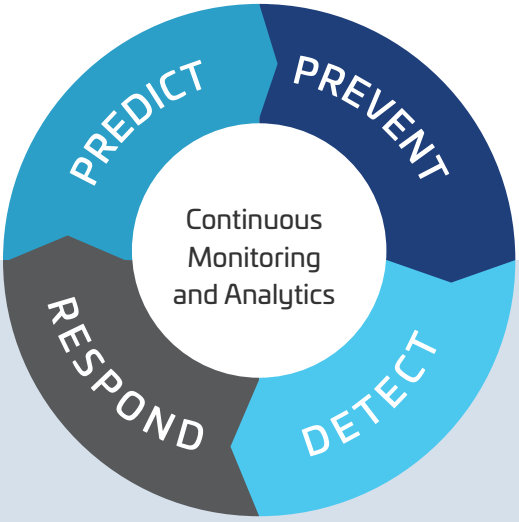

SecureSky
Dynamic Cloud Security
The Modern Enterprise-Level Security Stack
Fully Integrated Security Solution for Organizations of All Sizes
www.securesky.com

The security technology stack has evolved over the years, and the version that many security professionals are using today is not cloud aware, efficient or integrated. In many cases, we've iterated our approach based on best practices at the time, the technologies of the day and the sometimes meager budgets available to us. As in many things IT-related, hanging on to a legacy approach is rarely the best path forward. This is especially the case with something as important as the tool set driving your security posture, which can make or break virtually every part of your business.

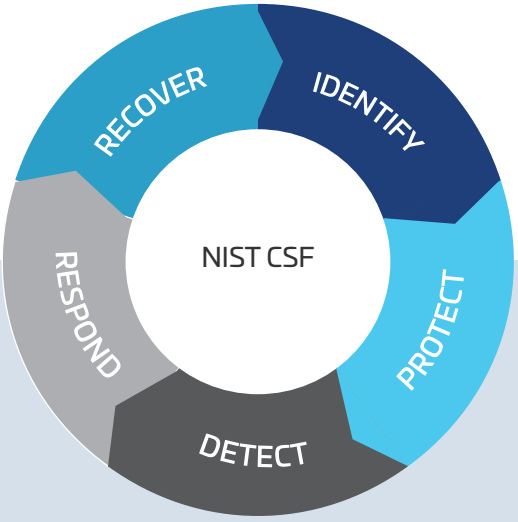
Fortunately, the next-generation security stack, powered by the cloud, is available for cloud environments, large enterprises and small and medium businesses alike.

Evolution of the Security Technology Stack

Most cybersecurity practitioners follow a version of a continuous cycle of risk identification (prioritized by likelihood and impact of threats), prevention (risk protections or controls), threat detection, threat response and, finally, further hardening based on actual or potential threats (remediation or optimization). Two such cycles, Gartner's Adaptive Security Architecture and the NIST Cybersecurity Framework are illustrated below.



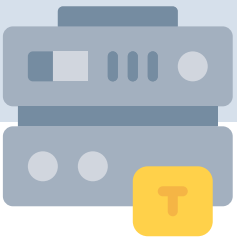
Gartner, Adaptive Security Architecture



NIST Cybersecurity Framework

IT, network and security veterans will vividly recall the early days of attempting to select the best products to address the elements of such full lifecycle frameworks, based on their risk and budget.

First generation providers, many having been spawned from traditional IT networking roots, took a "product" approach, choosing their best fit from emerging technologies in respective categories and having to install, configure, maintain, operate and respond to alerts arising from disparate products. This often led companies to hire specialized, expensive and in-demand resources, or retain external service providers to support their security stack.

