

# 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 can originate from on-premises

infrastructure, the cloud, or endpoints. Cybercriminals can also move laterally between these disparate systems.





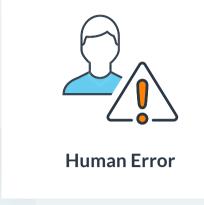


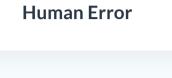
Unpatched/ **Outdated Software** 

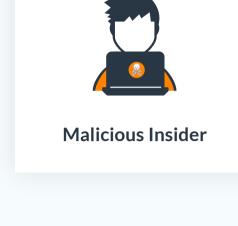














**Current Prevention Solutions** 

### **Have Proven 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



Annual increase in

businesses that find

exploits are evading perimeter defenses

Ponemon Research, 2017

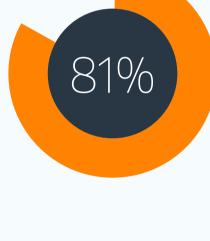
and intrusion detection systems

More businesses find that exploits

and malware evade their firewalls

"Prevention is not enough!"

**Endpoints** 



Annual increase in

antivirus solutions

businesses that find

malware evades their

Antivirus solutions haven't kept

up with new malware strains and

have become increasingly porous.

Cloud



Risk Report 2016

The approximate

number of cloud-based

experience each month McAfee Cloud Adoption and

incidents businesses

The cloud expands the attack

surface and creates an added

burden for IT and security teams

### 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.

**Comprehensive Security** 

**Comes with a Price** 

Technological **Budget Constraints and** Complexity Skills Shortage

## shelfware.

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

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



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



The number of in-house

security analysts and incident

responders needed for

Only large enterprises typically have the budget

Especially as today's skills gap keeps widening and

and skillset to build, maintain and staff a SOC.

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

285,00 Unfilled U.S. Cybersecurity Jobs National Initiative for Cybersecurity Education (NICE), 2017



**Applications** 

Cloud

aws •

laaS Cloud

Workloads

Wireless **Access Points** 

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<sup>™</sup> 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.

Arctic Wolf's AWN CyberSOC™ Service Is the Answer



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

Read the White Paper on **Cloud Security: Combat Threats** to Your SaaS-Powered Business. Download Now

