WHITEPAPER

Securing Cloud Infrastructure and Applications with a SOC-as-a-Service

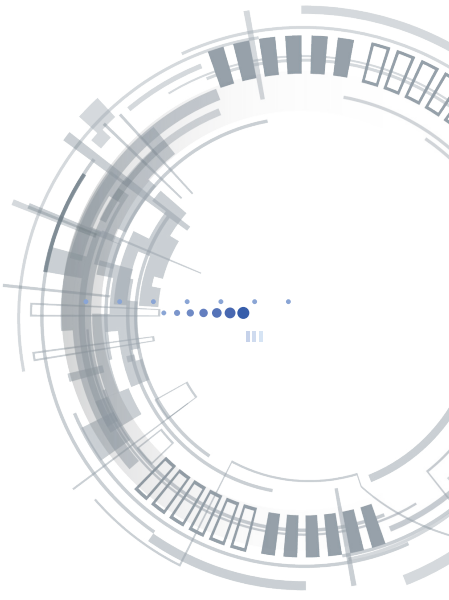
Arctic Wolf Networks protects midsized enterprises that increasingly depend on cloud services

Now, more than a decade into the cloud computing revolution, cloud deployments are routine for organizations of all sizes and industries. Many concerns that slowed early cloud adoption, including security concerns, have proven unfounded. Modern cloud services are generally seen as secure, reliable, and an important part of most business strategies. Today, infrastructure-as-a-service (IaaS) public clouds enable rapid deployment of computing resources, flexible reconfiguration and affordable pricing. And software-as-a-service (SaaS) tools are increasingly embedded within ordinary business activities, allowing low-cost outsourcing of important back-office functions.

Modern enterprises often use a hybrid computing architecture consisting of both on-premises and cloud-based resources, which poses new challenges in terms of security. As cyberattacks grow more common, and bad actors increasingly exploit the cloud to threaten businesses, IT professionals need robust cloud security strategies to protect their companies.

This whitepaper discusses the hybrid architecture of modern business, and how it increases exposure to all major types of cyberattacks. It also reviews the division of security responsibilities between customers and cloud vendors. Additionally, it explores solutions that cloud users can employ to secure their data and systems, with a focus on the comprehensiveness, effectiveness, and affordability of security operations center (SOC)-as-a-service solutions like Arctic Wolf's AWN CyberSOC™.

"As cyberattacks grow more common, and bad actors increasingly exploit the cloud...IT professionals need robust cloud security strategies to protect their companies."



The Hybrid Cloud Architectures for the Modern Business

Companies have data on-premises and in any of these three major cloud environments:

Infrastructure-as-a-Service

Many companies host some or all of their proprietary applications stacks in infrastructure-as-a-service (IaaS) platforms, such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform and others.

In an IaaS cloud, the cloud provider makes storage and compute resources available for companies to run their own code. The IaaS provider defines hardware requirements, controls physical security and access, and may deploy virtual compute instances (so that customer code does not need to run on bare metal). The customer defines what software runs in the cloud, and can use the IaaS instances for any compatible application.

Platform-as-a-Service

Another cloud option is platform-as-a-service (PaaS). A PaaS provider, such as Oracle, IBM or Cloud Foundry, establishes an operating environment in which end users can run any compatible code. A PaaS solution thus provides a balance of flexibility as well as a streamlined setup, as users are not required to define and install operating systems.

Software-as-a-Service

The final major component of a business architecture are software-as-a-service products, including corporate tools such as Google Office or Microsoft Office 365, sales tools like Salesforce, HR tools such as Workday, and countless others. In a SaaS product, the vendor operates and maintains all necessary hardware and software, and company end users simply use the software application that runs in the cloud as if it were managed on-premises.

Security-as-a-service (SecaaS) is a specialized subset of SaaS providers who provide security services in the cloud, such as identity-as-a-service (IDaaS) with companies like Okta, Ping Identity, and security operations center (SOC)-as-a-service, which enables companies to monitor cloud systems, regardless of architecture. Arctic Wolf Networks is one of the leading providers of SOC-as-a-service.

Hybrid Cloud Architectures

Most companies begin with their data and applications on-premises. This includes laptops, desktops and mobile devices, as well as on-site computer systems that aren't directly used by employees. Company IT teams retain control over hardware, software and networking, and internal security teams can freely set their own security policies.

Now, as collaboration with external partners, suppliers and customers grows and IT budgets shrink, companies increasingly migrate many of their applications and data to the cloud. However, companies often retain their most sensitive and confidential information in on-site servers and private data centers.