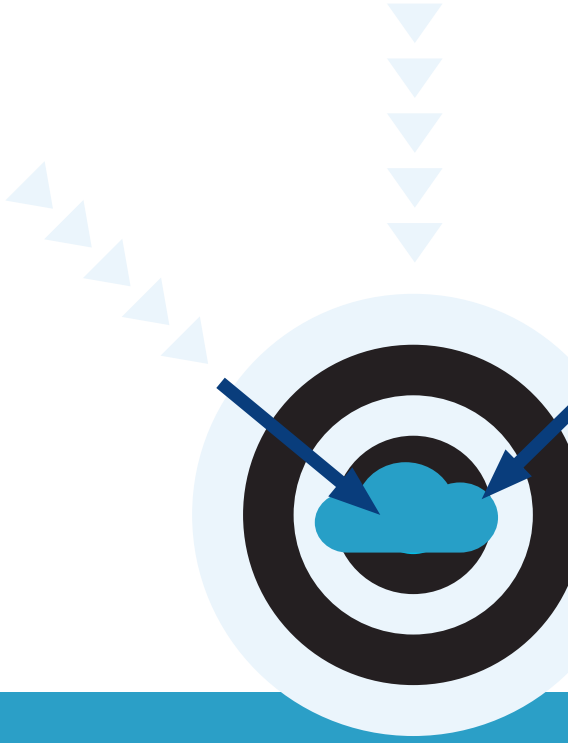


The Security Product Explosion

Public and private investment increased dramatically in the cybersecurity space in the past decade. As security company funding and exit valuations skyrocketed, almost every stage of angel and venture capital flocked to the space to get in on the gold rush. Many startups designed business models specifically to disrupt historical providers or to create niche products to be acquired. Capital also flowed to large established players or consolidations, who used the money to build-out their portfolios. The result was a dizzying array of products and marketing claims that was (and remains) almost impossible to follow.

Most CISOs ultimately procured dozens of products to integrate and monitor, with many overlapping categories from a massive number of vendors. The use of so many fragmented products in many organizations also spurred the growth of consolidation technology such as multi-product management consoles, security information and event management (SIEM), governance, risk and compliance (GRC), and ultimately security orchestration and automation response (SOAR) solutions, as well as their outsourced managed service provider (MSP), managed security service provider (MSSP/MDR) and system integrator (SI) brethren.

The word array below represents the vast array of cybersecurity-related threats, technology, services and outside influences that CISOs and their teams have had to try to deploy and integrate in this massive cyber security explosion.



CASB ENDPOINT SECURITY GRC
DATA SECURITY IoT-OT ZERO TRUST
CLOUD SECURITY SIEM CSPM CARTA
COMPLIANCE & DLP ADAPTIVE SECURITY
BLOCKCHAIN HW-BASED ATTACKS
CYBER INTELLIGENCE FRAUD SOAR
MOBILE SECURITY IAM COVID-19 INSIDER THREATS
SOC DETECTION & PREVENTION
CWPP EMAIL SECURITY CLOUD SECURITY PHISHING
APPLICATION SECURITY WEB SECURITY
INCIDENT RESPONSE & FORENSICS
MSSP/MDR DECEPTION BEC
NETWORK SECURITY

Add the Public Cloud and Digital Transformation to an Already Complex Landscape

Amazon Web Services (AWS) had a few starts and stops in its early days, but it launched officially in 2006. Google Cloud followed in 2008 and Microsoft Azure in 2010.

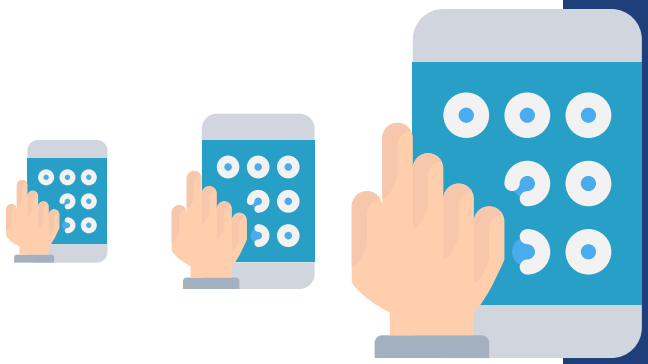
According to a recent Cloud Security Alliance (CSA) report, AWS is the most popular public cloud infrastructure platform, comprising 41.5% of application workloads. Microsoft Azure currently holds 29.4% of the installed base, measured by application workloads. Google Cloud houses 3.0% of application workloads, followed by IBM SoftLayer, Rackspace, and multiple other providers that comprise another 20.7% of the market.

The advent of cloud computing, lowering barriers of availability, access and cost, together with advances in development tools, mobile communications and edge-processing capabilities, have fundamentally changed modern life. Much of the global population is now able to access and respond to data in a manner once considered science fiction, with proliferation of cloud services and almost 10 billion IoT devices and sensors today, which many analysts predict will double or triple in the new few years.

