Centralized Security for a Fragmented World

Help your team make sense of the ever-increasing threat of cybercrime with comprehensive coverage and insights that help protect your organization. See how Arctic Wolf helps you do more with less.

Top Threats

- Ransomware/Malware
- Cryptojacking
- Phishing
- Malicious Insider
- Data Exfiltration
- SaaS API Abuse
- Unpatched/Outdated Software
- Account Hijacking
- Cryptojacking

Current Prevention Solutions Have Proven Ineffective

- Prevention is not enough!
- Malware and exploits evade firewalls and intrusion detection systems.

Your Centralized Visibility, 24x7 Threat Detection

- SOC-as-a-Service
- SIEM
- Annual increase in businesses that find exploits are evading perimeter defenses

Comprehensive Security Comes with a Price

- Antivirus and endpoint security solutions
- Mobile devices
- Cloud applications
- SaaS applications
- IaaS cloud workloads
- Web gateways
- Routers/Switches
- Wireless access points
- Internet of Things
- On-premises endpoint solutions

SOC-as-a-Service

- Arctic Wolf's AWN CyberSOC™ service provides a single pane of glass across all attack surfaces with 24/7 monitoring and comprehensive visibility.
- Our vendor-agnostic model leverages your existing investments, at a predictable price, which includes vulnerability assessment, real-time threat intelligence, custom reporting, and access to a Concierge Security™ team of experts assigned to secure your business.
- Arctic Wolf's AWN CyberSOC™ service is the answer to the challenges of today's fragmented security environment.

More businesses find that exploits and malware evade their firewalls and intrusion detection systems. A siloed approach to cybersecurity will no longer work.

As companies rely more heavily on SaaS applications, security solutions and strategies developed in isolation aren’t adequate to secure them. Today’s cyberthreats are more sophisticated than ever before. Data breaches can originate from on-premises infrastructure, the cloud, or endpoints. Cybercriminals can also move laterally between these disparate systems.

Only large enterprises typically have the budget and skillset to build, maintain and staff a SOC. Especially as today’s skills gap keeps widening and security experts command higher salaries than ever before.

Arctic Wolf’s SOC-as-a-service provides all the people, process and technology you need to ensure your business is always secure. Each customer has a dedicated Concierge Security™ team that monitors their systems around the clock, and detects and responds to threats in a timely fashion to make sure your business is always secure.

A SIEM is a powerful tool, and is the essential component of a SOC. But it can overwhelm IT professionals with its deployment complexity and need for constant care and feeding. For many companies, it becomes very costly shelfware.

Percentage of daily alerts that aren’t investigated

- 8 to 12%

The number of in-house security analysts and incident responders needed for 24/7 monitoring

- 44%

The three-year cost of building and maintaining a SOC, including a SIEM, vulnerability scanning, threat intelligence, and the security experts needed to manage it

- $2.365 M

Average number of days it takes to discover a data breach

- 214

Unfilled U.S. Cybersecurity Jobs

- 285,000

Unpatched/Outdated Software

- 81%

Annual increase in businesses that find malware evades their antivirus solutions

- 66%

Cloud

- The approximate number of cloud-based incidents businesses experience each month

- 23

Technological Complexity

- 86

Budget Constraints and Skills Shortage

- 81

Arctic Wolf’s AWN CyberSOC™ service provides a single pane of glass across all attack surfaces with 24/7 monitoring and comprehensive visibility. Our vendor-agnostic model leverages your existing investments, at a predictable price, which includes vulnerability assessment, real-time threat intelligence, custom reporting, and access to a Concierge Security™ team of experts assigned to secure your business.

Arctic Wolf’s AWN CyberSOC™ service is the answer to the challenges of today’s fragmented security environment.