iSequre
MANAGED NETWORK SECURITY

12 Must Haves

For Network Security In The Ransomware Age

Table of Contents

iSequre
MANAGED NETWORK SECURITY

Overview

In today's digital world, companies must rely on their technology to help them grow their business endeavors. While technology has many perks, it also adds in the need of network security.

When it comes to network security, it is easy for small to medium sized businesses to say "not me", "they are only after the big guys." The reality is that attacks on all networks have been increasing year after year as hackers have become more sophisticated, and small businesses are also being affected every day due to relaxed or non-existent security policies. Protection is vital to growth in today's climate as shown by a cyberattack report case analysis:

1. The United States if the top target for hackers worldwide. 62% of US companies experienced a ransomware attack in 2019.
2. 74% of companies have malware activity that spread from one employee to another.
3. 61% of companies in 2020 experienced a ransomware attack that lead to a partial disruption of business operations. This was a 10% increase from the prior year.
4. 268,362 new looking malware variant attacks occurred in 2020, a 74% increase from the 2019 report which listed 153,909.
5. 3.7 million malware attacks were sent over encrypted SSL/TSL traffic. The encryption made it harder for standard freemium data programs to detect the anomalies.

With the rapid growth of new malware and ransomware variants, it is important to have a trustworthy and stable network security in place. Using freemium software downloaded online may cause issues. This guide will go through 12 essential "must haves" for your network security in the ransomware age.

1

Threat Response & Removal

1: Threat Response & Removal

Cybersecurity products on the market today lack the most important capability that a product should offer; real-time threat response.

Many freemium security softwares offer you the ability to see an infection after it occurs. While some of the threats may be removed, some may have snuck past, undetected.

The reality is that hackers will find a way to breach your network no matter how many preventative measures are put in place, and when that happens it is imperative that you have the tools necessary to put an end to the hack before mayhem occurs.

Cybercriminals will continue to target companies in hopes of securing a large, one-time payment in order to save the company from closure due to data leakage/deletion.

Having a proactive, as opposed to reactive, threat response and removal network security in place is vital.

Defenses, such as SNAP-Defense, provides this threat response; detain infected devices instantly, kicking the hacker off your network and saving your critical assets, reducing downtime, and saving your company financial stress.

2

Automated Security Awareness Training

2: Automated Security Awareness Training

With the new variants of malware, ransomware, and other threats in the digital landscape, it is vital for all employees to be technologically savvy. While they do not need to know all the ins and outs of security programming, they do need to learn to be aware of threats.

Having automated programs that test awareness of employees is a simple yet effective way to increase knowledge. This can be found in a variety of ways including:

- Training courses to take online.
- Weekly questionnaires emailed out.
- Fake “harmful” spoofing emails sent to employees that report back if clicked on.
- Fake “harmful” spoofing pop-up virus ads.

Frontiers in Computer Science did a study on the harmful nature of phishing attacks, and how it can harm more companies than expected due to a lack of security awareness training. These are the two most common attack types:

- Phishing e-Mail. A fraudulent email with a link or attachment is sent, often to a work email address. If clicked, the malware will begin downloading without the user’s approval. It may then ask for payment to unlock the computer, or it may secretly start monitoring data transfers on the servers.
- Spoofed website. An employee may find their way onto a spoofed website after a series of redirects (click-jacking). While the intended site may still appear, a fake site may be digging information in the background.

3

Access Control Configuration

3: Access Control Configuration

With multiple points of access, most IT administrators fall into the trap of having too much to manage for employees, that they have no time to focus on digital security measures.

On a daily basis, IT administrators may have to set up new user accounts, integrate repository changes, set department policies, process sign-on auditing, authorization, and more!

