832

[10] Entrepreneur | https://www.entrepreneur.com/article/284754