Protect your extended network by using SecurityMetrics Pulse to identify vulnerabilities, utilize risk reports, and receive expert remediation advice.
SecurityMetrics Pulse provides visibility into your extended network, spanning across various locations of your organization. Many corporations have a network that extends past their main office, making their attack surface larger. Limited visibility of remote locations leaves this attack surface vulnerable. Pulse increases your visibility, allowing you to visualize threats across your extended network and prevent these vulnerabilities from being exploited.

**INCREASE VISIBILITY AND COLLECT YOUR NETWORK DATA**

Organizations expend enormous amounts of their resources protecting attack surfaces against malicious threat actors. A single, unprotected attack surface can offer a threat actor the opportunity they need to compromise your organization. Ensuring your extended network is protected, as well as your other attack surfaces, is increasingly vital.

Even if you spend millions of dollars on security products, limited visibility across your extended network can leave you unaware or guessing the location of your organization’s vulnerabilities. SecurityMetrics Pulse allows you to see your extended network locations as threat actors see them—with a multi-sensor and defense-in-depth approach. SecurityMetrics Pulse uses sensors placed in/around your organization’s different attack surfaces to monitor traffic, check for known vulnerabilities, identify bad IPs, and traffic from known threat actors.

Once the sensors gather this data, it is sent to SecurityMetrics Threat Intelligence Center (TIC) for further analysis and to generate a monthly report.
Your monthly executive-level summary report includes:

- A grade of your network security health, based on the risk-level of identified vulnerabilities.
- A breakdown of the risk level of newly discovered, persistent, and resolved vulnerabilities.
- A map of your locations and which locations are actively sending data to the SecurityMetrics TIC.

SecurityMetrics Security Information and Event Management (SIEM) software analyzes the data received from your network. SIEM software then classifies these threats according to their CVSS score risk level. Once your top vulnerabilities have been identified, Pulse provides a summary prioritizing your most critical vulnerabilities and compromised locations.
SecurityMetrics Pulse utilizes Sophos Intercept X, an endpoint security tool that focuses on protecting your locations from malware, ransomware, exploits, and viruses. Intercept X uses anti-ransomware technology to detect malicious encryption processes and stop them from spreading across your network. The endpoint then allows the SecurityMetrics TIC team to detect attack trends on your network, such as unknown threats, exploits, and hackers.

SecurityMetrics Pulse scans your locations both externally and internally to identify which network points are vulnerable, checking for misconfigured firewalls, malware hazards, and remote access vulnerabilities.

Because scan environments change frequently, it’s important you have the flexibility you need. Using vulnerability assessment tools and Perimeter Scan Portal, you can:

- Add or remove your specific targets
- Schedule your scans
- Review your results
To further free up your IT team, customers who lease their firewall from SecurityMetrics will enjoy a managed firewall service. SecurityMetrics Managed Firewall takes care of your day-to-day firewall maintenance and sends your firewall log data to SecurityMetrics Threat Intelligence Center. Your firewall will be regularly updated and managed by in-house data security and compliance experts.

Pulse also uses a centralized portal, providing a status report of all your locations’ firewalls, saving you from manually tracking each location’s security. SecurityMetrics Managed Firewall identifies if your network has encountered malware, ransomware, or other illegal activity. If this happens, a support specialist will quickly notify you to help prevent further unknown data loss and protect your organization.
Many organizations have IT teams that are overloaded with work, and prioritizing main-office attack surfaces can be easier than addressing your extended network. SecurityMetrics Pulse software detects, monitors, and hunts your cyber threats 24/7. This continuous, around-the-clock monitoring and analysis of your network traffic frees up your IT team to focus on remediation. Pulse is also engineered to help you prioritize your security efforts. Identified vulnerabilities are compiled into a prioritized action list, outlining both the total number of vulnerabilities and your most-compromised locations.

Your brand image is not limited to only your main office. When any of your locations are compromised, there can be far-reaching consequences. The SecurityMetrics Threat Intelligence Center uses the best SIEM solutions to gather your potential security incidents, review, and add contextual analysis to your threats. If one of your locations is compromised, a SecurityMetrics Threat Intelligence Center Analyst will contact you and help you make the necessary steps to prevent further damage.
Because attack vectors are continually changing and increasing, it can be challenging to devote the energy needed to learn the current threat landscape. IT teams understand the overwhelming resources required for identifying and understanding current threats. Instead of overburdening your IT or security team, you can leverage SecurityMetrics’ twenty years of data security experience.

SecurityMetrics Analysts take the time to understand and anticipate current risks so they can give you the answers you need. Using strategic planning and guidance, SecurityMetrics Analysts will work with you to strengthen your extended network office security. Your monthly Pulse report includes:

- A suggested security focus area.
- Information on the latest attack vendor trends.
- How to protect against attack vendor trends.

Armed with the most accurate threat information, ranked and identified vulnerabilities, and remediation plans, your IT or security team can strengthen your security posture.
Interested in learning more?

Request a Quote
We help customers close data security and compliance gaps to avoid data breaches. We provide managed data security services and are certified to help customers achieve the highest data security and compliance standards.

We're a:

- PCI certified Qualified Pin Assessor (QPA)
- Qualified P2PE Assessor (P2PE QSA)
- Qualified P2PE Application Assessor (P2PE PA-QSA)
- Approved Scanning Vendor (ASV)
- Qualified Payment Application Assessor (PA-QSA)
- Qualified Security Assessor (QSA)
- Certified Forensic Investigator (PFI)
- Managed Security provider with 18 years of data security experience

We help local shops as well as some of the world’s largest brands achieve data security through managed services and compliance mandates (PCI, HIPAA, HITRUST, GDPR).