INFOGRAPHIC

Centralized Security for a Fragmented World

While the cloud unlocks great new possibilities, it also creates new attack surfaces and leaves companies more exposed to cyberattacks. Today's companies must secure data not only on-premises, but also on endpoints and in the cloud.

Top Threats

Today's cyberthreats are more sophisticated than ever before. Data breaches originate from on-premises infrastructure, the cloud, and endpoints. Cybercriminals are also able to move laterally between these disparate systems.

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- Unpatched/ Outdated Software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

Current Prevention Solutions Are Ultimately Ineffective

As companies rely more heavily on SaaS applications, security solutions and strategies developed in isolation aren't adequate to secure them. A siloed approach to cybersecurity will no longer work.

On-Premises

66%

Annual increase in businesses that find exploits are evading perimeter defenses
Ponemon Research, 2017

"Prevention is not enough!" More businesses find that exploits and malware evade their firewalls and intrusion detection systems

Endpoints

81%

Annual increase in businesses that find malware evades their antivirus solutions
Ponemon Research, 2017

Antivirus solutions haven't kept up with new malware strains and have become increasingly porous.

Cloud

23

The approximate number of cloud-based incidents businesses experience each month
McAfee Cloud Adoption and Risk Report 2016

The cloud expands the attack surface and creates an added burden for IT and security teams

Comprehensive Security Comes with a Price

What companies need is the technology, repeatable processes, and skilled expertise in a security operations center (SOC), with 24 x7 monitoring and complete visibility of all systems on-premises and in the cloud.

Technological Complexity

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 shelf-ware.

44%

Percentage of daily alerts that aren't investigated
Cisco Research 2018

214

Average number of days it takes to discover a data breach
Ponemon Institute's Global 2017 Cost of a Data Breach Study

8 to 12

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

Budget Constraints and Skills Shortage

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.

$2.365 M

The three-year cost of bulding and maintaining a SOC, including a SIEM, vulnerability scanning, threat intelligence, and the security experts needed to manage it
Frost & Sullivan 2018 report

285,000

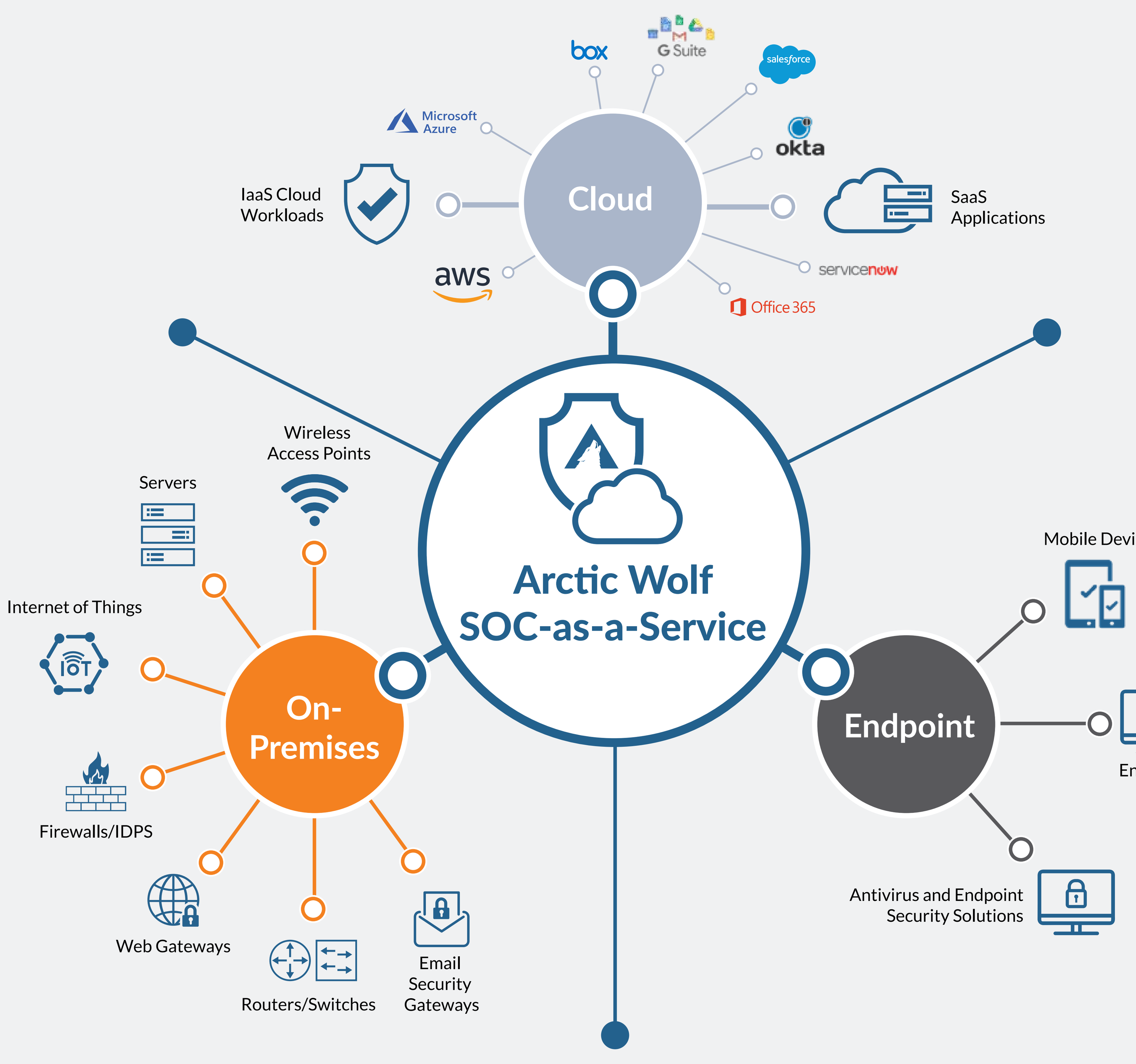
Unfilled U.S. cybersecurity jobs
National Initiative for Cybersecurity Education (NICE), 2017

SOC-as-a-Service

Your Centralized Visibility, 24x 7 Threat Detection

Arctic Wolf's SOC-as-a-service provides all the people, process, and technology you need to ensure you stay secure from cyberthreats whether on-premises or in the cloud. Each customer has a dedicated Concierge Security™ Team that monitors your systems around the clock, and detects and responds to threats in a timely fashion to make sure your business is always secure.

The Arctic Wolf SOC-as-a-Service Is the Answer



The Arctic Wolf SOC-as-a-service provides a single pane of glass across all attack surfaces with 24x7 monitoring for 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.

Read the White Paper on

Cloud Security: Combat Threats to Your SaaS-Powered Business.

Download Now