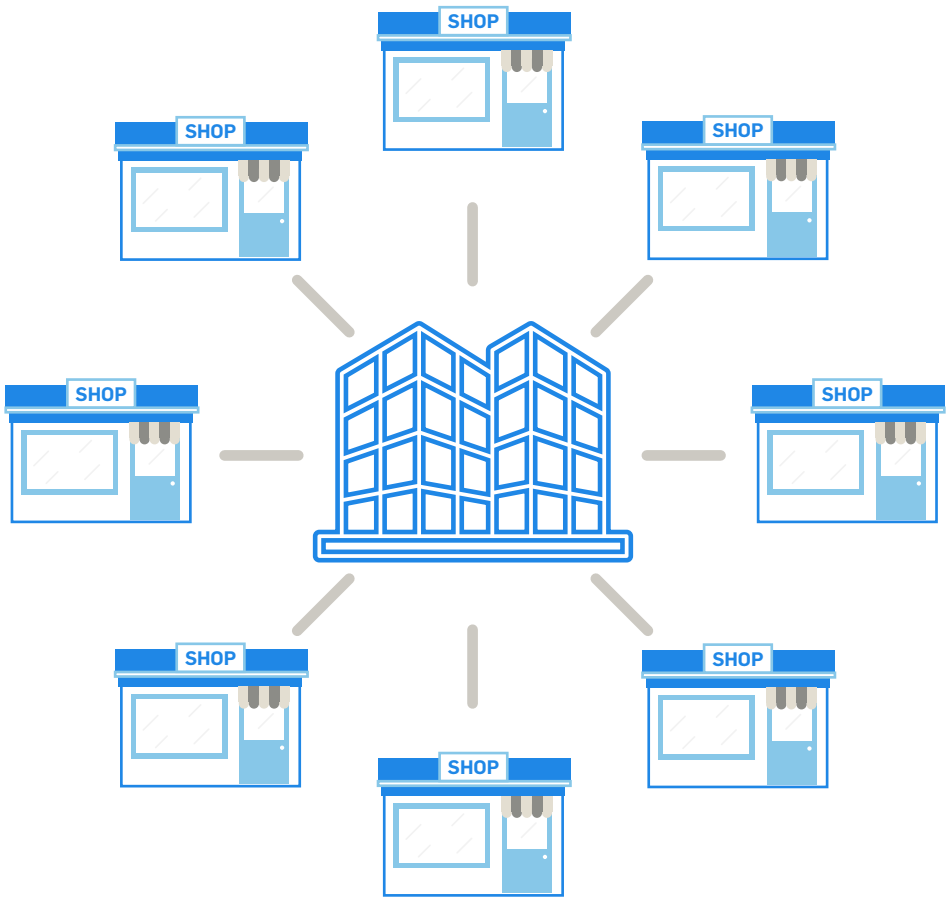
SecurityMetrics

Guide to Managed Security Services

Managed Security Solutions for Businesses



securityMETRICS®

Managed Security Overview

When it comes to data security, your in-house IT staff may be capable of maintaining a secure network, but the time and effort required to do so can become overwhelming without any outside help.