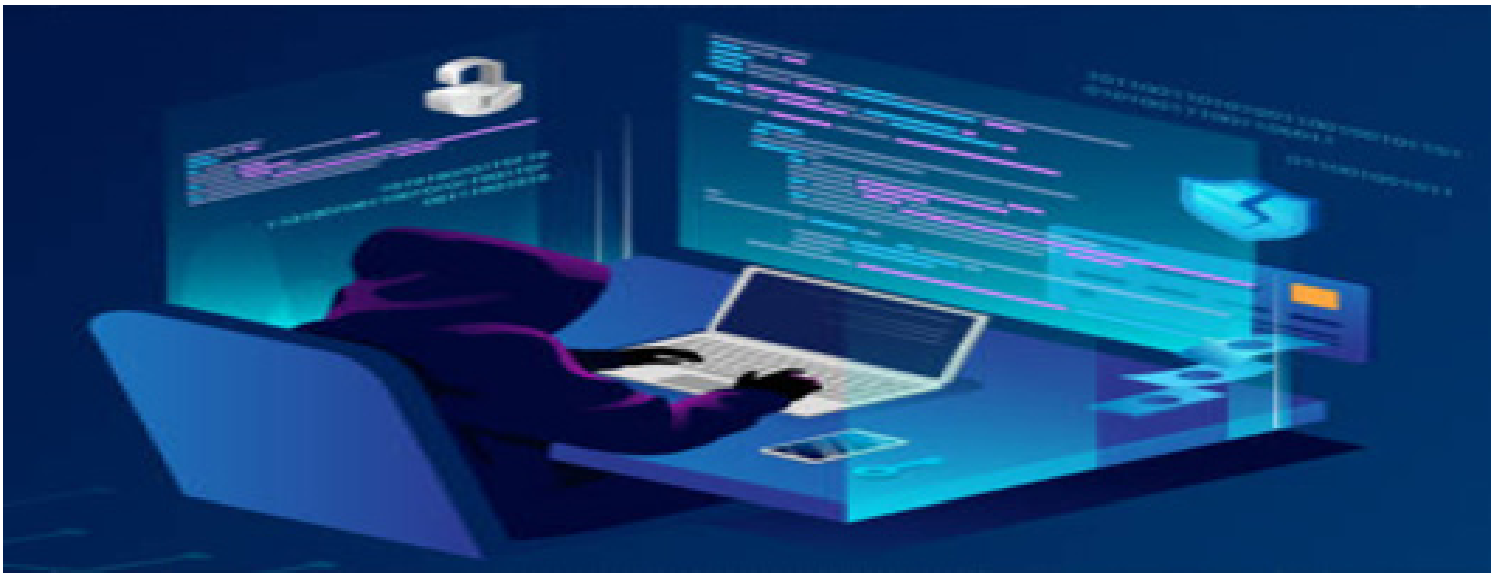
Having an access control configuration where it can be narrowed down into more user-side simplistic measures is vital to maximizing an effective IT department for a company.

Many freemium software online may find ways to help narrow down the access control processes. However, they may often be on a singular variable. Thus if the software goes down or is hacked, it may cause major downtime to the process until it is resolved. Or the software may fall prey to ransomware until paid off to restore.

For most companies, they will need to look to a dedicated external party to help out the company's IT department. This external party may help by providing their own servers that have programming to monitor multiple configurations without having to miss out on vital digital security measures.


4
Endpoint Security Forensic Software

4: Endpoint Security Forensic Software



While some hacking attempts on companies may be one-off situations, there will often be repeated attacks from the same individual(s) in hopes to get into the data servers.

It is important to have software that can not only reactively fight back attacks, but also proactively hold back attacks before they even happen.

Endpoint security forensic software allows you the ability to identify hacker behaviors, tactics, methods, and the ways they attack. Having this data handy makes it easier to see where potential attacks may happen based on prior data obtained. Not all malware attacks are easily visible, some may be hidden each time.

The software used needs to be able to check not only one user's computer being attacked, but also peer-to-peer packets being sent within a company. Forensic software allows a continual sweeping check of data servers to see if any anomalies are occurring between users. If there are anomalies, it can be reported to the system for future studies, while also stopping hacking.

Top line forensic software is able to securely observe a company's network without having to physically be in the building. It can collect data without interrupting any accepted processes that are part of the daily operations for workers. This not only provides a security boon, but it also saves money in the long-run.

5

Deep Threat Vulnerability Scanning

5: Deep Threat Vulnerability Scanning

Vulnerabilities can occur throughout servers, softwares, or systems due to misconfigurations that exist within. These misconfigurations can cause variants in which hackers can gain access and start attacking the network and/or system.