This has led to a pervasive use of hybrid-cloud environments, where data is distributed across on-premises and multiple cloud environments—IaaS, PaaS, or SaaS. This means the responsibility for securing data is likewise distributed across multiple service providers and the originating company. Therefore, the company must have comprehensive visibility of user activity across on-premises applications and all three types of cloud architectures.

Every Cyber Threat Menaces the Cloud

Although the earliest fears regarding cloud security have proven overblown, cyber threats don't discriminate between cloud-based and on-premises data and applications.

While the widespread adoption of cloud technologies represents a genuine transformation of business architectures, the broad categories of cyberattacks remain the same, driven by the same underlying set of motivations.

Attack Category	Description	Examples
Theft	Any attack where cybercriminals attempt to acquire and remove sensitive data—IP, customer data, etc.	In general, "data breaches" fall into this category; Target (2014), Equifax (2017), and Yahoo (2013-14) are famous examples.
Resource Misuse	An attack where bad actors, either internal or external, seek to use computing resources for their private purposes.	Bitcoin mining and running personal web services with company resources are examples of this type of attack.
Destruction + Disruption	An attack that interferes with an organization's activities, rather than acquiring something of value.	DDoS attacks are the major example of this category of cyber threat, but attacks where malicious hackers delete records rather than steal them also qualify.
Extortion	An attack where hackers threaten an organization with theft, destruction or disruption, and demand payment in exchange for not acting upon the proposed threat.	Ransomware attacks like WannaCry or Petya are automated extortion; the Uber attack (2016) involved hand-crafted extortion.

None of these attacks are unique to the cloud, but all can be perpetrated against any cloud platform. Indeed, some of these attacks can be facilitated by the cloud. The cloud makes data accessible from multiple locations, streamlining theft. The cloud delivers rapid, low-touch provisioning and deployment of resources, allowing bad actors to misuse it without filing a ticket or installing a server. In theory, there's never downtime with the cloud, which leaves businesses especially vulnerable to disruption. In fact, each of these features puts organizations at greater risk.

Given companies' increasing reliance on cloud services, the cloud represents a continuously higher percentage of an organization's surface area of risk. And as cloud deployments grow, so do the vulnerable points within an organization that hackers may attempt to exploit.

Security in the Cloud Is Not Automatic

Businesses have grown accustomed to the benefits the cloud provides. Many of these benefits fall under the broad heading of outsourcing, where IT teams can brush aside formerly burdensome tasks and challenges and say, "That's the cloud provider's problem." When a business sets up a new AWS EC2 instance, or adds a new user to Salesforce, IT staff do not need to rack new hardware, or install software on additional machines.

But security in the cloud is not automatic. While cloud providers deliver certain components of an overall security strategy, they represent security partners, not a security solution. The balance of shared responsibilities shifts between the cloud provider and end user depending on the type of cloud environment. But regardless of that balance, the end user has a clear security role to play.

SaaS	PaaS	IaaS	On Premises
• User Policies • Administrators	• User Policies • Administrators	• User Policies • Administrators	• User Policies • Administrators
• Applications • Database	• Applications • Database	• Applications • Database	• Applications • Database
• Operating System	• Operating System	• Operating System	• Operating System
• Servers • Storage • Data Center	• Servers • Storage • Data Center	• Servers • Storage • Data Center	• Servers • Storage • Data Center

Shaded areas = Company responsibility **Unshaded areas =** Provider responsibility

Even with SaaS, organizations must set the correct user permissions and policies for appropriate access to SaaS data, and only a security expert with insight into the organization is equipped to effectively monitor the SaaS instance. SaaS vendors typically do not offer such an expert as part of their product. In fact, SaaS products are designed to drive margin improvement by automating as many processes as possible.

With an IaaS cloud provider, organizations also assume responsibility for the security of their cloud applications and data. IaaS providers generally execute any software made available to them—which means they don't certify that software is secure. And IaaS cloud providers may not have the instrumentation or monitoring capabilities to detect application-level intrusions.

Effectively Securing the Cloud

For the many reasons previously mentioned, cloud security remains essential for today's hybrid business architectures. Organizations must adopt some cloud security strategy, and their options fall into three basic categories: use of native tooling, cloud-specific security vendors, and integrated service solutions.

Native Tooling + DIY

All reputable cloud services come with native instrumentation, which can be used to monitor cloud instances. In AWS, the flagship tracking tools are CloudTrail and CloudWatch. CloudTrail records all API calls to an AWS account; CloudWatch collects and tracks multiple types of records across an instance. In Azure, a similar (though not identical) set of capabilities are offered through Azure Application Insights and Azure Monitor.