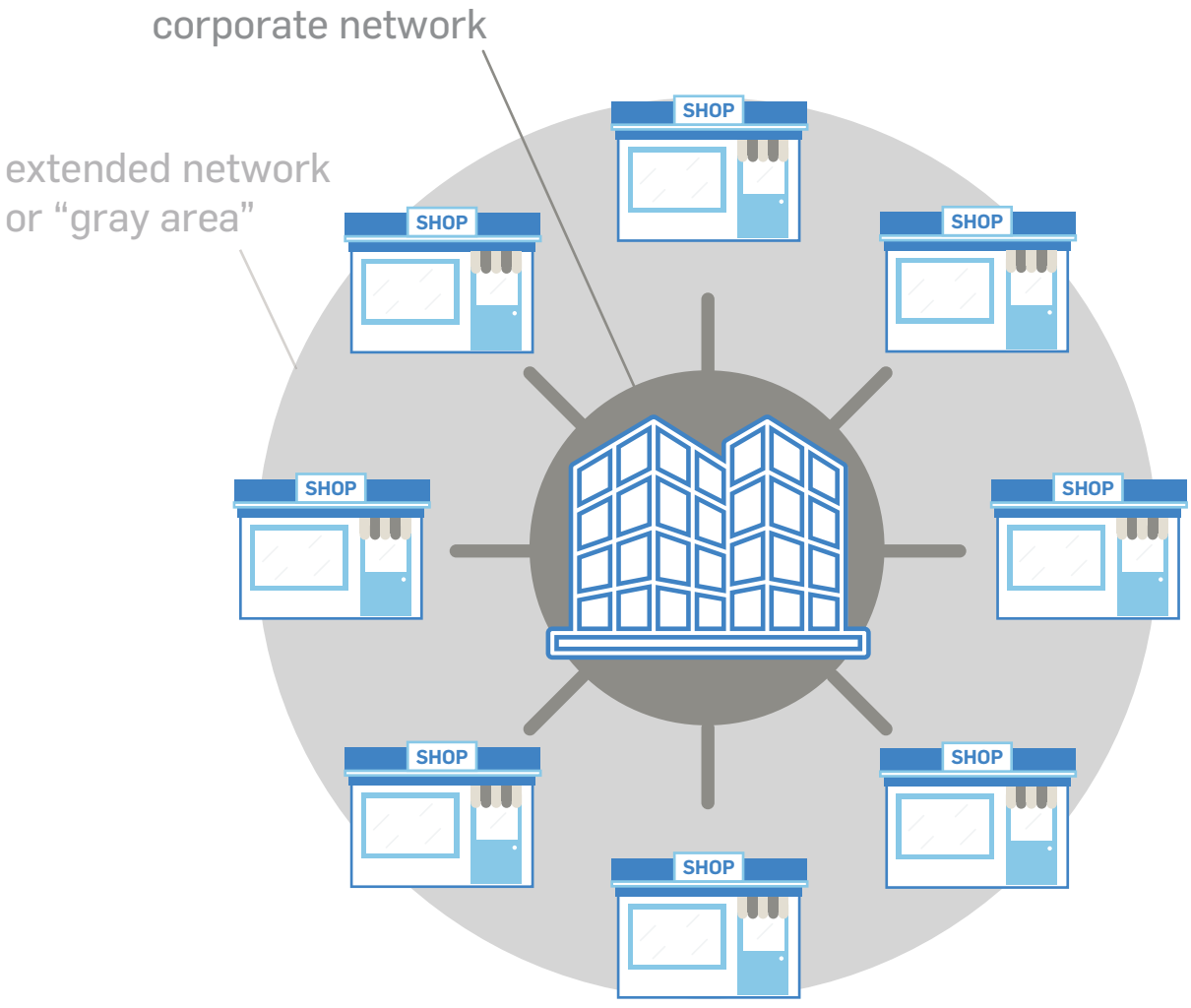
For large corporate entities, it's crucial to find a managed security company that can provide a level of visibility into your network to monitor for threats, vulnerabilities and malicious activity while also providing assurance to network owners that they are still in control of their own security and privacy.

THE "GRAY AREA NETWORK"

Large businesses and franchises often have one central headquarters and many smaller remote or satellite locations. We refer to the network that spans across all your organization's locations as your "extended network." While security efforts tend to focus on headquarters, remote locations are just as critical for your extended network security.

At SecurityMetrics, we've seen entire headquarters' operations "held ransom" by malware that was initially downloaded onto the network through a remote franchise location. Situations like this are due in part to the "gray area" that tends to surround remote locations, where the strength of data security is often unknown. How secure is your network at your franchisees' locations?

SecurityMetrics' managed security service, Pulse, provides visibility into these gray areas of your extended network so you can discover threats, take action, and stop a data breach before it happens.



Using Pulse, you can:

1. Discover vulnerabilities in your extended network
2. Understand at a glance what threatens your network
3. Take action against the vulnerabilities

Discover vulnerabilities in your extended network

Take the guesswork out of identifying threats through proven scanning, data collection, and analysis.

GET A HIGH-LEVEL VIEW INTO HOW YOUR NETWORK IS VULNERABLE

Pulse overview provides an executive level summary that includes:

- A grade of your network security health based on the risk level of your identified vulnerabilities.
- A map of your total locations and which ones are at risk.
- A risk breakdown of newly discovered, persistent, and resolved vulnerabilities.

OPERATE YOUR BUSINESS AS USUAL

Pulse sensors seamlessly collect data from your identified locations. The sensors collect data at a designated time, in the background, so you don't have to interrupt business operations.

CONSOLIDATE YOUR FIREWALL STATUS REPORTING TO A SINGLE REPORT

Pulse's centralized portal provides a report of the status of your firewalls in all your locations, saving time of manually tracking the security of your locations.

DETECT COMMON ATTACK VECTORS

Pulse internally and externally scans your network to detect common attack vectors including misconfigured firewalls and cross-site scripting.

Understand at a glance what threatens your network

Understand what threatens your network using prioritized reports in your easy-to-read dashboard.

AVOID ALERT OVERLOAD

Pulse uses machine learning and SIEM tools to identify which vulnerabilities are the most pervasive across your network, saving you and your employees from having to sift through them yourselves.

UNDERSTAND AT A DEEPER LEVEL THE THREATS POSED TO YOUR EXTENDED NETWORK

Through reports on known bad actors, known bad IPs, and port traffic. Pulse Firewall Traffic (intrusion detection) report provides traffic protocol activity allowing you to discover known bad IPs accessing your network and which ports have the most traffic. Pulse Malicious Activity report provides insight into your inbound and outbound connections with known bad actors.