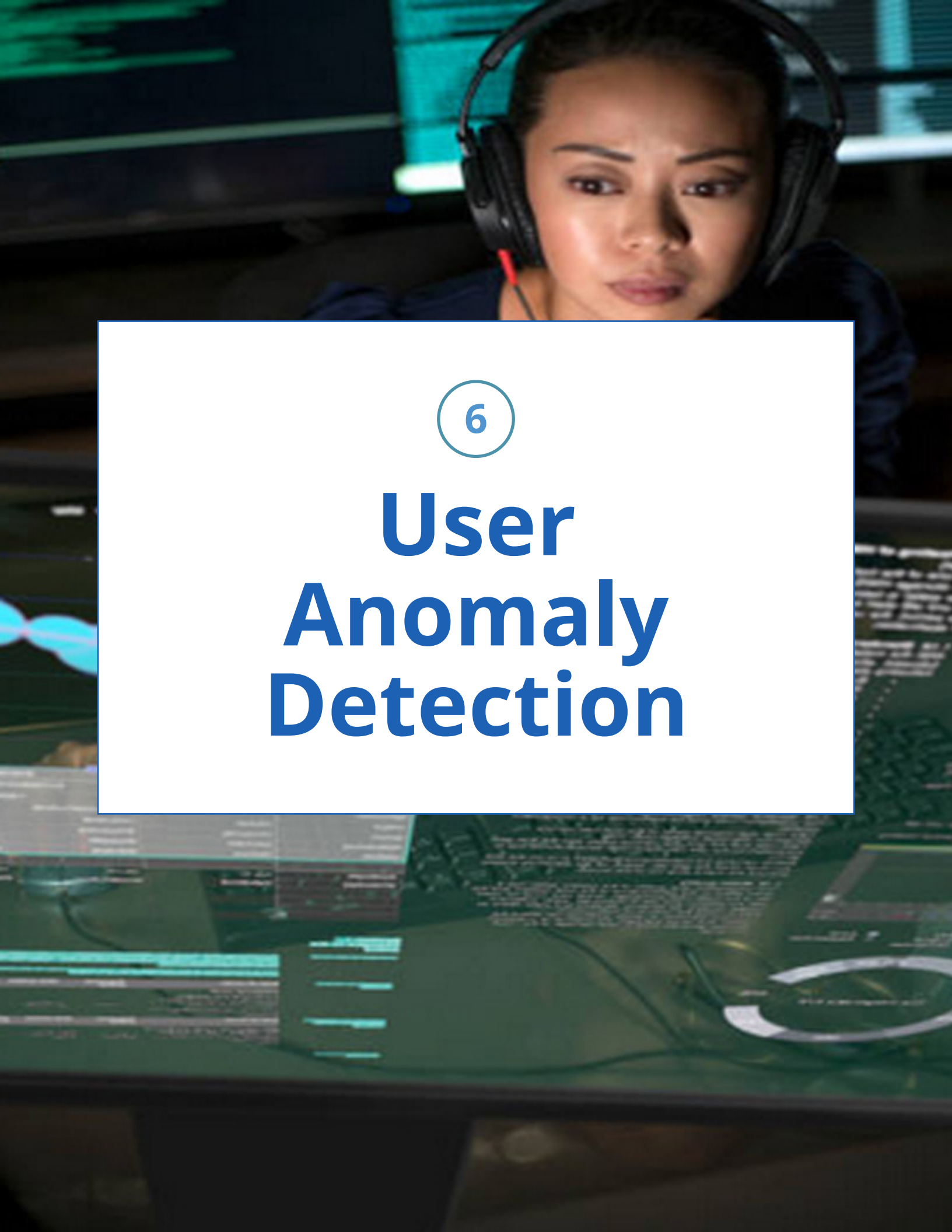
If a major vulnerability exists in one's systems, it can be easily exploited by multiple hackers with ease. Hackers are likely to target easier to access data systems that take less effort, than to focus on hard to breach security.

Vulnerability scans attempt to find variations in coding that may be flaws rather than intentional changes. Most freemium softwares will assign a threat level and inform you if deletion, quarantine, or other options are recommended.

While many freemium software programs may feature web application or software vulnerability scans, they often fail to go deep into the root issue, failing to protect company systems.

Companies should instead look towards deep threat vulnerability scanners that can cover multiple operational modalities including:

- External scanning such as packets sent from a company's firewall to guest Wi-Fi.
- Internal scanning from internal computers connected to the mainframe data systems.
- Unauthenticated scanning looks at discoverable servers that could be connected.
- Authenticated scanning are connected and have precise information packets shared.
- Limited or Comprehensive scanning scopes.