Since instrumentation can generally be accessed at no additional charge, it can be tempting for businesses to simply attempt a "DIY" integration of these services with their existing security tools and workflows. However, no additional charge does not mean no additional cost. Most organizations find that the DIY approach to security ends up costing far more than any of the alternatives.

Why? Well, to "use native instrumentation" does not mean that security analysts should simply stare at the raw data feeds from CloudTrail and CloudWatch. Instead, security engineers and other developers must build integrations, connecting cloud instrumentation to log analysis platforms. This is a demanding task; it can take experienced developers a substantial amount of time to build, test and validate log parsers. And the work is not complete when the integration is built. Instead, engineers must maintain, update and modify the integration to ensure that the internal log tracking solution continues to function optimally.

Engineers must also build out security rules, and identify which log data and combinations of log data should escalate to security alerts. Security rules are potentially more volatile than integrations; they must be continually updated not merely to reflect changing software, but also as a response to new threats and indicators of compromise, as well as new company policies.

In the end, this complex and homegrown technology must be constantly monitored by trained security experts, at additional expense, making DIY security solutions neither secure nor affordable for most companies.

Cloud-Specific Security Vendors

Because it is impractical to apply existing on-premises security resources to the cloud, businesses must purchase a cloud security solution. Cloud-exclusive offerings may offer a wealth of cloud-specific features and expertise. However, exclusive reliance on such vendors represents a dead end in today's hybrid business environment.

For security to be truly effective, security experts must have access to a holistic view of a business's entire systems through a single pane of glass. This comprehensive view enables analysts to detect attacks along any vector and, crucially, view attacks that rely on multiple means of attack. For example, a phishing attack against on-premises systems could gather employee credentials and passwords, and then those passwords could be used on cloud instances, in order to hijack an account with the appropriate security or data-access permissions. Without an integrated solution, the cloud dimension of this attack could go undetected. Even if the on-premises element of the phishing attack is rapidly detected and remediated, hackers could still make off with important company data.

Additional access control and security sensors located within the cloud are always welcome, but can only do so much. Unless businesses purchase a solution that integrates and analyzes data from across all sources, including the cloud, their overall defense will be fragmented and ineffective.

Integrated Hybrid Cloud Monitoring Solutions

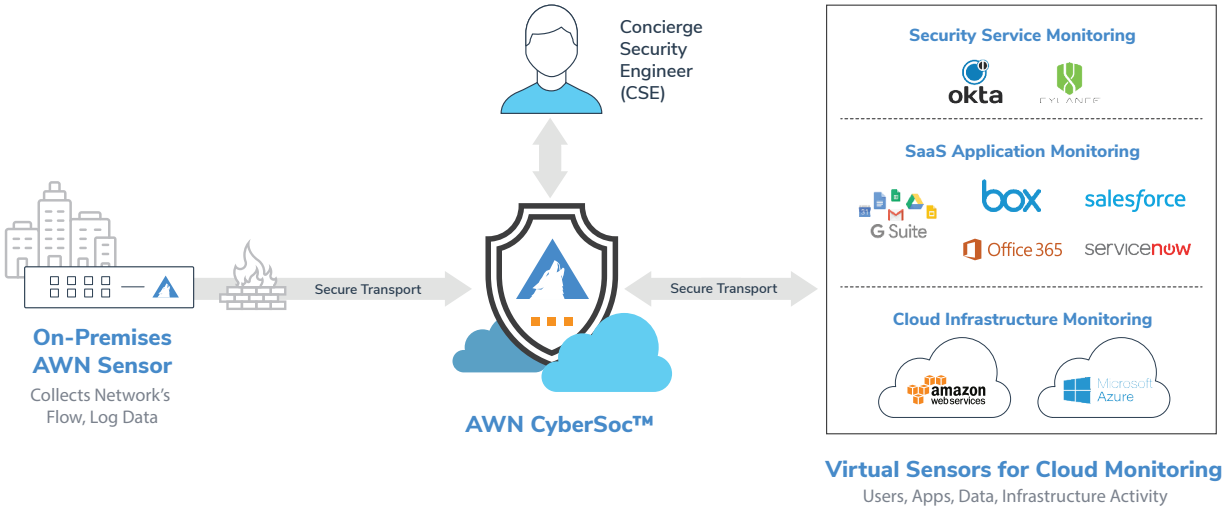
Effective cloud security solutions fully integrate with on-premises solutions. A cloud security strategy may involve specialized access control for cloud users, and dedicated endpoint instrumentation on cloud systems. The lynchpin of successful cloud security, however, is having a single, integrated monitoring service that provides visibility across both cloud and on-premises systems, allowing security experts to detect attacks wherever they threaten your business.