Much of the global population is now able to access and respond to data in a manner once considered science fiction, with the proliferation of almost

10 billion

IoT devices and sensors today, which many analysts predict will double or triple in the new few years.



Legacy Providers vs. Cloud Providers

The requirements for an expansive scope, intelligent automation and tight integration to secure cloud environments has created, and will continue to create, two distinct provider types.

Security innovators described above are still attracting large amounts of capital, however most are currently below $100 million of revenue, and often losing money. To attempt to create fuller-scope product suites required, large players such as NTT, IBM, Verizon, AT&T, Cisco, Palo Alto Networks, Symantec and McAfee, as well as traditional consulting firms such as Accenture and Deloitte, will continue to acquire and develop to expand their offerings.

The second rapidly emerging category of security providers are the public cloud providers themselves. The COVID-19 crisis and related remote workforce scenarios will accelerate the transition of many of the remaining holdouts to the cloud, but the public cloud and SaaS providers know that to retain and continue to grow their market share, they must provide an integrated, enterprise-level security fabric that includes edge-based security.

Cloud Security Maturity

Today, neither of these categories are making security any easier.

The large security players are continuing their traditional "bolt-on" approach, attempting to modify legacy data center solutions for the cloud. Those that are acquiring cloud functionality—such as Palo Alto Network's recent acquisitions of Redlock, Evident.io, Zingbox, Demisto, Twistlock, PureSec and Aporeto—often present as a suite of products but will require multiple-year projects to truly integrate them.

While the major public cloud providers have recently made serious security strides, they still present a plethora of disparate systems, configuration modules, alerting methods and black-box data flows.

While the major public cloud providers have recently made serious security strides, they still present a plethora of disparate systems, configuration modules, alerting methods and black-box data flows.

So Which Category Will Win?

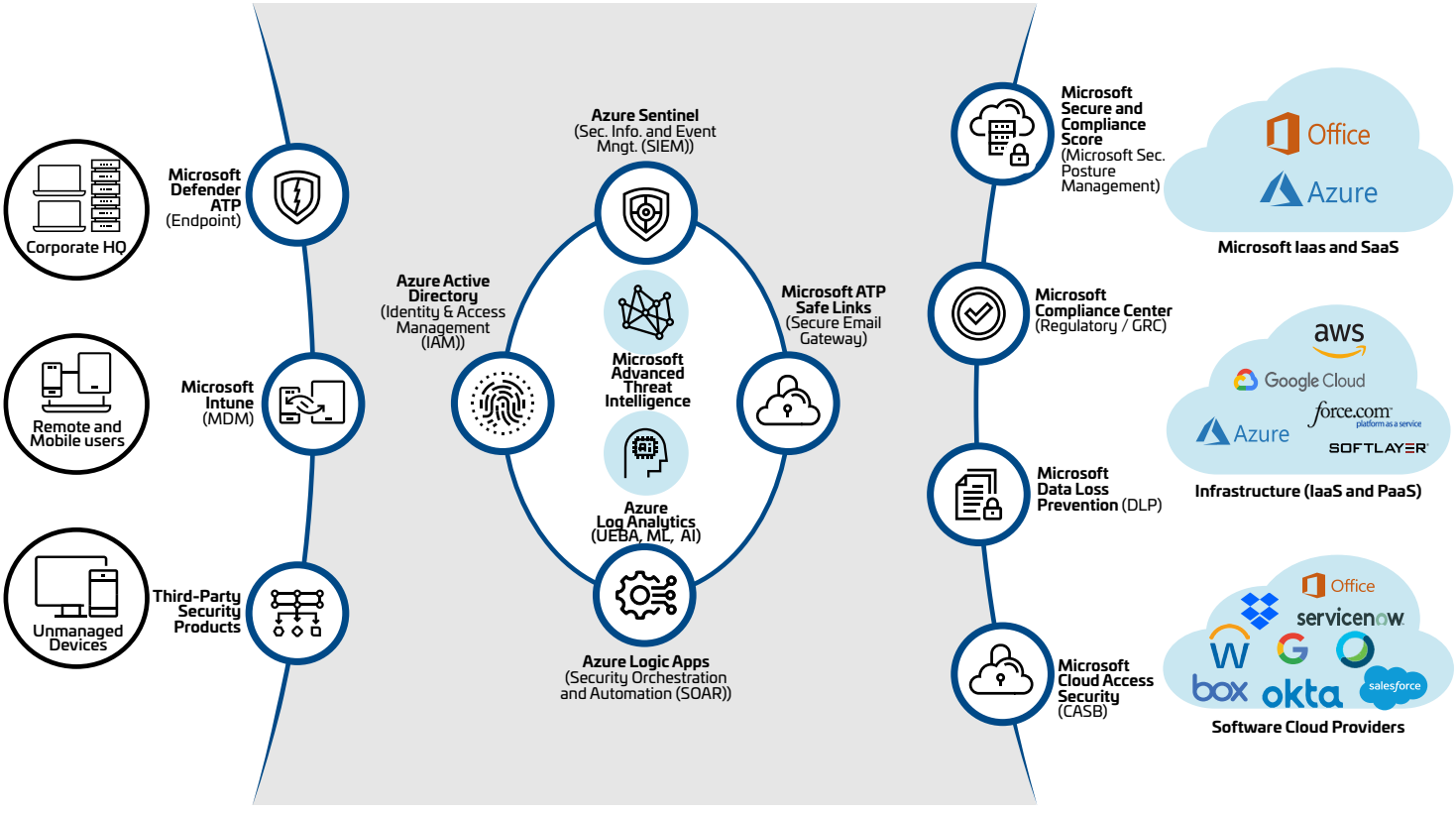
SecureSky believes the latter, for three reasons.