6

User Anomaly Detection

6: User Anomaly Detection

On any company network, users (employees) will be actively using the Wi-Fi, ethernet servers in order to complete and process work tasks. While in an ideal world only work sites are accessed, that is not always the case.

Personal email is a common side distraction/ necessity for employees to check during their time working. This can lead to potential threats making their way into the company servers due to finding breaches via user input.

User anomaly detection is important as software creates theoretical models to find what is normal user behavior versus unusual. If an input or DNS ping back looks far from normal, the system may flag it and prevent loading.

Finding user anomalies in a servers' network is quite simplistic if implemented correctly.

An anomaly detection can see if packets being sent back are too short to be real packets, see if broken files are being sent, or if applications are sending back data in multiple hidden layers.

If incoming traffic is quickly being flooded on the server out of nowhere it may be due to a Distributed Denial-of-Service (DDoS) attack being sent to the server(s). If detected early, it may be able to help prevent or slow the flooding.

If outgoing traffic from a normally quiet user suddenly spikes, such as opening 100 new tabs within a short time period, it may be a worm. Anomaly detection shuts down the worm.

7

Advanced Breach Detection

7: Advanced Breach Detection

Breaches can occur at a company in a variety ways including hackers gaining access to a main server data, system servers, applications, Wi-Fi networking, or other devices.

Security breaches are common for most freemium softwares to find as it will state that at “x” time “x” malicious virus attacked “x” location.

However, it may not necessarily find or prevent a data breach from occurring. A data breach is when the criminal manages to breach through security and successfully exit with important server data from a company or user. This data is then held ransom or sold on the dark web.

Advanced breach detection takes both security breaches and data breaches into the software security consideration.

By taking both into consideration, it can prevent customer data from being leaked or sold. For many companies, if data is leaked it could lead towards value loss, sustaining PR backlash, or even fines for compliance failure.

In one case, freemium antivirus software Avast was security breached in 2019. While they were also technically data breached, the hacker didn’t leak customer details and instead input malware into the programming.

8

Executive Cybersecurity Reports

8: Executive Cybersecurity Reports

Companies in any industry have an obligation to secure the information collected, whether it be client data, transaction card readings, or even third-party sales data purchased.

Additionally, each industry has their own compliance and regulations that are required to follow. It is important for your cybersecurity software to have self-auditing reports. While it may show some vulnerabilities were found, that is not a bad thing if it is resolved and you have the documentation to prove so.

Top line software programmers are able to run reports, often monthly, to ensure your safety and compliance is at the forefront of their mind as operational work is completed.

Summary report data should include:

- Outstanding alerts by critical level designation (criticality), type, and time.
- Overall system health.
- Overall system uptime/downtime status.
- Suppressed events by type and time.

Reports should also keep track of user data in your company that is taking place, including:

- Privileged users by level (e.g. new, most, least, inactive, active).
- Remote executions by user.
- Remote applications by user.
- New peer-to-peer share activity.
- New point-to-point connections.
- New USB activity by device.

