4 Ways to Strengthen Data Security With Network Monitoring

eBOOK

Introduction

For most IT organizations, network monitoring is an essential piece of the IT toolkit. Network monitoring tools play an important role in letting IT pros get complete visibility into the status of network devices, systems and applications, so that they know where issues exist before helpdesk tickets start coming in, keeping the IT team aware of problems with services, networks, application performance, and more.

But despite its reputation as an IT Swiss-Army Knife, there is one area where Network Monitoring tools are rarely used to their full potential: Security.

And that's too bad because you can easily put the data and insights generated by network monitoring to good use for security purposes. With a little tweaking and creative thinking, you can put the information, alerts, and reports that network monitoring tools are designed to give to work beefing up your security posture.

Think of it this way: if your network monitoring tools monitor the health of your network, and security events such as attacks or malware adversely affect the health of your network, then network monitoring tools can, in a sense, monitor for security events. And in a world where 68% of all data breaches took months or longer to discover, according to Verizon's 2018 Data Breach Investigations Report (DBIR), who wouldn't want all the help they can get monitoring for breaches?

What's more, because these tools are already in place, they can provide security value at a relatively low cost. That's good news for organizations with a limited budget for security tools.

In this eBook, we'll give you four techniques you can use to put your network monitoring solution to work for security.

Defend your Network Castle with Network Monitoring Tools.

Discover Breaches Faster By Knowing Your Network

It doesn't take long for hackers to break into networks, often it can be a matter of minutes or even mere seconds, but what matters most is what happens after they break in, and the amount of time they're afforded to move about in your network or systems. Unfortunately, 68% of data breaches take months or longer to discover, according to Verizon's 2018 DBIR. That gives hackers plenty of time to escalate their privileges, observe your network and look around for further vulnerabilities and valuable information.

A properly configured network monitoring solution can cut this discovery period drastically by giving you an understanding of how your network works and where key metrics typically stand. When things go awry, and your metrics start breaking away, your network monitoring system can alert you that something is up. This capability makes network monitoring tools useful for security forensics because, in the process of gaining access to networks, attackers often employ techniques that can reconfigure services or hosts, or even make them temporarily unavailable— precisely the kinds of conditions that network monitoring tools are designed to look for and alert on. Even something as simple as a downed machine, or ports opening when they're not supposed to can tip you off.

With a modern network monitoring tool, you can set up email notifications and alerts for changes to the configuration of network devices, and audit configuration against defined policies. WhatsUp Gold also lets users view and compare device configurations in the device properties page, and if configurations are lost, you can automate network device configuration backups for any device that supports Telnet or SSH.

A capable network monitoring tool can set up scheduled SNMP-based or system-specific discoveries on a regular basis, which can help you stay on track of changes in your environment and find new devices on your network. You can also perform ad hoc discoveries when things don't seem right. With WhatsUp Gold, you can even set up notifications and alerts via email or Slack when a discovery finds unexpected devices.

Real World Example

When Chinese hackers broke into the US Offce of Personnel Management's network in 2014, they remained undiscovered on the network for nearly a year before they were found when outbound traffc from the OPM's network pinged a suspicious URL in April 2015. By then, the hackers had made off with the personally identifiable information of 21.5 million US federal government employees.

Detect Cryptominers Using Your Resources

Cryptojacking, or hijacking other people's processing power and using it to mine cryptocurrencies, is a growing trend amongst cybercriminals. This is typically achieved with scripts that run behind the scenes on websites, though it's also possible to hijack machines and servers to run full-blown cryptocurrency mining software, which is either installed by malware or by rogue employees.

For the perpetrators, the benefit is obvious: they can mine cryptocurrencies without worrying about the taxing resource usage that comes from such activity, and if their victims are unprepared, it's easy to get a way undetected.

But with a Network Monitoring tool like WhatsUp Gold, it's easy to detect the increase in resource usage caused by cryptomining.

Regardless of the method used, mining cryptocurrency is going to be a major resource hog, which will make the machines doing it stand out. This is especially true in off-business hours when most machines will be less active, but those with cryptominers installed will continue using resources at a high rate.

With a modern network monitoring tool, like WhatsUp Gold, you can easily monitor for CPU spikes and set up alerts for when CPU usage exceeds 90% (or any other threshold you want) on machines that don't regularly perform CPU-intensive tasks. This is a simple way to keep track of your machines and find out if there's anything strange going on.

In WhatsUp Gold, monitoring for CPU spikes is a preset configuration, and blackout policies can be used to limit monitoring to off-business hours if so desired. Likewise, setting up alerts for spikes in CPU usage is easy to configure.