Of course, there are many varieties of integrated hybrid cloud security solutions. They range from software solutions that customers must install, maintain and monitor themselves; to co-managed security services; to SOC-as-a-service (SOCaaS) offerings, which directly provide managed detection and response (MDR) capabilities.

This last category can be the most attractive to companies that seek to rapidly and effectively secure their entire hybrid architecture. Unlike on-premises or co-managed services, SOCaaS providers deliver the technology, people and process required to entirely secure a company's systems without the burden of slow-moving rollouts and expensive and staff-intensive in-house monitoring activities.

Arctic Wolf Networks' Hybrid Cloud Monitoring Solutions

AWN CyberSOC™ differs from traditional managed security services. It is a dynamic combination of world-class Concierge Security Engineers (CSEs), advanced machine learning, and comprehensive, up-to-the-minute threat intelligence. Your CSE conducts both routine and non-routine tasks to protect you from known and emerging threats.



AWN CyberSOC™ for the Cloud

The cloud-based AWN CyberSOC™ provides comprehensive visibility into your IaaS cloud resources such as AWS and Azure, and monitors network traffic flows by using native APIs. The AWN cloud security solution provides:

- 24x7 cloud monitoring to detect unauthorized access or misuse of your resources
- The expertise of the AWN Concierge Security Engineer (CSE) who becomes the trusted security advisor to your IT team
- A unified view of your attack surface across both on-premises network infrastructure and your cloud-based applications, whether IaaS or SaaS

AWN CyberSOC™ for IaaS

AWN CyberSOC™ enables you to detect and respond to the following types of IaaS events and alerts:

- **Detects suspicious resource usage:** including unauthorized access to web console; stop, reboot, terminate instances; massive resource deletions; create new users and security groups; update user profiles; and upload/delete certificates
- **Detects IaaS attacks:** including brute force login attacks, concurrent access from multiple geolocations, sign-in from blacklisted IPs, and suspicious administrative actions

Pre-defined AWS Alerts—AWS is the premier IaaS platform, and used by the vast majority of companies with cloud deployments. AWN provides streamlined monitoring for AWS, including 100+ alerting rules based on AWS CIS Benchmark, with simplified setup via the CloudFormation template. It also provides comprehensive log capture using CloudWatch to monitor AWS resources, and captures network flow data using VPC Flows, as well as captures security and application logs.

AWN CyberSOC™ for SaaS

AWN CyberSOC™ enables you to detect and respond to the following types of SaaS events and alerts:

- **Detects suspicious SaaS actions:** which includes modifications to authentication settings; anomalous sign-in activity and anomalous user account status; user password changes and resets; unauthorized, geo-based access; settings updates, rules creation, etc; and DLP rule violations, including anonymous links to file resources and ACL updates, as well as resource downloads/uploads, renames, deletions and more
- **Detects unauthorized access of the SaaS application.** This could include brute force login attacks, concurrent access from multiple geolocations, and uploading or downloading sensitive data

Pre-defined Office365 Alerts—Office365 is the predominant SaaS office platform, and AWN provides streamlined monitoring for Office365, including 50+ alerting rules upon setup, plus additional customization with the CSE. It also provides comprehensive monitoring for Active Directory, SharePoint, OneDrive, and Exchange admin and mailbox. Additionally, it has alerting rules for authentication: users and access; resource sharing; mail and file operations; and mobile device administration.

AWN CyberSOC™ for Security as a Service (SecaaS)

There is an additional dimension of cloud security: increasingly, security solutions include a cloud-based back end. Businesses rely on single-sign-on services like Okta or directory management services such as Cylance, which also store their data in the cloud. AWN CyberSOC™ integrates with these tools, so it can monitor users and user access regardless of the customer's preferred solution.

Conclusions

Today's businesses rely on sophisticated hybrid architectures, using on-premises hardware alongside a wide range of cloud offerings to maximize IT flexibility and effectiveness.

While this provides organizations with many key benefits, responsible IT leaders must also ensure security for this new architecture. In order to secure today's hybrid businesses, IT leaders must implement a security solution that allows trained cybersecurity professionals to monitor all company systems using a single pane of glass.

AWN CyberSOC™, a security operations center-as-a-service, meets this need. It provides the people, process and technology required to identify and respond to cyberattacks in progress, regardless of which company systems are targeted. It supports detection in major cloud services. And it does all of this through an affordable turnkey solution, allowing organizations of any size to achieve the highest standard of cybersecurity.

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com