9

Inbound & Outbound DNS Filtering

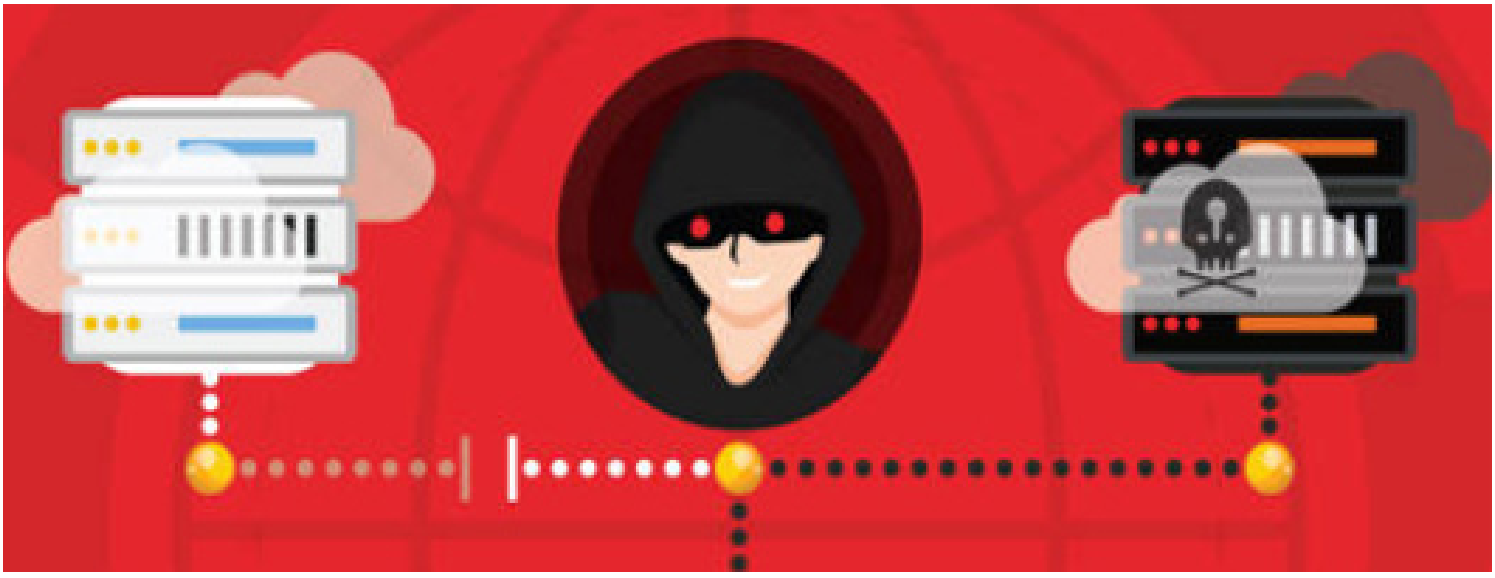
9: Inbound & Outbound DNS Filtering

Domain Name System (DNS) filtering helps prevent hackers from jumping onto your server as a website or application is loaded that leads towards a spoofed hacking. Filtering helps prevent hackers from being able to load onto user devices. If it is loaded, this allows hackers an easy way to go through a company's server and extract or lock data.

Having both inbound and outbound filtering is important. Inbound prevents the hackers from easily sending malicious data to the user. Outbound helps prevent sites that should not be viewed from being loaded.

When a user enters a domain, a DNS query is sent to a DNS resolver. It then matches the domain name with an IP address. The DNS sends the user device the correct IP address for the user to connect with. With DNS filtering, no content can be loaded prior to the DNS check process occurring.

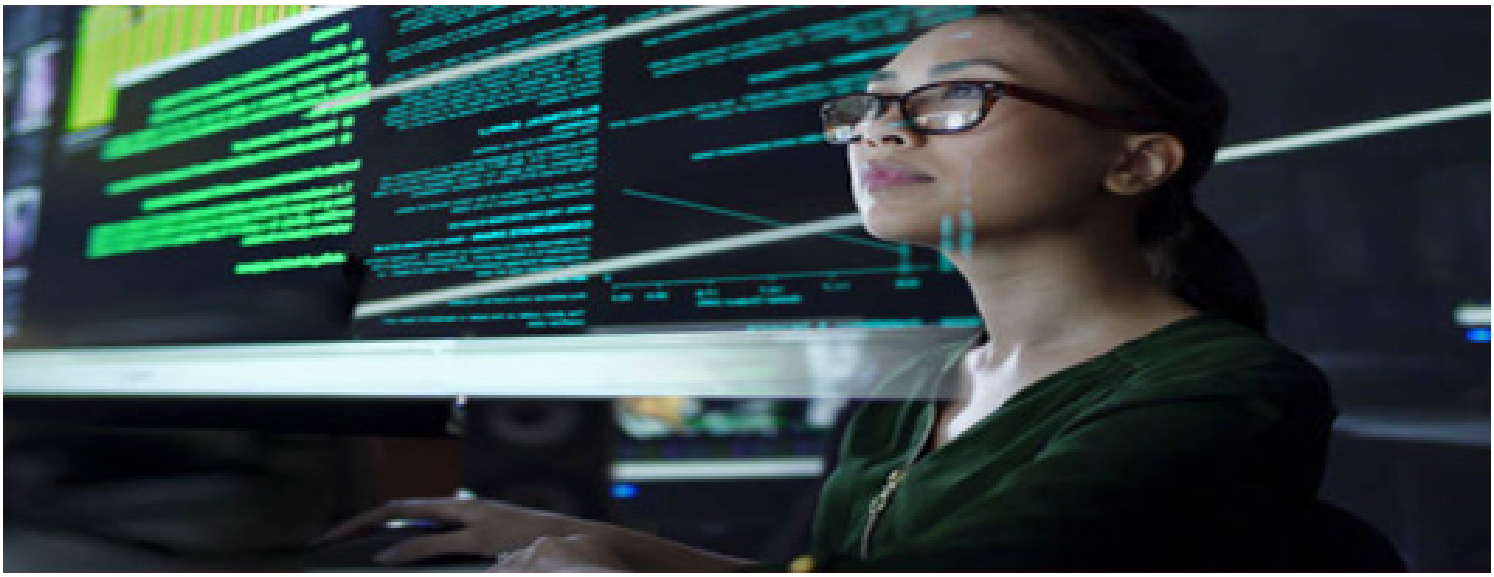
DNS filtering can block malicious properties by the domain name or IP address it sends. If by a domain name, the DNS filter will not send a query to the DNS resolver. Thus, the site will fail to load. If it's by a blocked IP address the DNS resolver will be unable to send it back to the user device, thus preventing the IP transfer.