Real World Example

The rate of illegal cryptojacking attacks grew 459% in the first half of 2018, according to a recent report from the Cyber Threat Alliance. Cryptojackers are usually implanted on compromised websites via hidden scripts, but vulnerabilities such as EternalBlue can also deliver them. In one extreme case, Russian nuclear scientists were arrested for attempting to use one of Russia's most powerful supercomputers to mine Bitcoin.

Progress®

Detect DDoS Attacks and Anomalous Network Behavior with Network Traffic Analysis

The most apparent crossover security capability of any network monitoring tool is Network Traffic Analysis, which analyzes NetFlow, NSEL, S-Flow, J-Flow, and IPFIX records to give you granular details about who—or what— is consuming your bandwidth. This can alert you to a lot of unusual behavior, from on-the-clock Netflix binges to machines compromised by botnets, to hackers exfiltrating data.

By monitoring real-time bandwidth usage and historical bandwidth trends, network flow monitoring can proactively identify security issues like DDos attacks, unauthorized downloading and other suspicious and potentially malicious network behavior. Network flow monitoring can be your best ally for performing security forensics and analysis by automatically identifying high traffc flows to unmonitored ports, exposing unauthorized applications like file sharing and video streaming, monitoring traffic volumes between pairs of source and destinations, and detect failed connections.

Unusual patterns in ingress or egress traffc, (such as when a machine pings an unknown or suspicious IP address), are good indicators of the presence of bad actors, and further examination of IP addresses involved, the number of packets sent, the bytes per packet, and the duration of the communication can give further indication. The majority of traffc on a given network is fast, with relatively few packets of decent size. If a server begins sending small volumes of bytes via a large amount of packets over a long time period, it is likely suspicious traffic. Unusual traffic should be treated with even more suspicion during off-business hours such as nights or weekends.

As with any other metric, it's easy to set bandwidth thresholds in WhatsUp Gold, so that you can get alerts when machines behave abnormally. You can set up multiple configurable thresholds tracking the volume of traffic between conversation pairs, failed connections per host, top senders and receivers, and specific interfaces over time. Custom configurable thresholds provide even more granular tracking of network traffic. Alerts are sent when the configured thresholds are exceeded, enabling network managers to proactively troubleshoot and resolve performance bottlenecks and eliminate malicious network behavior.

This also doesn't have to cost a lot. A key feature of WhatsUp Gold is the fact that it's licensed by device rather than by element or by monitor. This means that you're paying the same amount to monitor every interface on a 12-port switch as a 120-port switch. Many network monitoring solutions charge for each interface which means administrators only bother monitoring the 'important' ones. This can leave as much as 85% of the network interfaces unmonitored which makes things much easier for malicious intruders. Monitoring every single port in your network makes it easier for you to see abnormal traffic patterns and makes it harder for them to hide.

Real World Example

A 2018 Bloomberg article accuses China of installing thousands of spy chips into Super Micro motherboards used in servers owned by Amazon, Apple, and the US Government. According to Bloomberg, the nefarious chips were first noticed when one called out to an unrecognized IP address.
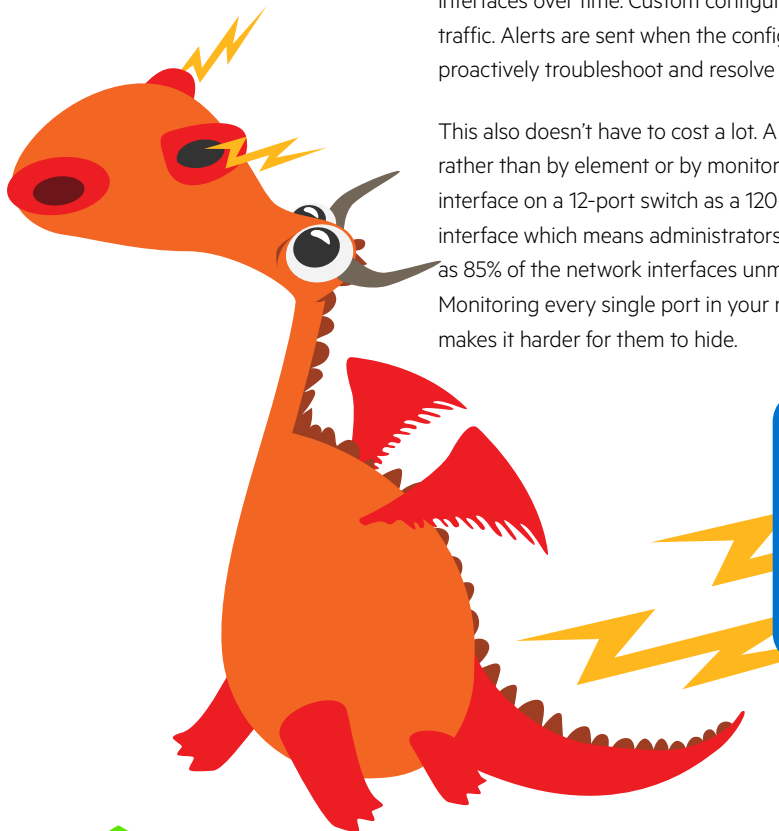
Stop Rogue Users from Exfiltrating Data and Selling your Secrets