PROTECT YOUR NETWORK WITH A PRIORITIZED LIST OF VULNERABILITIES THAT THREATEN YOUR SECURITY

Because Pulse scans your network for over 70,000 known vulnerabilities, its findings may reveal the need for additional work. Pulse provides a dashboard summary that outlines the total number of vulnerabilities and your most compromised locations segmented by threat level. It also identifies the top vulnerabilities at each location, ranking by risk and organizing into the following categories: outdated software/services, design flaws, network misconfigurations, and unsupported OS.

Take action against the vulnerabilities

Remediate the vulnerabilities using Pulse's location-specific technical reports.

REVIEW REMEDIATION METHODS FOR VULNERABILITIES

With each discovered vulnerability comes a recommendation on how to remediate it, saving you from having to spend time coming up with a solution on your own.

GET THE HELP YOU NEED AND UNDERSTAND YOUR THREATS BY WORKING WITH PULSE SECURITY ANALYSTS

SecurityMetrics Analysts help keep you updated with the latest attack vectors and provide support on your monthly report so you can quickly act to resolve threats.

RELY ON KNOWLEDGE FROM SEASONED VETERANS

SecurityMetrics has worked with some of the largest brands and helped secure over a million systems, which means you can get the answers you are looking for quicker.

"The relevance of ensuring proper ecommerce website security...continues to be paramount for our organization, and we could not manage this process better without the reporting tools and excellent technical expertise provided by SecurityMetrics..."

JASON DRAKE
Director of Infrastructure and Security, Premiere Sports Travel

FROM THE SECURITYMETRICS BLOG

What is Network Security?

Network security consists of the policies, procedures, programs, hardware, software, and people you use to protect your corporate network. Network security is intended to prevent unauthorized access or inadvertent exposure of protected and sensitive information like payment card data, protected health information (PHI), corporate financials, or intellectual property.

There are many steps, processes, layers, people, and technologies associated with network security. Organizations need network security tools: applications like internal/external scanning, firewalls, and log monitoring, to protect their network, detect vulnerabilities, and react to threats. They may also need to consult network data security experts to make sure they're not missing vulnerabilities or security gaps. And no security plan is complete without proper training of all stakeholders.

WHAT ARE THE FOUNDATIONS OF NETWORK SECURITY?

AUTHENTICATION

- Network security begins with usernames and passwords. This is where multi-factor authentication comes in. Security standards like the PCI DSS and NIST no longer consider single-factor authentication (i.e., a password) secure. It's far too easy to retrieve or crack passwords these days.

FIREWALLS

- Firewalls control traffic into and out of the network. For users, this translates to which websites and applications they can access. Organizations should properly configure firewalls according to their environment.

ANTIVIRUS, INTRUSION DETECTION, AND INTRUSION MANAGEMENT SYSTEMS

- Firewalls may not be able to catch everything, especially viruses and worms, so antivirus, intrusion detection (IDS), and intrusion management (SIEM) systems can help detect and stop malware.

ENCRYPTION

- Organizations sometimes encrypt communications within a network to further secure data.

EMPLOYEES

- Awareness about and training on information security is crucial to maintaining a secure network.
- Personnel must be trained for proper implementation and maintenance of network security, including making sure all security patches and hotfixes are up to date.
- Dedicated staff must be assigned to monitor and act on security alerts.
- It is important to note that these fines apply to both controllers and processors, and data 'clouds' will not be exempt from GDPR enforcement.

MANAGING NETWORK SECURITY AT FRANCHISES AND LARGE CORPORATIONS

The five areas represent some of the foundational principles of network security. However, large corporate networks and structures can enforce and manage network security in a variety of ways. Since they typically need more network security than a basic home office or small business, they usually have more resources, time, and even entire positions and departments dedicated to the matter.

In addition to the five areas listed above, large organizations will likely need to utilize some or all of the following security services to increase network security:

- **Vulnerability scanning:** Vulnerability scanning identifies big risks such as misconfigured firewalls, malware hazards, remote access vulnerabilities, and can be used for cyber security or compliance mandates like PCI DSS and HIPAA.
- **Penetration testing (also known as "ethical hacking"):** Penetration testing is a service that involves a professional penetration tester uncovering network security weaknesses at their root.
- **On-site audits:** Depending on whether you are working towards security mandate compliance (PCI, GDPR, HIPAA), you may need to schedule an onsite audit for your organization.
- **Remediation:** Do you have the personnel at your organizations to remediate a vulnerability? Or will you need a third party's help? Do you have an IT team that can open and close ports on your network? Does someone check for and regularly install patches?

PROTECTING NETWORKS FROM ATTACKS

Working backwards from large corporate data breaches, we've been able to pinpoint some of the most common attack vectors used in network breaches:

- Phishing emails
- Social engineering
- Gray area network attacks from franchise, employee, or 3rd-parties making remote connections.
- Less secure networks with intermittent access into more secure networks.

If you are a large franchise or corporate entity with many remote locations, it's crucial to find a network security company that can provide a level of visibility into your gray area networks to monitor for threats, vulnerabilities and malicious activity while also providing assurance to network owners that they are still in control of their own networks and privacy.

To Discuss Your Business's Network Security Needs, Contact Us.

801.705.5656
compliance@securitymetrics.com