10

24/7 Threat Detection & Monitoring

10: 24/7 Threat Detection & Monitoring



A vast majority of companies have IT staff on duty during normal working hours (primarily between 9AM and 5PM) to monitor and detect any potential incoming or present threats.

However, hackers realize this and attempt to avoid breaching during working hours. Instead, 90% of breaches occur during non-working hours due to the lack of security present.

Having a freemium software that actively monitors company employee usage during the work day may work, but a lot of them go into standby mode if the user turns off their device. Companies need a system in place that can monitor servers 24/7.

Having a system in place to detect and resolve the solution during off-hours will help grow a company by protecting valuable data and preventing ransomware.

With 24/7 threat detection and monitoring, potential weak points in the server's security system can be identified and corrected in advance before an attack can occur.

Additionally, having a 24/7 threat detection and monitoring server software in place can help save on payroll with no need to worry about hiring externally in other time zones during off-hours. Instead, the software will always be on duty and can send critical alerts if necessary.

11

2 Factor Authentication Software

11: 2 Factor Authentication Software

As 2 Factor Authentication (2FA), or multi-factor authentication, becomes a necessity in today's digital frontier, some companies do not have this implemented yet.

From a security standpoint, having 2FA as a requirement for all workers helps mask data from the average hacker. The less appealing your data looks, due to the masking, the more likely hackers would rather look towards someone who is not using 2FA.

Setting up a 2FA to be fully secure can require the use of a third-party IT specialist to set up software that is unique to your servers. Freemium software and apps exist online, but could potentially be hacked into easier.

2FA mixes logging in with a different factor to ensure you are not compromised. Common ways to ensure 2FA consist of something you have on you:

- A cellphone.
- A key card/fob.
- An authentication USB.
- A 2FA key generator stick.

Or something you are:

- Fingerprint authentication.
- Iris scanning.
- Information checking such as date of birth.
- Secret security questions.
- Face scanning software.

12

Virus & Ransomware Software

12: Virus & Ransomware Software

Computer viruses are no small laughing matter. They can infiltrate your company's data and start spreading around the server. They are sophisticated enough to find ways to damage a computer beyond repairable usage. They can even hold your data hostage and turn it into ransomware.

One of the most common uses for antivirus software is using the freemium version that a computer may be bundled with. While it is better than having nothing, a lot of the freemium antivirus softwares can only prevent intrusion of common computer hacking methods.

If you have a company of any type, having a digital security plan in place is vital to growth.