The first and obvious reason is they own the workload stack, and in the case of Microsoft, the largest SaaS application in the world in the form of Microsoft 365. They are in the ideal position to tightly integrate inside their platform and with SaaS providers running on their platforms, as well as orchestrate actions natively.

The second reason is resources. In the most recent trailing twelve months, Microsoft ($41.1 billion), Google/Alphabet ($32.6 billion) and Amazon ($11.3 billion) cleared a total of $85 billion of operating income, meaning revenue minus all business expenses, and none of these companies carry a heavy debt load to service. And as mentioned previously, all three of these businesses are expected to materially grow based on today's uncertain business patterns. This growth will be driven both by movements to the cloud, as well as further movement of shopping patterns away from brick and mortar retail outlets in the case of Amazon. Suffice to say, the major public cloud providers have the resources to impact the security sector in a substantive and transformational way.

Active protection, reducing the attack surface of the environment and automating response, stops the vicious manual response cycle many organizations find themselves in today.

Microsoft Integrated and Distributed Enterprise-Grade Security Solution

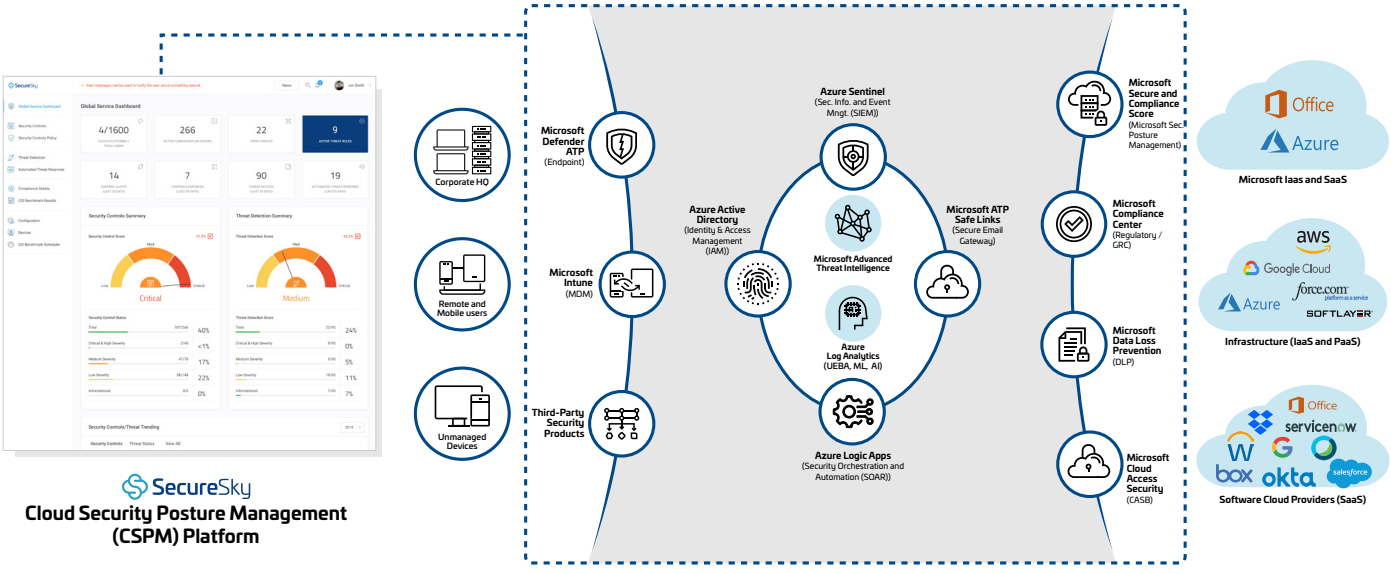


While Microsoft is the current security leader in the competitive cloud provider space, substantial security improvements are also being incorporated, or are in development, at AWS, Google/ Alphabet and other cloud providers as well.

SecureSky's Microsoft Security Enablement

SecureSky's Active Protection Platform greatly simplifies deploying and maximizing the Microsoft security suite, especially for SMBs without specialized resources, by creating full visualization of risks and threats, prioritizing cloud security posture management and enabling rapid remediation and threat response. The platform offers:

- Security and compliance configuration and detection policy assessment as compared to industry-leading benchmarks
- Visualization of cloud security assets, security control configurations and security gaps
- Continuous validation of settings against a security-hardened standard
- Automated or alerted enforcement should changes occur
- Security alert collection, as well as streamlined and automated response mechanisms



SecureSky's Active Protection technology also monitors, remediates and enforces security controls, detects and responds to threats in other IaaS platforms such as AWS and GCP, as well as multiple additional SaaS products.

Rethinking Your Approach

As organizations continue to migrate more and more to the cloud, some will choose to continue with the vicious cycle of category-based product selection, selecting dozens of security products from multiple vendors for their arsenal. They will continue with these attempts, adding resources as needed to integrate and automate across disparate systems.