While outsiders account for the majority of cyber-attacks, that doesn't mean they're the only threat. Insider attacks also account for a large proportion of attacks and data thefts. In fact, according to the Verizon's 2018 DBIR, 28% of all attacks involved insiders.

But managing insider threats can be one of the most difficult areas of Cybersecurity. Identity and Access Management controls are a good start, but it's also important to utilize the tools you already have, such as activity and Netflow monitoring to search for suspicious behavior.

While, sometimes, an increase in user activity may be completely explainable, other times it can indicate something more concerning. Some users may work from home to complete projects which shouldn't immediately be seen as suspicious behavior, while others may have work that calls for intensive GPU or CPU usage. That said, if an employee has sudden and dramatic increases in their activity and resource usage combined with suspicious activity, this should be cause for concern.

For example, if a member of your marketing team whose job usually involves handling social media and scheduling events is suddenly using 100 percent of their GPU, 24 hours a day, seven days a week, that's a good indicator that they're up to no good, or their machine is compromised.

If an employee is communicating with suspicious IP addresses, that can be another cause for concern. And traffic from Tor clients would be a major cause for investigation.

With WhatsUp Gold, you can alert administrators when users access the Dark Web (Tor) with a feature that monitors all Network Traffic Analyzer Sources and can alert admins when any host exceeds a configurable number of connections to known Tor ports during a set period. This allows administrators to control access to the Dark Web by their users.

Real World Example

According to a 2017 report from security firms RedOwl and IntSights, the monetization of insider access is a growing trend on dark web marketplaces. Sites such as "Kick Ass Marketplace" are increasingly paying workers to leak corporate secrets, which are vetted and offered to clients of the site for a subscription fee. The information offered up for sale can be as complex as insider trading secrets, or as simple as real estate client lists, according to the report. That site alone makes approximately $36,000 a week in subscription fees.

Progress®

How WhatsUp Gold Can Help Straighten Out Your Security Posture

WhatsUp Gold is an ideal solution for both typical network monitoring needs, and for the security cases outlined in this eBook. With WhatsUp Gold, you can get complete visibility to the status of network devices, systems, and applications, and see network devices, servers, virtual machines, cloud and wireless environments in context. Click on any device to get immediate access to a wealth of related network monitoring settings and reports so that you can see how everything is connected and get answers faster.

WhatsUp Gold also makes it easy to get detailed visibility into your network traffic to see which users, applications, and protocols are consuming bandwidth. This insight allows you to setup bandwidth usage policies, and detect unusual usage that could indicate a security issue.

What's more, WhatsUp Gold can help you avoid the negative consequences of accidental or malicious network device configuration changes with a configuration management add-on that lets you set up network devices to send an SNMP trap to WhatsUp Gold and trigger a notification whenever a configuration changes. You can even set up an action policy in the alert center to automatically initiate a backup, add or remove users, or update firmware.

Of course, none of these capabilities matter much if you aren't getting actionable alerts and reporting from your network monitoring solution. That's why it's critical to choose a solution that has a robust alerting system that can let you and your coworkers know as soon as things start to go awry.

WhatsUp Gold leverages a dependency-aware network monitor to generate more actionable alerts and features automated actions that trigger when a state change occurs, including email alerts, SMS alerts, Slack alerts, IFTTT posts, service restarts, and web alarms. WhatsUp Gold's web-based interface also makes reporting easy by quickly collecting, refining, and delivering information to your IT team, with features such as an overview dashboard, timeframe or business hour filters, and the ability to export reports in multiple formats.

For Your Free Trial of WhatsUp Gold Visit:
www.whatsupgold.com/trial

About Progress

Progress (NASDAQ: PRGS) provides the leading products to develop, deploy and manage high-impact business applications. Our comprehensive product stack is designed to make technology teams more productive and enable organizations to accelerate the creation and delivery of strategic business applications, automate the process by which apps are configured, deployed and scaled, and make critical data and content more accessible and secure—leading to competitive differentiation and business success. Learn about Progress at www.progress.com or +1-800-477-6473.

f facebook.com/progresssw

  twitter.com/progresssw

  youtube.com/progresssw

in linkedin.com/company/progress-software

Progress®