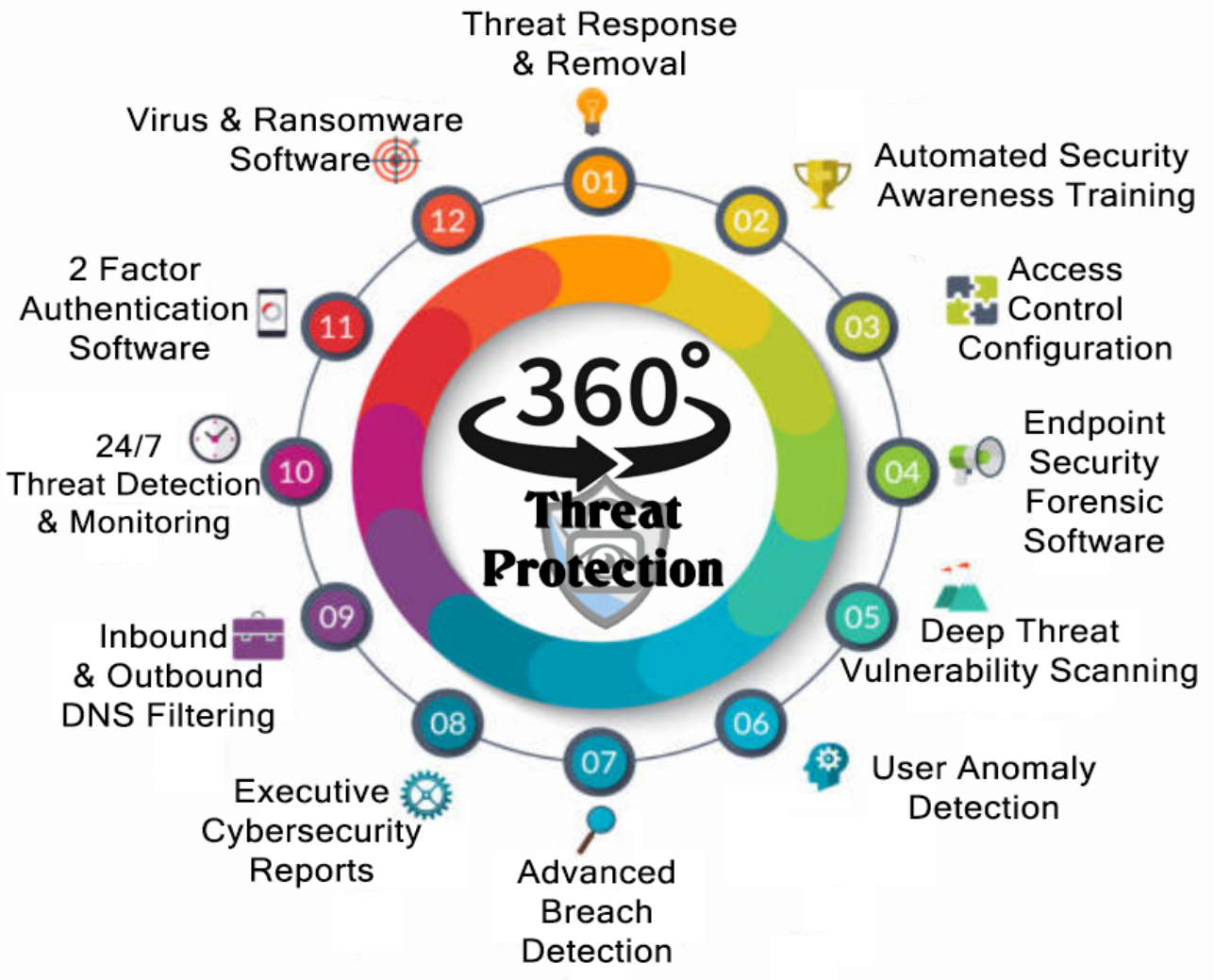
Having a quality virus and ransomware software to fight back is very important. Even if freemium seems enticing due to the low price, it may not be covering everything it needs to:

- The average cost of a data breach for companies of all sizes is approximately $200,000.
- The average ransomware payment for a small to mid-size business is $42,000.
- For most freemium antivirus programs, it takes 193 days on average to identify a data breach in the servers.
- For most freemium antivirus programs, it takes 39 days to fully contain a data breach.
- The majority (90%) of server breaches occur during non-working hours.

Resources & About iSequre

iSequre specializes in securing and optimizing your electronic assets, so you can rest easy knowing your data is secure!

With iSequre, we take your security seriously with the utmost care to stay compliant, effectively monitor your servers at all times, and help save your company time and money. Leave the stressful technical work of implementing all 12 Must Haves for Network Security to us and instead focus on other aspects of your business endeavors.