SecureSky recommends embracing public cloud native security integration and automation, especially considering Microsoft's recent advances, which offer a modern security technology stack for all organizations. We believe this next wave of security evolution from the public cloud providers will continue and accelerate in the future, which will drive innovation.

Five Things Buyers Can Do Today to Prepare

1. Understand the current capabilities and roadmaps of security tools available from your cloud provider(s) of choice, compared with your current security technology stack. In cloud migration planning and deployments, incorporate security measures in your strategies.

2. Review your existing cloud licensing to find redundant functionality you may be paying for twice. You may find this type of redundancy as part of your legacy security technology stack and cloud-native functionality that is included with your current licenses. Determine if the tools available to you provide adequate cloud coverage to assess risk or security control status real-time, as well as provide automation capabilities for security posture management enforcement and threat response.

3. Message corporate leaders on the current and future state of cloud security, and address the upcoming realities with those executives who voice such opinions as "the fox is watching the henhouse," "we are putting all of our eggs in one basket," or "the cloud will never be as secure as on-premise." As discussed throughout this paper, major IaaS and SaaS providers will soon be much more secure than on-premise solutions because of their ability to tightly integrate operational and security tools,

SecureSky recommends embracing public cloud native security integration and automation, especially considering Microsoft's recent advances, which offer a modern security technology stack for all organizations.

automate functions that were once almost exclusively manual and to collect and apply massive amounts of threat intelligence. The caveat to this, of course, is the ability of IT and security practitioners to take advantage of these capabilities.

4. Fully deploy your modem security architecture, extend your zero trust model to include cloud resources and invest in training and optimize security controls to detect, investigate and respond to threats using new automated techniques.

5. Extend and modify your enterprise risk program to include data flows and other risk factors associated with each cloud environment, for example authentication policies, access controls, file sharing, guest users, and application connections.

About SecureSky

SecureSky is a Cloud Security Posture Management (CSPM) company, focused on the continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack against its clients' cloud applications, services and environments. In addition to real-time validation and enforcement to mitigate risk, the SecureSky Active Protection Platform also provides response to current and emerging threats across the entire cloud stack. SecureSky also provides security, compliance and forensic services to enable the enterprise to defend against cybercriminals and state-sponsored attacks.

SecureSky
Dynamic Cloud Security

1 833.473.2759 • info@securesky.com
www.securesky.com