Resources

Malware 2021 Statistics

Managed IT Services

Network Security

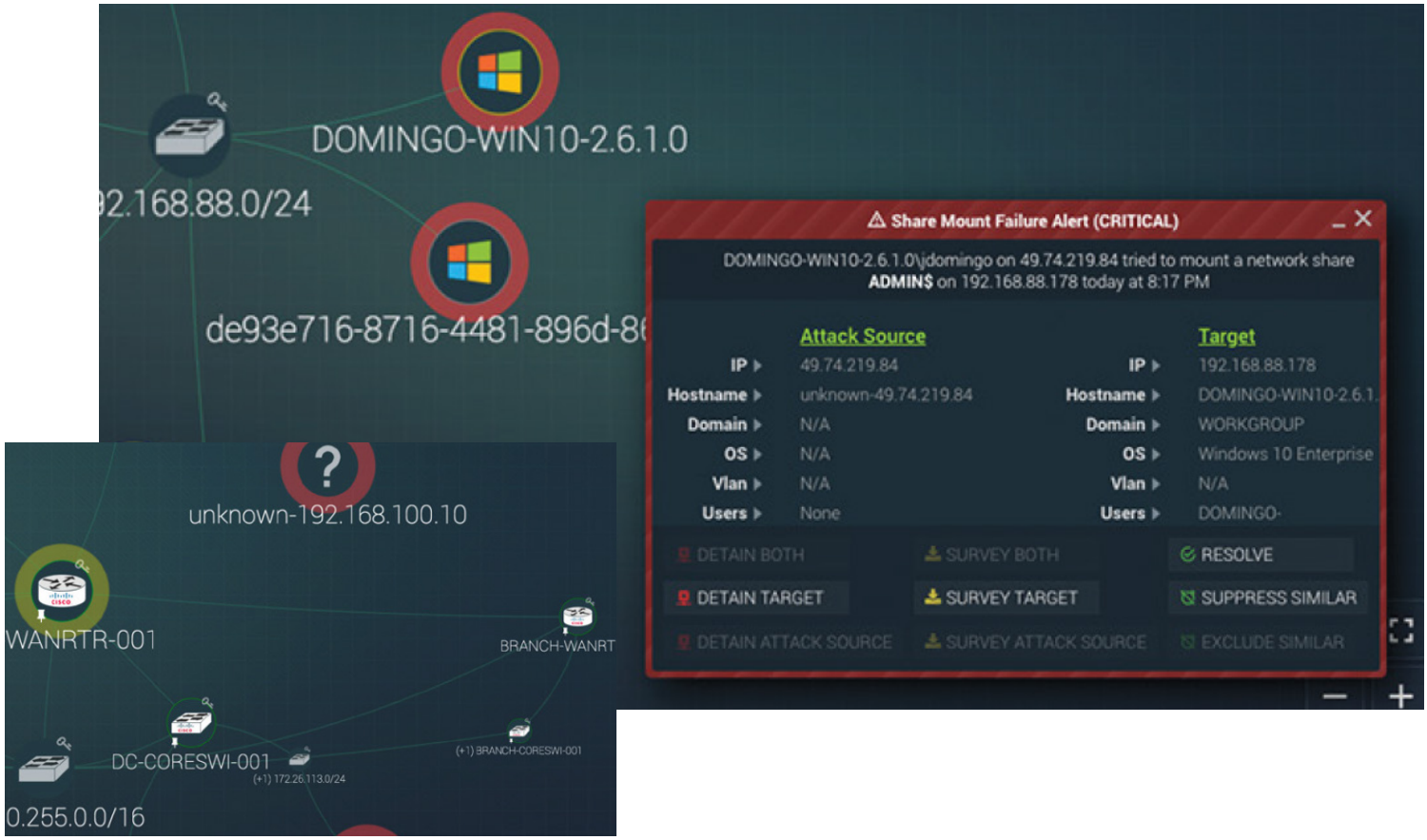
Data Backup/Recovery

Cloud Computing

Virtualization Services

Daily Security News

iSequre LinkedIn



Are you sequre from spying eyes?

Don't risk your company's digital security by placing it in the hands of a risky freemium software company that doesn't have all 12 Must Haves for Digital Security.

The average cost of a data breach for companies of all sizes is $200,000. The average ransomware payment for a small to midsized business was $42,000.

Don't risk your company's future, get all 12 Must Haves sequred now with iSequre.

Request an iSequre meeting to implement the 12 Must Haves